Reflections on the murky legal practices of political micro-targeting from a GDPR perspective

Cristina Blasi Casagran * and Mathias Vermeulen**

Introduction

Political campaigns are increasingly shifting their campaigning efforts from traditional media to online platforms, utilizing the advertising tools offered by Facebook/Instagram,[1] Google/YouTube, Twitter, Pinterest or TikTok. Advertisers believe they are better able to target or reach an audience that may be interested in their message by using an ad platform's targeting tools. Online data collection practices by both the advertiser and the platform allow them to classify and segment their desired audience in an attempt to tailor their messages according to the make-up and profile of specific groups.

Within this context, the phenomenon of political micro-targeting has emerged. The term 'micro-targeting' refers to the extreme form of audience segmentation made possible by mining audience data and combining multiple datasets for predictive analysis.[2] The prefix *micro-* is used to indicate that a highly specific audience is being targeted, ie it always focuses on small, precise, homogeneous groups based on common factors. However, the precise threshold criteria that distinguish micro-targeting from 'regular' targeting practices are not clearly defined elsewhere, as they really depend on each specific context and scope.[3] Micro-targeting can be seen as a subset of 'online behavioural advertising' (OBA),[4] in the sense that not commercial actors but political actors[5] tar-

Key Points

- This article seeks to explore one of the recent controversial EU debates related to political micro-targeting (PMT): is the practice of PMT compliant with the EU's General Data Protection Regulation (GDPR)?
- After examining the two most relevant ad targeting tools used for PMT, this article examines how PMT raises several questions related to (i) some of the principles listed in Article 5 of the GDPR, (ii) the uncertainty on who the data controller is, (iii) the ways to gather valid consent, (iv) excessive profiling practices, and (v) the limited privacy by design and default features.
- It can be argued that significant changes are necessary with regards to the manner in which political actors and social media platforms engage with their data protection obligations in PMT. If these cannot be met and/or are not being complied with, the current way in which PMT is performed could likely be considered unlawful.

* Cristina Blasi Casagran, Assistant Professor, Public Law Department, Autonomous University of Barcelona, Bellaterra, Spain, Email: cristina.blasi@uab.es

** Mathias Vermeulen, Associate Fellow Law, Science and Technology Research Group Vrije Universiteit Brussels, Brussels, Belgium.This work was supported by the Re:constitution programme of Forum Transregionale Studien and Democracy Reporting International. The authors would also like to thank the editors of this journal, the anonymous reviewers, as well as the useful suggestions and comments from Colleen Boland, Daniel Morente, Christopher Neeson and Laureline Lemoine on this article.

1 See 'Facebook Ad Library', *Facebook* <https://www.facebook.com/ads/library> accessed 6 August 2021.

2 'Who targets me' <https://whotargets.me/en/definitions/> accessed 6 August 2021.

3 Tom Dobber, Ronan Ó Fathaigh and Frederik Zuiderveen Borgesius, 'The Regulation of Online Political Micro-targeting in Europe' (2019) 8 Internet Policy Review 4.

4 See Juan Miguel Carrascosa and others, 'I Always Feel like Somebody's Watching Me: Measuring Online Behavioural Advertising', *CoNEXT '15: Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies* 13 (2015), 1–13; Edith G Smit, Guda Van Noort and Hilde AM Voorveld, 'Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe' (2014) 32 Computers in Human Behavior 15–22.

5 For the purpose of these study, the general term of 'political actor' includes political advertisers, political parties, political consultants, data brokers or other data analytics companies.

get individual voters with highly personalized messages by applying predictive modelling techniques to voter data.[6]

In the European Union (EU) and its Member States, the practice of PMT has been increasingly considered a threat to the electoral process, partly because it can operate as a vector for disinformation.[7] It also raises concerns due to the fact that PMT could be used to increase polarization of the electorate,[8] and identify and target weak points where groups and individuals are most vulnerable to strategic influence,[9] amongst others. For instance, it has been evidenced that during the US presidential election of 2016, the Russian Internet Research Agency (IRA) used online targeted advertising to exacerbate tensions and suppress voter turnout among certain groups, including most notably young black Americans involved in racial justice activism. [10] In fact, it was as a result of the experiences in the 2016 US presidential elections that PMT began to receive increased attention from policymakers in the EU.

This study seeks to explore one of the recent controversial EU debates related to PMT:[11] is the practice of PMT compliant with the EU's General Data Protection Regulation (GDPR)?[12] After examining the two most relevant ad targeting tools used for PMT the article explores how PMT raises several questions related to some of the principles listed in Article 5 of the GDPR, namely (i) lawful processing (ii) the purpose limitation principle (iii) the data minimization principle (iv) the data accuracy principle, and (v) data accountability. It can be argued that significant changes are necessary with regards to the manner in which political actors and social media platforms engage with their data protection transparency obligations in PMT. If these cannot be met and/or are not being complied with, the current way in which PMT is performed could likely be considered unlawful.

Ad targeting tools relevant for political micro-targeting

PMT usually takes place via social media platforms. The majority of online ad-driven platforms enable advertisers to define particular target groups for the ad prior to its creation. Then the platform delivers the ad to specific users based on the advertisers' budgets, their ad performance objectives, and the predicted relevance to certain users. For PMT conducted by social media platforms, two advertising mechanisms stand out: (i) Attribute-based Audiences technology, and (ii) Personally Identifying Information Audiences technology.[13]

Attribute-based Audiences targeting tools allow political actors to manually select a target audience for a particular ad or ad campaign based on various characteristics, using data that the social media platform has previously collected and processed about individuals. Facebook, for instance, lists five characteristics that can be selected for such targeting: (i) location, (ii) demographics, (iii) interests, (iv) behaviour, and (v) connections. Through this tool, political actors could, for instance, specify that their ad campaign should target 'males living in Barcelona interested in politics and religion, between the ages of 25-30'. Their ad would be displayed for users that the platform estimates fit these attributes, but political actors in principle will not have access to those users' personal information. It is important to add that for these cases, the ad platform is the sole data controller.

