re:constitution
Working Paper

Cristina Blasi Casagran

Analysing Political Micro-Targeting from a GDPR Perspective

working papers, Forum Transregionale Studien 4/2022

re:constitution - Exchange and Analysis on Democracy and the Rule of Law in Europe
c/o Forum Transregionale Studien e. V., Wallotstr. 14, 14193 Berlin

Cristina Blasi Casagran
Analysing Political Micro-Targeting from a GDPR Perspective
Working Papers, Forum Transregionale Studien 4/2022
DOI: https://doi.org/10.25360/01-2022-00052

Design: Plural | Severin Wucher

The Forum Transregionale Studien is an institutional platform for the international cooperation between scholars of different expertise and perspectives on global issues. It is funded by the Berlin Senate Department for Higher Education and Research, Health, Long-term Care and Gender Equality.

Working Papers are available in open access via *perspectivia.net*, the publication platform of the Max Weber Stiftung.

re:constitution - Exchange and Analysis on Democracy and the Rule of Law in Europe is a joint programme of the Forum Transregionale Studien and Democracy Reporting International, funded by Stiftung Mercator.

Abstract

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)? 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.

Keywords: Political micro-targeting, GDPR, political advertising, data protection, social media

Suggested Citation:

Blasi Casagran, Cristina, "Analysing Political Micro-Targeting from a GDPR Perspective", re:constitution Working Paper, Forum Transregionale Studien 4/2022, available at https://reconstitution.eu/working-papers.html

Analysing Political Micro-Targeting from a GDPR Perspective*

Cristina Blasi Casagran[1]

Introduction

The phenomenon of political micro-targeting (hereinafter, PMT) during political campaigns has recently emerged in the European Union (EU). 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, i.e., 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] Similarly, the concept of PMT could be defined as the same form of direct marketing, but in this case launched by political actors[4] who target individual voters with highly personalised messages using predictive modelling techniques to voter data.[5]

In the 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.[6] It also raises concerns due to the fact that PMT could be used to identify and target weak points where groups and individuals are most vulnerable to strategic influence.[7] 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. Likewise, we have lately witnessed events such as the Cambridge Analytica scandal,[8] Facebook being used in Myanmar to incite racial hatred fuelling racial genocide against the Rohingya,[9] and fake Black Lives Matter memes created in the US by the Russian Government to attract online Black communities to protest events against Hillary Clinton during the 2016 Presidential Election,[10] among others.[11] In fact, it was as a result of the

* This paper is an extract of an early version of the article: Cristina Blasi Casagran, Mathias Vermeulen, „Reflections on the murky legal practices of political micro-targeting from a GDPR perspective", *International Data Privacy Law*, 2021, ipab018, https://doi.org/10.1093/idpl/ipab018.

1 Cristina Blasi Casagran is assistant professor of public international law and international relations at Autonomous University of Barcelona. She is a 2020-2021 re:constitution Fellow. Email: cristina.blasi@uab.es

2 'Who targets me' <https://whotargets.me/en/definitions/> accessed 8 May 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 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.

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

6 Dobber (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.

7 Anthony Nadler, Matthew Crain, 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 8 May 2021.

8 Christopher Wylie, Mindf*ck. Cambridge Analytica and the Plot to Break America (Random House Books 2020).

9 Paul Mozur, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military' (The *New York Times*, 15 October 2018) <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html> accessed 8 May 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 8 May 2021.

11 Ibid., 7. Other relevant examples are described in Dipayan Ghosh and Ben Scott, 'Digital Deceit: The Technologies Behind Precision Propaganda on the Internet' (*New America Foundation*, 23 January 2018) <https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf> accessed 8 May 2021; Hamsini Sridharan and Ann Ravel, 'Illuminating Dark Digital Politics. Campaign Finance

experiences in the 2016 U.S. presidential elections that PMT began to receive increased attention from policy makers in the EU.

This paper seeks to explore one of the recent controversial EU debates related to PMT:[12] Is the practice of PMT compliant with the EU's General Data Protection Regulation (GDPR)?[13] It will examine the PMT's compliance with the main GDPR provisions. Particularly, the paper will assess: PMT compliance with the GDPR principles of lawful data processing; the existing concerns regarding excessive profiling through PMT; and the potential flaws in implementing the privacy-by-default and privacy-by design principles. The overall goal of this study is to flag the main issues of concern regarding PMT and to determine whether or not this practice aligns with the GDPR.

1. 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: (a) the data subject has given consent; (b) the processing is necessary for the performance of a contract; (c) the processing complies with a legal obligation to which the controller is subject; (d) the processing seeks to protect someone's vital interests; (e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) 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 principle. 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.