A second category of targeting tools is termed Personally Identifying Information Audiences (PII Audiences) ad delivery tool. Depending on the platform, this tool is referred to as 'Custom Audiences'

6 Ira Rubinstein, 'Voter Privacy in the Age of Big Data' (2014) 5 Wisconsin Law Review 861–936.

7 Dobber, Ó Fathaigh and Borgesius (n. 3); Kirill Ryabtsev, 'Political Micro-Targeting in Europe: A Panacea for the Citizens' Political Misinformation or the New Evil for Voting Rights (2020) 8 Groningen Journal of International Law 1.

8 Judit Bayer, 'Double Harm to Voters: Data-driven Micro-targeting and Democratic Public Discourse' (2020) 9 Internet Policy Review 1, 10; Matteo Cinelli and others, 'The Echo Chamber Effect on Social Media' (2021) 118 Proceedings of the National Academy of Sciences 9.

9 Anthony Nadler, Matthew Crain and Joan Donovan, 'Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech' *Data & Society Research Institute*, 5 (*datasociety.net*, 17 October 2018) <https://datasociety.net/library/weaponizing-the-digital-influence-machine/> accessed 6 August 2021.

10 Jason Parham, 'Targeting Black Americans, Russia's IRA Exploited Racial Wounds' (*Wired*, 12 August 2018) <https://www.wired.com/story/russia-ira-target-black-americans/> accessed 6 August 2021.

11 Samuel Stolton, 'EU Executive Mulls Tougher Rules for Microtargeting of Political Ads' (*Euractiv*, 3 March 2021) <https://www.euractiv.com/section/digital/news/commission-mulls-tougher-rules-for-microtargeting-of-political-ads/> accessed 6 August 2021.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 ('GDPR').

13 These technologies have been previously analysed by Giridhari Venkatadri and others, 'Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface' *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2018; and Giridhari Venkatadri and others, 'Investigating Sources of PII used in Facebook's Targeted Advertising' (2019) 1 Proceedings on Privacy Enhancing Technologies 227–44.

Table 1. Main personal data items that political actors can upload to create PII Audiences

	Name	Email	Phone Nr.	City/ ZIP	State/ Province	Birthday/ Gender	Employer	Site user ID	Mobile Advertiser ID
Facebook	●	●	●	●	●	●		●	●
Instagram	●	●	●	●	●	●		●	●
Twitter		●	●					●	●
Google	●	●	●	●				●	●
Pinterest		●							●
LinkedIn							●		●

Giridhari Venkatadri and others, 'Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface' Proceedings of the IEEE Symposium on Security and Privacy (S&P), May 2018, 2.

(Facebook),[14] 'Customer Match Audiences' (Google),[15] 'Tailored Audiences' (Twitter),[16] 'LinkedIn's Audience Match' (LinkedIn)[17] and 'Pinterest's Audiences' (Pinterest)[18] respectively. In theory, these tools would allow political actors to target their existing contacts on the ad-driven platform via multiple methods. The most common way to execute this is by uploading a list of email addresses, phone numbers or mobile advertiser IDs[19] the political actor already possesses in order to then identify the associated social media accounts of the existing customer. The personal information that political actors can upload varies from one platform to another, as shown in Table 1 below.

Some of these items are sufficient as stand-alone attributes to create a custom audience. For instance, on Facebook it is enough to have an e-mail address, phone number, mobile advertiser ID, Facebook app user ID, or Facebook page user ID to create a custom audience, whereas other items such as the user's first name or the city require complementary personal data before such a custom audience can be generated.[20] There is no limit on the size of lists that can be uploaded to PII Audiences tools. As a result, in theory political actors (and advertisers in general) are able to introduce thousands of pieces of personal data if they wish to do so. Political actors using these tools could have obtained personal data (online or offline) through a variety of methods and sources, including from the membership/donors registers of the political party, from public voter files, or in return for some form of 'free' service/voucher for which users had to first provide their personal details.

It is important to note that in this context US political parties have access to far more personal information on their voters than political parties in the EU. Both the Republicans and the Democrats have their own 'in-house' databases, a system called 'Votebuilder', which include voter registration data, data from commercial and public sources, as well as data from telephone polling and voter contact. Similar data sources do not exist in Europe, so there is comparatively less information available on how such parties collect data on the wider electorate, beyond that of their members, donors, and regular contacts.[21] These parties rely on the expertise of political marketers and analysts who can easily produce so-called 'enhanced voter files' by merging their lists with other databases, and double check the accuracy of the results through targeted surveys on political preferences.[22]

Once the personal data is uploaded to the social media platform, the platform creates an audience of users that correspond with an attribute. It typically takes up to a few hours for the social media platform to create

14 See 'How to use Facebook custom audiences' <https://www.facebook.com/business/a/custom-audiences> accessed 6 August 2021.

15 See 'Google customer match help' <https://support.google.com/adwordspolicy/answer/6299717?hl=en> accessed 6 August 2021.

16 See 'Tailored audiences' <https://business.twitter.com/en/targeting/tailored-audiences.html> accessed 6 August 2021.

17 See 'Account Targeting' <https://business.linkedin.com/marketing-solutions/ad-targeting/account-targeting> accessed 6 August 2021.

18 See 'Stop interrupting. Start inspiring.' <https://business.pinterest.com/en/advertise/> accessed 6 August 2021.

19 Mobile advertiser ID is a mobile-OS-provided identifier, unique for each device (although it can be reset by the user). Advertisers use it to target mobile users who have already installed the advertiser's app.

20 Ibid 3.

21 Colin J Bennett, 'Voter Databases, Micro-targeting, and Data Protection Law: Can Political Parties Campaign in Europe as they do in North America?' (2016) 6 International Data Privacy Law 4, 262 and 267.

22 Solon Barocas, 'The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process' (2012) In: International Conference on Information and Knowledge Management, Proceedings, *PLEAD'12 - Proceedings of the 2012 ACM Workshop on Politics, Elections and Data, Co-located with CIKM 2012*, 32.

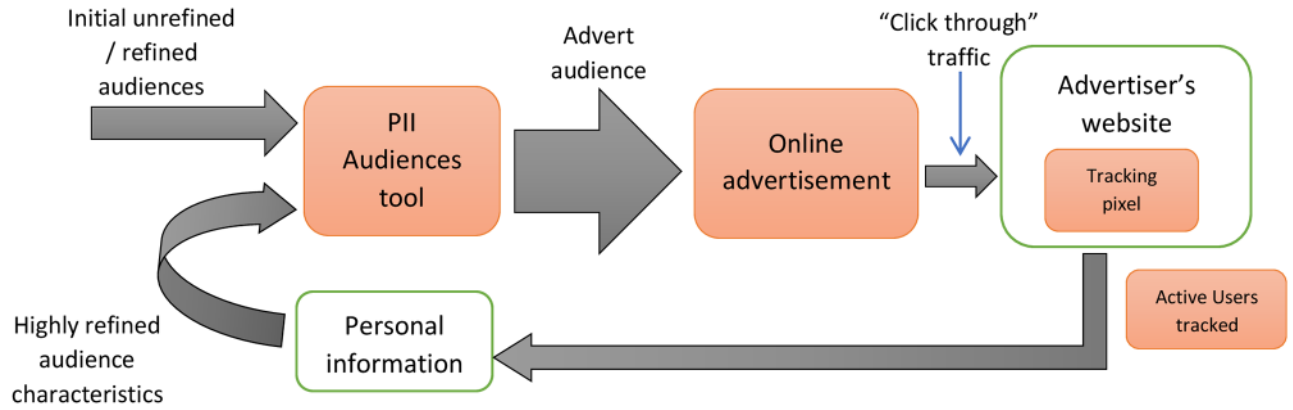

Figure 1. Tracking pixel audiences' procedure. *Source*: Own elaboration.

the custom audience after the advertiser uploads the personal data.[23] This is performed through an algorithmic method that matches the initial personal data with people who supposedly share similar interests and traits.[24] Although the relationship between party databases and ad-targeting through social media differs significantly from country to country, investigations conducted by data protection authorities (DPAs) have helped clarify the sources of personal data collected, used and combined for PMT.[25] As illustrated in the Table 2 below, after comparing three of the main ad platforms, it can be concluded that each of them offers different attributes for targeting purposes.[26]

Many of these categories do not formally reveal political affiliations,[27] but they could serve as a proxy for someone's political views, without being political data as such. This could be the case with data on social policies, education, national economy, homeland security, or migration-related issues. When combined, some of these pieces of information can serve as extremely relevant for political parties, as they may indirectly indicate political ideology traits. For instance, by targeting people who are interested in environment and animals, one could assume that the user might be more inclined to vote for Green parties.

In addition, on Facebook there is an interesting feedback loop made available to advertisers (including political actors) to redefine their ads as well as their audience. In fact, social media platforms like Facebook constantly refine elements such as text, imagery, organization, and colour when serving ads. As illustrated in Figure 1, once advertisers have created unrefined and/or refined custom audiences for their ad, they receive a pixel code to include on their website. The pixel is a small portion of Javascript code from Facebook that advertisers can install on their website, which collects information on whether a user actually arrives there from the Facebook ad. By monitoring Facebook users' interactions with the website, advertisers can then use the personal characteristics of these users who visited the external website to refine their original audience, discarding those users that are not likely to click on the advert.

Many researchers and campaigners have long raised concerns about the lack of transparency related to the use of both categories of ad delivery tools,[28] with transparency being a critical component in determining

23 Venkatadri and others, Privacy Risks with Facebook's PII-based Targeting (n 13) 2.

24 Most platforms state that they do not capture customer information uploaded for custom audience creation. See 'What Happens When I Upload My Customer List to Facebook?' <https://www.facebook.com/business/help/112061095610075> accessed 6 August 2021; 'Intro to Custom Audiences < https://business.twitter.com/en/help/campaign-setup/campaign-targeting/custom-audiences.html> accessed 6 August 2021; 'Audience Targeting' <https://help.pinterest.com/en/articles/targeting> accessed 6 August 2021; and 'How Google uses Customer Match data'<https://support.google.com/adwords/answer/6334160> accessed 6 August 2021.

25 Information Commissioner's Office (ICO), 'Democracy disrupted? Personal information and political influence', 22 and ff, July 2018 <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf> accessed 6 August 2021.

26 This information was collected through three different experiments conducted in December 2020, following the regular procedure that advertisers (including political actors) need to go through to launch an ad via each of these social media platforms. One of the authors followed the procedure to create and publish political ads for each of the three selected social media platforms (Facebook, Twitter and LinkedIn). Throughout this process they could identify all the available categories of data that advertisers can tick before the ad is actually launched.

27 ICO (n 25).

28 Upturn, 'Leveling the Platform: Real Transparency for Paid Messages on Facebook' May 2018 <https://www.upturn.org/reports/2018/facebook-ads/> accessed 6 August 2021; Mathias Vermeulen, 'The Keys to the Kingdom. Overcoming GDPR-concerns to Unlock Access to Platform Data for Independent Researchers' (2020) *OSF Preprints* <https://ideas.repec.org/p/osf/osfxxx/vnswz.html> accessed 6 August 2021. See also the letter that more than 200 Researchers Signed Supporting Knight Institute's 'Proposal to Allow Independent Research of Facebook's Platform' <https://knightcolumbia.org/content/more-than-200-researchers-support-knight-institute-call-to-facilitate-research-of-facebooks-platform> accessed 6 August 2021.