1.1. 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 various types of subjects, which could make it difficult to identify the actual data controllers and data processors. 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 subjects could qualify as data controllers of data processed during PMT: online platforms and political actors. Online platforms such as Facebook, Twitter or LinkedIn should be

Disclosure for the 21st Century' (*Maplight*, October 2017) <https://mymadison.io/documents/illuminating-dark-digital-politics> accessed 8 May; Jeff Chester and Kathryn C. Montgomery, 'The Role of Digital Marketing in Political Campaigns' (2017) 6 *Internet Policy Review* 4; and Emma L. Briant, 'Cambridge Analytica and SCL – How I Peered inside the Propaganda Machine' (*The Conversation*, 17 April 2018) <http://theconversation.com/cambridge-analytica-and-scl-how-i-peeredinside-the-propaganda-machine-94867> accessed 8 May 2021.

12 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 8 May 2021.

13 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').

considered the only data controllers if the ad is distributed via Attribute-based Audiences tool. Yet, the same conclusion does not seem to apply when the Personally Identifying Information Audiences (PII) tool[14] 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 this sense, 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.[15] Similarly, the Court of Justice of the EU (CJEU)[16] as well as national data protection authorities[17] 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 individual exercising influence over the processing of personal data can be considered a data controller, regardless of whether this person has issued written instructions to that effect.[18]

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 in 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.[19] The first sub-group would include core political advertisers, i.e., 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, i.e., actors which (a) either receive any form of compensation from core political advertisers to spread their messages or (b) speak on behalf of core political advertisers and their interests.

A full legal assessment of the usage of PMT by all of these actors is beyond the scope of this paper. 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.[20] In practice, political parties are given significant leeway to process personal data, and even special category data such as political beliefs or religion. Yet, that same leeway is not afforded to other political actors (e.g. political advertisers) and to online platforms - which in practice would need to rely on users' consent to process special category data.

14 This tool is referred to as 'Custom Audiences' and allows political actors to target their existing contacts on the ad-driven platform via multiple methods. See 'How to use Facebook custom audiences' <https://www.facebook.com/business/a/custom-audiences>accessed 6 August 2021.

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

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

17 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 9 May 2021.

18 Case C-25/17 Tietosuojavaltuutettu [2018] ECLI:EU:C:2018:551, para. 68.

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

20 GDPR (n.13), recital 56.

1.2. The Need for Valid Consent to Process Data for PMT

Given the lack of transparency surrounding social media ad delivery,[21] 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,[22] 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 Article 29 Working Party, a data subject should be able to determine in advance what the scope and consequences of the processing entails, and they should not be taken by surprise at a later point about the ways in which their personal data has been used.[23] This criterion is clearly not met with the ad delivery practices mentioned 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.[24] 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.[25]

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.[26] For the purpose of this study, the possibility to withdraw a user's consent from being micro-targeted on Facebook has been explored.[27] 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 (a) advertisers including the user in a list, (b) shops interacted with through the platform, (c) pages liked, and (d) 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,[28] PMT performed by any other actor than political parties should require 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-

21 Upturn, 'Leveling the Platform: Real Transparency for Paid Messages on Facebook', May 2018 <https://www.upturn.org/reports/2018/facebook-ads/> accessed 8 May 2021; Mathias Vermeulen, 'The Keys to the Kingdom. Overcoming GDPR-concerns to Unlock Access to Platform Data for Independent Researchers' (2020) *OSF Preprints*, 12-15. <https://ideas.repec.org/p/osf/osfxxx/vnswz.html> accessed 8 May 2021.

22 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 10 May 2021.

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

24 C-673/17 Planet49 GmbH [2019] ECLI:EU:C:2019:801, para. 61.

25 Ibid., para. 55.

26 GDPR (n.13), recital 42.

27 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.

28 GDPR (n.13), Article 9.

friend even when they were sharing their status in a 'Friends Only' visibility mode.[29] 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.[30] 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 consent from targeted 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.

2. 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 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. Personal data collected by social media platforms and then processed for political advertising are 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 minimisation 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. It would also require periodic reviews of the data, with deletion of those data items that are no longer necessary. Assessing whether PMT conforms with this principle is considerably complex. Micro-targeting as such 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,[31] 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 minimisation principle may be infringed due to the vast amount of data categories collected and put at the disposal of political actors. In fact, data items used for PMT could correspond to the very

29 Aleksandra Korolova, 'Privacy violations using microtargeted ads: A case study' (2011) 3 *Journal of Privacy and Confidentiality* 1, 35.

30 Kurt Thomas, Chris Grier and David M. Nicol, 'Unfriendly: Multi-party Privacy Risks in Social Networks' (2010) *PETS, Springer-Verlag*; 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.*

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

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 the right to the freedom of expression, enshrined in Article 10 of the European Convention on Human Rights (ECHR). It could be argued that PMT itself 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.[32]

In addition, a proper application of the transparency principle would lead to necessary reinforcement of the accuracy principle, too**.** Users should be able to check what data has been used to build their profiles for targeting by political actors, and they should 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 personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person) could be challenged by a user as in breach of the data accuracy principle.[33] However, social media platforms could always argue that the spotted inaccuracy is of a subjective nature,[34] as the same data item separated from the profile would not require any rectification at all.