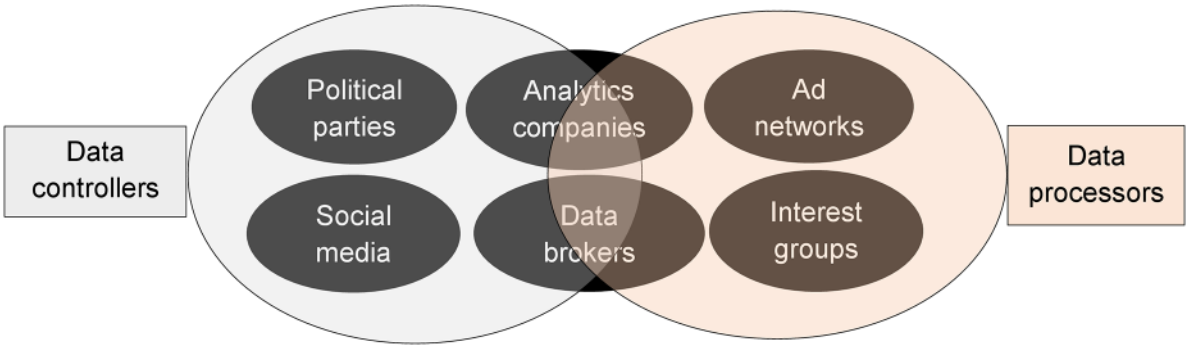

Figure 2. Potential data controllers and processors in PMT. *Source:* Own elaboration.

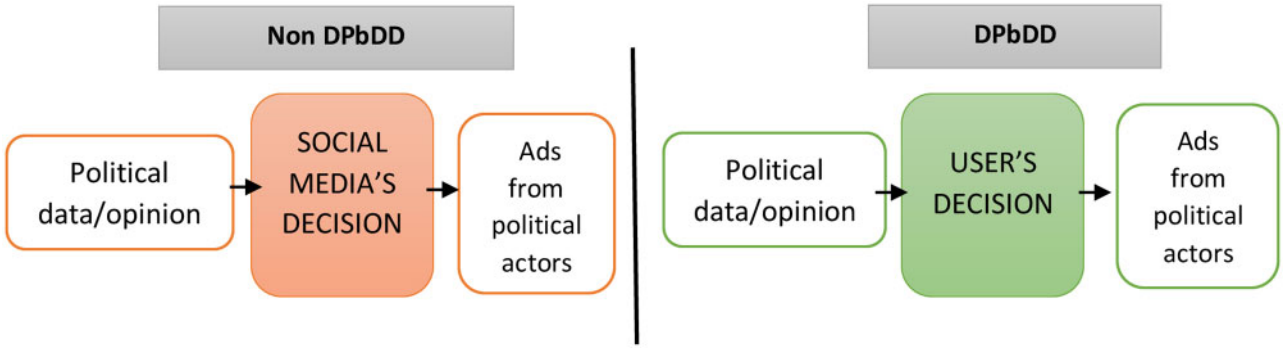

Figure 3. *Non DPbDD v. DPbDD* practices. *Source:* Own elaboration.

GDPR compliance. Likewise, the European Data Protection Board stated in 2019 that the manner in which personal data is processed to enable micro-targeting by political actors could pose serious risks, not only to individuals' rights to privacy and data protection, but also to wider trust in the integrity of democratic processes themselves.[29]

Moreover, as detailed in the following sections, PMT raises several questions related to some of the principles listed in Article 5 of the GDPR, namely (i) lawful processing, (ii) the purpose limitation principle, (iii) the data minimization principle, (iv) the data accuracy principle, and (v) data accountability.

Is personal data lawfully processed for PMT purposes?

Pursuant to Article 6(1) of the GDPR, personal data processing is lawful only if the data controller applies one of six legal grounds for processing: (i) the data subject has given consent, (ii) the processing is necessary for the performance of a contract, (iii) the processing complies with a legal obligation to which the controller is subject, (iv) the processing seeks to protect someone's vital interests, (v) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and (vi) the purpose is of legitimate interest pursued by the controller or by a third party.

Two main issues of concern arise when assessing the compliance of such principles. First, it is not always easy to determine in PMT who the data controller is. In addition, once the data controller is identified, it is often unclear whether they have obtained valid consent from users prior the processing of their personal data for PMT purposes. This is especially important because PMT performed by any other actor than political parties requires explicit consent, regardless of whether the data items used are sensitive or not.

Who is data controller?

To determine whether these grounds are adequately met, it is essential to first identify who the data controller is. In this regard, one of the main complexities underlying PMT is how it can involve many different actors, which could create uncertainty as to who the

29 EPDB, 'Statement 2/2019 on the use of personal data in the course of political campaigns' (13 March 2019) <https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_en> accessed 6 August 2021.

data controllers and data processors are. In particular, PMT could include the participation of political advertisers, political parties, political consultants, online platforms, data brokers and data analytics companies.

In general, two types of actors could qualify as data controllers of data processed during PMT: the online platforms and the political actors. Yet, as illustrated in Figure 2 above, these two groups could be still divided into many different sub-categories of actors that may use personal data in the course of political campaigns, such as interest groups, data brokers, analytics companies, or ad networks. All these actors can play an important role in the election process and their compliance should be subject to supervision by independent data protection authorities.[30] On data brokers specifically, the Commission has explained that they 'may act as controllers or processors depending on the degree of control they have over the processing'.[31] Similarly, analytics companies could be data controllers or data processors depending on whether they collect data on potential voters themselves or they process data originally collected by political parties.

Online platforms such as Facebook, Twitter, or LinkedIn should be considered the only data controllers if the ad is distributed via the above-mentioned Attribute-based Audiences tool. Yet, the same conclusion does not seem to apply when the Personally Identifying Information Audiences tool is used. Online platforms have long argued that they are mere data processors in the use of Personally Identifying Information Audiences tools, as it is the advertiser who initially collects and introduces personal data items into the online platform system. In 2018 the Bavarian Administrative Court had to assess whether it was only the advertiser or also Facebook who processed personal data via PII Audiences tool. The Court concluded that both Facebook and the user of the Audience tool should be considered joint data controllers.[32] Similarly, the Court of Justice of the EU (CJEU)[33] as well as national data protection authorities[34] have supported this idea that social media companies offering 'custom' audiences should be considered joint controllers with the advertiser. This broad interpretation of joint controllership is based on the rationale that an entity exercising influence over the processing of personal data can be considered a data controller, regardless of whether they have issued written instructions to that effect.[35]

However, it could be possible that PMT be conducted entirely by political actors without any involvement from online social media platforms (for instance, by sharing an ad on their own websites). In such cases, the political actors themselves should be considered sole data controllers. A debate has emerged in this regard because the term 'political actors' encompasses a variety of sub-categories.[36] The first sub-group would include core political advertisers, ie actors which exist for the sole purpose of gaining and exercising political representation. This can include (European) political parties, elected officials, candidates, parliamentary factions or political foundations. The second sub-group would be composed of peripheral political advertisers, ie actors which either (i) receive any form of compensation from core political advertisers to spread their messages or (ii) speak on behalf of core political advertisers and their interests, such as social media influencers, or independent organizations and corporations running political ads.

A full legality assessment of PMT by all of these actors is beyond the scope of this article. However, for the purposes of this analysis, it is important to flag that currently the GDPR does allow political parties to process personal data on people's political opinions 'for reasons of public interest' where, in the course of electoral activities, the operation of the democratic system in a Member State requires such processing.[37] Yet, the meaning of 'electoral activities' and 'reasons of public interest' is not clearly defined and the issue has not been raised yet in complaints to data protection authorities. Therefore, in practice, political parties are given significant leeway to process personal data, including even special category data such as political beliefs or religion. Yet, that same leeway is not afforded to other political actors and to online platforms—which in practice would need to rely on users' consent to process special category data.

30 Ibid.

31 European Commission, 'Answer given by Ms Jourová on behalf of the European Commission. Question reference: E-000054/2019' (2019) <https://www.europarl.europa.eu/doceo/document/E-8-2019-000054-ASW_EN.html> accessed 6 August 2021..

32 VG Bayreuth, Beschluss v. 08.05.2018 – B 1 S 18.105.

33 Case C-210/16 Wirtschaftsakademie Schleswig-Holstein [2018] ECLI:EU:C:2018:388.

34 ICO, 'Direct Marketing Code of Practice Draft Code for Consultation', 8 January 2020 <https://ico.org.uk/media/for-organisations/documents/2021/2619043/direct-marketing-code-draft-guidance-122020.pdf> accessed 6 August 2021.

35 Case C25/17 Tietosuojavaltuutettu [2018] ECLI:EU:C:2018:551, para 68.

36 Julian Jaursch, 'Defining Online Political Advertising. How Difficulties in Delineating Paid Political Communication Can Be Addressed' (2020) Stiftung Neue Verantwortung 19–20.

37 GDPR (n 12) recital 56.

The need for valid consent to process data for PMT

Given the lack of transparency surrounding social media ad delivery,[38] it is virtually impossible to validly obtain consent from data subjects for PMT. Articles 13 and 14 of the GDPR have strict requirements on information that must be provided to data subjects, such as the purposes for collecting data, the recipients of data and the legal basis for processing. In this sense, it is particularly important to ensure transparency in cases of 'invisible' processing,[39] where users are not aware that a specific actor is collecting and using their personal data for a specific purpose—which is often the case with PMT. In line with the transparency requirements described by the Article 29 Working Party, a data subject should be able to determine in advance what the scope and consequences of the processing are, and they should not be taken by surprise at a later point by the ways in which their personal data has been used.[40] This criterion is clearly not met with the ad delivery practices described in the Section 'Ad targeting tools relevant for political micro-targeting' above.

Even obtaining general consent for non-special category data is challenging for PMT purposes. Pursuant to Article 7 of the GDPR, consent needs to be 'freely given, specific, informed and unambiguous'. Yet, consent in relation to targeting practices is generally bundled into wider terms and conditions associated with the social media platform, which makes it difficult to fulfil the requirement outlined above. As concluded by the CJEU in the Planet49 case, failing to collect consent via a 'clear affirmative action' by the users could led to a breach of the GDPR.[41] For instance, according to the court, it would appear impossible in practice to determine objectively whether users had actually given their consent by not deselecting a pre-ticked checkbox that is required for continuing their primary activity on the website visited.[42]

Furthermore, consent should not be regarded as freely given if the data subject has no genuine or free choice, or is unable to refuse or withdraw.[43] For the purpose of this study, the possibility to withdraw a user's consent from being micro-targeted on Facebook has been explored.[44] After navigating through all options accessible to Facebook users, it was concluded that Facebook only partially allows withdrawal of consent to being subject to micro-targeting, and there is no possibility to withdraw consent to being subject to PMT. In particular, Facebook users have the capacity to uncheck (i) advertisers including the user in a list, (ii) shops interacted with through the platform, (iii) pages liked, and (v) ad clicks through the platform. However, users have no choice to opt out of being targeted via specific attributes such as location, gender, age, etc. Also, users have no possible way of preventing exposure to ads launched by political actors.

Lastly, since a user's political beliefs are considered a special category of data,[45] PMT performed by any other actor than political parties requires explicit consent, regardless of whether the data items used are sensitive or not. In 2011, Korolova had already demonstrated that through the Attribute-based Audiences technology on Facebook, advertisers could correctly infer the sexual orientation of a non-friend even when they were sharing their status in a 'Friends Only' visibility mode.[46] Many similar experiments conducted on Facebook have also shown that the platform—through 'likes' and content uploaded from other users—can automatically and accurately predict a range of highly sensitive personal attributes such as sexual orientation, ethnicity, religious, gender, and political views.[47] Therefore, based on these precedents, it could be argued that PMT should be considered sensitive in and of itself: it consists of targeting users who are likely to agree with the particular political ideology of a political actor. Consequently, prior explicit

38 Upturn (n 28); Vermeulen (n 28) 12–15.

39 ICO, 'Audits of data protection compliance by UK political parties', *Summary Report*, November 2020 <https://ico.org.uk/media/action-weve-taken/2618567/audits-of-data-protection-compliance-by-uk-political-parties-summary-report.pdf> accessed 6 August 2021.