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 no sufficient knowledge about the amount and type of data that are used for targeting, and there is no public accountability or scrutiny mechanisms on algorithms created by social media to deliver ads either.[35] Thus, there is 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.[36]

3. Profiling Concerns

While people's interactions with online social media services serve as inputs for the construction of personal profiles,[37] 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.

32 Dobber (n. 3), 8.
33 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.
34 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.
35 Muhammad Ali and others, 'Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging' (2019) *Cornell University*, 13.
36 IDEA (n. 31), 2.
37 Taina Bucher, '(Big) data and algorithms' in Leah A. Lievrouw, Brian D. Loader (eds.) *Routledge Handbook of Digital Media and Communication* (Routledge, 2020), 93.

According to the GDPR, 'profiling' consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person.[38] 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.[39] Such profiling practices need to be transparent and easily accessible, and the data is entitled to oppose them at any time.[40] Yet, PMT practices demonstrate that this is not always the case.

Political actors that are interested in targeting voters online, via social media, have two main sources of data: (1) profiles already created in their own registers; or (2) 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 of individuals as well, and it can be direct or indirect.[41] 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.[42]

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 Attribute-based Audiences tool,[43] 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 of the targeted users. The platform would only inform the advertiser about the number of matched records (i.e., the audience size). Likewise, if advertisers decide to use the PII Audiences tool instead, they would introduce one external piece of personal information. The platform would then link such data item to its own data, targeting group profiles with characteristics similar to the original piece of information.

38 GDPR (n. 13), recital 7.

39 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 9 May 2021.

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

41 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.

42 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 11 May 2021.

43 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.

Although these two Facebook tools are designed to provide only group profiles, previous studies have demonstrated that it is possible to achieve individual profiling on Facebook by specifying a combination of criteria that match only with one individual. In such a case, an ad campaigner could single a person out and learn additional information about this person.[44] 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.[45] 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.[46] 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.[47] Another way to achieve individual profiling on Facebook is customising 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.[48]

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 from those individual profiles. Moreover, profiling should never be based on special categories of data without explicit consent.

4. 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 in 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 had revealed that multiple pieces of users' personal information —such as the 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.[49]

Today, social media privacy settings still do not directly let a user view or control which personal data is used for advertising.[50] 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,[51]

44 Korolova (n. 29); 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.

45 Korolova (n. 29).

46 The threshold established by Facebook and Instagram is 20 users; whereas Google is 1,000 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 11 May 2021.

47 Faizullabhoy & Korolova (n. 44), 3.

48 Ibid.

49 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*.

50 Giridhari Venkatadri and others, 'Investigating sources of PII used in Facebook's targeted advertising' (2019) *Proceedings on Privacy Enhancing Technologies* 1, 229.

51 Faizullabhoy & Korolova (n. 44), 3.

violating the principles of DPbDD. Another study proved that users' phone numbers could be disclosed to advertisers without the user being aware of it,[52] using the Custom Audience tool and de-anonymising all the visitors that accessed a particular website.[53] Therefore, these events could not only infringe upon the DPbDD principles, but they would also breach the purpose limitation principle and the requirement for adequate security measures.

Opting out of PMT is not available on any of the main social media platforms, either. Similarly, users cannot opt out from receiving ads by political actors on social media. 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,[54] allowing users to make the final decision as to whether they wish to be micro-targeted for political purposes or not.

Conclusion

Today an immense amount of data is being processed and analysed to craft tailored political messages to each potential voter. 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 paper has examined the most relevant GDPR provisions related to micro-targeting, especially when this technique is used by political actors to target potential voters. The study has concluded that political micro-targeting (PMT) may likely result in the violation of many individual rights when GDPR rules are not properly applied. In particular, this study has firstly 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 their prior consent. In addition, other data protection principles such as purpose limitation, data minimisation and data accuracy have been criticized, 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, in case of PMT, users are unable to exercise control over their data.

Therefore, in order to comply with the GDPR framework, new privacy techniques and tools need to be implemented by the ad platform services. PMT shall be conducted in a balanced and sensitive way, and in a manner that is beneficial for everyone in the democratic ecosystem —users, ad platform designers, and political advertisers. 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.

52 Venkatadri 2019 (n. 50).

53 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.

54 Ali (n. 35) 14.

Forum Transregionale Studien e.V.
Wallotstraße 14
14193 Berlin
T: +49 (0) 30 89001-430
office@trafo-berlin.de
www.forum-transregionale-studien.de