40 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) *wp260rev.01*.

41 C673/17 Planet49 GmbH [2019] ECLI:EU:C:2019:801, para 61.

42 Ibid, para 55.

43 GDPR (n 12) recital 42.

44 The experiment was conducted on December 2020 and it was focused on the social media platform Facebook as it is the main advertising platform that conducts PMT. The authors accessed the data through the option 'manage your data' on Facebook and could find out the business that had included them in their lists via 'Business who uploaded and used a list'. With this information, the authors could click on each of the businesses and were given the chance to stop being part of the specific list linked to the business. However, in the 'What to expect' tab Facebook warns that 'You may still see ads from advertisers for other reasons, such as your age, gender, visiting their website or shopping at their shop'. Similarly, the authors accessed 'Whose ads you've clicked' but for each of the identified businesses there was only the possibility to hide ads, but not to effectively withdraw micro-targeting.

45 GDPR (n 12) art 9.

46 Aleksandra Korolova, 'Privacy Violations using Microtargeted Ads: A Case Study' (2011) 3 Journal of Privacy and Confidentiality 1, 35.

47 Kurt Thomas, Chris Grier and David M Nicol, *Unfriendly: Multi-party Privacy Risks in Social Networks*, PETS (Berlin, Springer 2010); Michal Kosinski, David Stillwell and Thore Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) *PNAS: Proceedings of the National Academy of Sciences of the United States of America* 110, 15; Neil Zhenqiang Gong and Bin Liu, 'You Are Who You Know and How You Behave: Attribute Inference Attacks via Users' Social Friends and Behaviors' (2016) *Proceedings of the 25th USENIX Security Symposium*.

consent to target users should be obtained by political actors.

In conclusion, it can be argued that significant changes are necessary with regards to the manner in which political actors and social media platforms engage with their data protection transparency obligations in PMT. If these cannot be met and/or are not being complied with, the current way in which PMT is performed could likely be considered unlawful.

Compliance with other data protection principles

Apart from the aforementioned difficulty of proving valid consent to be subjected to PMT, the practice is difficult to square with a number of other data protection principles. One of the main data protection-related concerns of political advertising is the potential violation of the purpose limitation principle. Particularly, Article 5(1)(b) of the GDPR establishes that a specific and legitimate reason is needed for any personal data collected. Regarding the question of whether PMT processes data under a legitimate purpose, the answer is not as straightforward. One could assume that the legitimate purpose would be to increase 'political or democratic engagement'.[48] As such it would enable a wide range of political activities inside and outside election periods such as: communicating with electors and interested parties; surveying and opinion gathering; and activities to increase voter turnout.[49] But it is unclear whether all activities linked to PMT would fit within this definition. Also, it is worth adding that the collection of personal data by social media platforms and then processed for political advertising is based on an objective different from the original (commercial) collection purpose, and therefore this second processing should be restricted, unless there is informed consent from the user.

One of the other principles relevant to conducting PMT is the data minimization principle. Article 5(1)(c) of the GDPR establishes that the processing of personal data has to be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. In essence, compliance with this principle would mean that the personal data items used to target voters are the minimum criteria that political actors need to fulfil their purpose. It would also require periodic reviews of the data held, with deletion of the data items that are no longer necessary. Assessing whether PMT conforms with this principle is considerably complex. Micro-targeting requires the collection of large amounts of data: big data sets are first sorted by the online platform according to predictive analytics and psychological targeting,[50] but the exact type and number of personal data items combined and aggregated for micro-targeting purposes is usually not fully disclosed by social media platforms.

The data minimization principle may be infringed upon due to the vast amount of data categories collected and put at the disposal of political actors (see Table 2 above). In fact, data items used for PMT could correspond to the same categories selected by very different advertisers, such as those advertising perfumes or shoes. This could be used as an argument to impose additional restrictions on the kinds of available data sources certain political actors could use. However, any such restriction may in fact conflict with Article 10 of the European Convention on Human Rights (ECHR). It could be argued that PMT represents a form of political speech. Under Article 10 of the ECHR, such political expression would enjoy a 'privileged position', and would thus receive considerable legal protection.[51]

In addition, a proper application of the transparency principle would also lead to necessary reinforcement of the accuracy principle. Users would be able to check what data has been used to build their profiles for targeting by political actors, and they would also have the right to enforce the rectification principle on potential inaccurate personal data if necessary (Article 16 of the GDPR). Even in cases where the specific data item is correct, the aggregation of that piece of data to a profile could result in an inaccuracy. On the question of whether inferred data could be rectified if inaccurate, Article 29 WP concluded that both the 'input personal data' (the user's personal data used by the controller to create the profile) and the 'output data' (the profile itself created by the controller or 'score' assigned to the person) could be challenged by a user as in breach of the data accuracy principle.[52] However, social media platforms could always argue that the spotted inaccuracy is of a subjective nature,[53] as the same data item separated from the profile would not require any rectification at all.

48 Bennett (n 21) 266–67.

49 See ICO, 'Lawful databases' <https://ico.org.uk/for-organisations/guidance-for-the-use-of-personal-data-in-political-campaigning/lawful-bases/> accessed 6 August 2021.

50 IDEA, 'Webinar Series: Online Political Advertising and Microtargeting: The latest legal, ethical, political and technological evolutions', 15 and 18 June 2020, Meeting Report, 4.

51 Dobber, Ó Fathaigh and Borgesius (n 3) 8.

52 Article 29 Working Party (2018), 'Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679', *WP 251 rev.01*, 6 February 2018, 17–18.

53 Sarah Eskens, 'A Right to Reset your user Profile and more: GDPR-rights for Personalized News Consumers' (2019) 9 *International Data Privacy Law* 3, 169.

Table 2. User attributes identified for micro-targeting

Attributes	FACEBOOK	TWITTER	LINKEDIN
Education	✓	✓	✓
Financial status according to the ZIP code	✓		
Interest in economy and finance		✓	✓
Anniversaries	✓		
Information on whether the person in away from home / expats	✓		✓
Family and parenting, including age of children	✓	✓	
Relationship status	✓	✓	
Life stages (mum, dad, auto-intender, empty nester, students. . .)		✓	
Information related to work (employer, sector, job title. . .)	✓		✓
Work experience (skills, years, level)			✓
Recent change of job	✓		✓
Interest in business, industry, marketing & retail	✓	✓	✓
Interest in automotive topics		✓	
Interest in beauty, style & fashion		✓	
Interest in music & radio		✓	
Interest in books and literature		✓	
Interest in art & entertainment (movies & TV)	✓	✓	✓
Interest in specific movies or TV shows		✓	
Interest in specific events		✓	
Interest in politics	✓	✓	✓
Interest in charity	✓		
Interest in community issues and volunteering	✓		
Interest in environment	✓		✓
Interest in law / government	✓	✓	✓
Interest in religion	✓		
Interest in sustainability / home & garden	✓	✓	
Interest in careers / job search		✓	✓
Interest in sports & sporting events		✓	
Interest in specific food / drink		✓	
Interest in health		✓	✓
Interest in pets		✓	
Interest in science		✓	✓
Interest in travel		✓	✓
Hobbies and interests (guitar, gossip, cigars, comedy, dance, paranormal stuff etc.)			
Veterans	✓	✓	
Consumer classification for specific non-EU countries	✓		
Interest in digital activities, technology, computing, social media	✓	✓	✓
Engaged shoppers / people previous campaigns or ads	✓	✓	✓
Location	✓	✓	✓
Age	✓	✓	✓
Gender	✓	✓	✓
Languages	✓	✓	✓
Users' connections (eg friends of people who Like a political party page Group)	✓		
Specific conversation topics		✓	
Device model /carrier	✓	✓	

Finally, PMT practices may not conform with the accountability principle either. As stated in Article 5(2) of the GDPR, controllers and processors should take responsibility for their processing activities and put appropriate measures and records in place to demonstrate their compliance with data protection principles. Yet today the information and scope of PMT is still unknown: there is not sufficient knowledge about the amount and types of data that are used for targeting, and there is no public accountability or scrutiny mechanisms regarding the algorithms created by social media platforms to deliver ads either.[54] There is thus an accountability gap created by the use of massive amounts of personal data in non-transparent ways, as well as via the provision of countless ads targeted at various audiences to impact people's political choices.[55]

Profiling concerns

While people's interactions with online social media services serve as inputs for the construction of personal profiles,[56] PMT is a way to successfully create user profiles for ad delivery by political actors. Thus, in addition to the rules on lawful bases for processing, PMT may involve automated decision-making (profiling) related to a person's vote in an election.

According to the GDPR, 'profiling' consists of any form of automated processing of personal data evaluating personal aspects relating to a natural person.[57] This could include information on the subject's performance at work, economic situation, health, personal preferences, and interests and behaviour, as well as location or movements.

Under the GDPR, data profiling is not forbidden, but it is subject to certain restrictions.[58] Such profiling practices need to be transparent and easily accessible, as the data subject whose data is profiled has the right to oppose them at any time.[59] Yet, PMT demonstrates that this is not always the case.

As outlined above, political actors that are interested in targeting voters online via social media have two main sources of data: (i) profiles already created in their own registers or (ii) profiles created by social networks and online apps, accessed through paying intermediaries such as digital marketing analysts and data brokers. These two options could also be combined, pairing voter profiles from political registers with social media data.

It is worth adding that profiling can be applied to a group or to an individual, and it can be direct or indirect.[60] For political advertising, individual and direct profiling usually takes place when data is collected via membership registries or when users subscribe to any of the political party's products. An example can be found in the data collected by Brexit campaigners in 2016 through the app *thisisyourdigitallife*. This data was subsequently used to profile and build political audience characteristics. In this case, hundreds of thousands of users were paid to take personality tests and agreed to have their data collected for academic use.[61]

In contrast, if ads from political actors are delivered through social media platforms, in principle only group profiles are targeted, either directly or indirectly. Through the above-mentioned Attribute-based Audiences tool, advertisers do not introduce any specific personal information for the target group, but rather only attributes. For instance, advertisers could choose for their ads to be displayed for all 35-year-old females living in Paris and interested in environmental matters. Through its machine-learning algorithms—trained to detect relevant patterns—the social media platform would likely target thousands of profiles with the selected criteria. The advertiser would never know (in principle) the identity behind those targeted users. The platform would only inform the advertiser about the number of matched records (ie the audience size). Likewise, if advertisers decide to use the PII Audiences tool instead, they would introduce one external piece of personal information, through which the platform would then link to its own data, targeting group profiles with characteristics similar to the original piece of information.

Although these two Facebook tools are designed to provide only group profiles, previous studies have demonstrated that it is possible to achieve individual

54 Muhammad Ali and others, 'Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging' (2019) Cornell University, 13.

55 IDEA (n 50) 2.

56 Taina Bucher, '(Big) Data and Algorithms' in Leah A Lievrouw and Brian D Loader (eds), *Routledge Handbook of Digital Media and Communication* (London, Routledge 2020) 93.

57 GDPR (n 12) recital 7.

58 EDPB (n 29).

59 Pursuant to art 22 GDPR any 'data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling'.

60 Profiling is treated as 'individual' when personalised information about a single individual is aggregated, whereas the group profile will never analyse particular individuals but groups of persons with a common interest. In the same way, direct profiling takes place when data collected from a user is used to create a profile of that same subject; while indirect profiles will use data from several users to create a profile linked to a particular subject.

61 Carole Cadwalladr Carole and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian*, 17 March 2018 <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 6 August 2021.

profiling on Facebook by specifying a combination of criteria that match only one individual. In such a case, an ad campaign could single a person out and learn additional information about this person.[62] For instance, as for the Attribute-based Audiences tool, Korolova conducted an attack that allowed for targeting one single person by introducing a set of attributes that uniquely (or almost uniquely) identified the user among all Facebook users.[63] In the same way, for the PII Audiences tool, a user could be targeted individually on Facebook due to the very low threshold that the platform has for the Custom Audience size.[64] Facebook's threshold was easily surpassed by including users who were known to use AdBlock or were not active on Facebook in the Custom Audience specification.[65] Another way to achieve individual profiling on Facebook is by customizing the location and targeting a very small location (which could be as specific as a single house). Although the location targeting feature enforces a minimum 1-mile radius, a study showed that it was possible to combine 1-mile radius circles of what should be included and excluded from the targeting, enabling one to target a single household.[66]

These profiling practices could be considered excessive and thus contrary to the GDPR if there are no mechanisms in place for users to opt out or object to the processing used to create these individual profiles. Moreover, profiling should never be based on special categories of data without explicit consent.

Limited data protection by design and by default

According to Article 25 of the GDPR, personal data should not be made accessible to the controller without the individual's intervention. In other words, users should be able to decide on each platform what information they wish to make accessible to the data controller and what not. This is pursuant to the Data Protection by Design and by Default (hereinafter, 'DPbDD') principles.

Ten years ago, users did not have DPbDD options in their main social media platforms. Several studies during that period revealed that multiple pieces of users' personal information—such as name, city, zip code, email address, phone numbers, gender, birthday, age, employer, friends, activities, and interests—were either always available or available by default on most of the online social media sites.[67]

Today, social media privacy settings still do not directly let a user view or control which personal data is used for advertising.[68] In the case of Facebook, concerns have recently been raised regarding compliance with the DPbDD principles: a previous experiment has shown that even the information that an individual has shared on Facebook via the 'Friends Only'/'Only Me' designation can be obtained by anyone,[69] violating the principles of DPbDD. Another study proved that users' phone numbers could be disclosed to advertisers without the user being aware of it,[70] using the Custom Audience tool and de-anonymizing all the visitors that accessed a particular website.[71] Therefore, these events could not only infringe upon the DPbDD principles, but also would breach the purpose limitation principle and the adequacy of security measures in place.[72]

Options for opting out of PMT are not available on any of the main social media platforms, either. Similarly, users cannot opt out from receiving ads from political actors on social media. As seen in Figure 3 above, for PMT social media platforms automatically cluster users sharing common characteristics and directly target them with personalised political messages.

Therefore, more nuanced user-facing controls regarding political actors' advertising should be introduced,[73] allowing users to make the final decision as to whether they wish to be micro-targeted for political purposes or not. In fact, such measures could be foreseen in advance in a Data Protection Impact Assessment (DPIA). According to Article 35 GDPR, DPIAs are required when there is automated processing of data, processing on a large scale of special categories of data, and systematic monitoring of data. All of these criteria could take place in PMT activities, so detailing the risks

62 Korolova (n 46); Irfan Faizullabhoy and Aleksandra Korolova, 'Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions' (2018) *Computing Research Repository*, Workshop on Technology and Consumer Protection (ConPro), 4.

63 Korolova (n 46).

64 The threshold established by Facebook and Instagram is 20 users; whereas Google is 1000 users, Twitter is 500 users, and LinkedIn and Pinterest is 500 users, respectively. See Facebook Marketing API: Custom Audience. <https://developers.facebook.com/docs/marketing-api/reference/custom-audience> accessed 6 August 2021.

65 Faizullabhoy and Korolova (n 62) 3.

66 Ibid.

67 Balachander Krishnamurthy and Craig E Wills, 'On the Leakage of Personally Identifiable Information via Online Social Networks' (2009) *ACM SIGCOMM WOSN*, 2009; Balachander Krishnamurthy, Konstantin Naryshkin and Craig E Wills, 'Privacy Leakage vs. Protection Measures: The Growing Disconnect' (2011), *IEEE W2SP*.

68 Venkatadri (n 12) 229.

69 Faizullabhoy and Korolova (n 62) 3.

70 Venkatadri, 'Investigating Sources of PII' (n 12).

71 Venkatadri, 'Privacy Risks with Facebook's PII-based Targeting' (n 12).

72 See the section 'Compliance with other data protection principles' of the present study.

73 Ali and others (n 54) 14.

of PMT in a DPIA before any political campaign seems to be an adequate standard to put in place.

Conclusions

Today an immense amount of data is processed and analysed to craft tailored political messages to individual potential voters. Political actors rely on the large-scale collection and processing of personal data that is conducted by social media platforms and offered to advertisers for micro-targeting.

This article has examined the main GDPR provisions that are relevant to micro-targeting, especially when this technique is used by political actors in order to target potential voters. Political micro-targeting (PMT) may result in the violation of many individual rights connected to data protection if GDPR rules are not properly applied. In particular, this study has first concluded that PMT could result in a breach of the principle of lawfulness if data controllers responsible for data processing are not adequately identified, and if users are not provided with proper ways to grant prior consent. In addition, other data protection principles such as purpose limitation, data minimization and data accuracy have been critiqued, and found to be potentially unlawful in the case of PMT due to the current lack of mechanisms to supervise compliance with such rules. Finally, this study has evidenced how PMT could violate the GDPR provisions referring to profiling and DPbDD, unless users are provided with new options to control their data. Overall, this study has found that, currently, users are unable to exercise control over their data being used for PMT.

Therefore, in order to comply with the GDPR framework, new privacy techniques and tools need to be implemented by the ad platform so that PMT is done in a balanced and sensitive way, and in a manner that leads to outcomes that benefit everyone in the democratic ecosystem—users, ad platform designers, and political advertisers. Further restrictions on PMT must indeed be considered in light of the potential privileged position of PMT as a form of political communication under Article 10 ECHR, which covers politicians, political parties and platforms as well as users' right to receive information. As a result, propositions such as outright bans on PMT might be considered as inconsistent with freedom of expression in future case law. Moreover, at the EU level, platforms should be required to meet further transparency requirements in order to promote clarity with respect to PMT's scope and data use.

doi:10.1093/idpl/ipab018
Advance Access Publication 20 August 2021