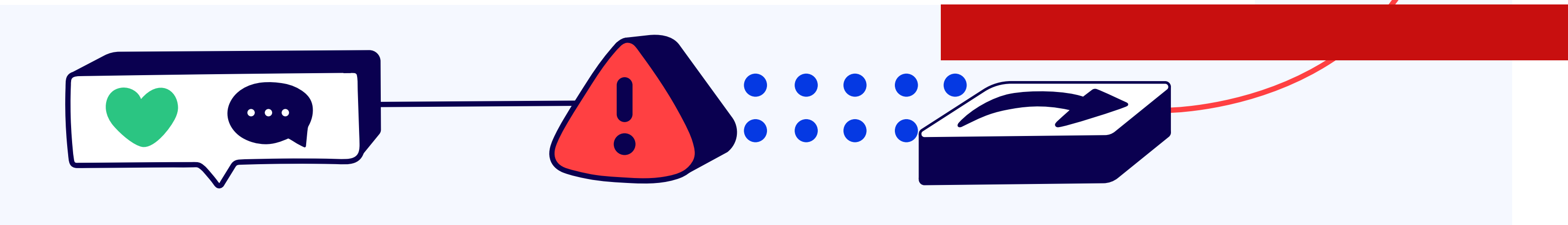
Mitigating the Risks of Political Microtargeting

Guidance for Policymakers, Civil Society, and Development Cooperation



Published by:

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Address
Sector Program International Digital Policy for Sustainable Development
Friedrich-Ebert-Allee 32+36, 53113 Bonn, Deutschland
T +49 2 28 44 60-0
F +49 2 28 44 60-17 66

E info@giz.de
I www.giz.de/en

Project:
Sector Project International Digital Policy for Sustainable Development

Authors:
Jacob Kröger, Emilia Errenst, Niklas Nau, Sanna Ojanperä

Design:
Studio GOOD, Berlin

Illustration:
Tara Monheim

About this report:
This report was produced by an international working group, led by Emilia Errenst and Jacob Kröger from the German Agency for International Cooperation (GIZ). The working group consisted of organizations specialized in democracy promotion, digital rights, platform regulation, fighting mis- and disinformation, and data protection, including organizations with expertise in tracking and investigating digital political campaigning.
The working group collaboratively developed this report as part of the "Year of Action" of the US Summit for Democracy (S4D), a flagship presidential initiative of the Biden-Harris administration for strengthening democracies worldwide in the face of growing dangers created by division and polarization, authoritarian tendencies and new technologies. The working group was convened in the context of the S4D Cohort on Information Integrity, hosted by Canada, Latvia, and the Alliance for Securing Democracy.

Acknowledgements:
We would like to thank all organisations that have participated in our working group and the hosts of the S4D Cohort on Information Integrity (Canada, Latvia, and the Alliance for Securing Democracy) for making this endeavor possible. We also thank Tessa Lennemann, Melanie Döring, Livia Hartmann, Anke Schlieker, Cindy Zheng, Antoine Paul, and Marielle Findorff for their valuable support in creating this report.

Supported by:
German Federal Ministry for Economic Cooperation and Development (BMZ)
Divison Governance, Bonn

Bonn, 2024

Supported by:

Federal Ministry
for Economic Cooperation
and Development

We express our sincere appreciation to the co-signatories of this report whose dedication and active involvement have been instrumental in its creation. Their profound commitment and expertise have enriched our collective effort to better understand—and help mitigate—the risks of data-driven political campaigning in the digital age.

African Internet Rights Alliance (AIRA)

ANDI - Communication and Rights
ANDI Comunicação e Direitos

Code4Africa +
African Digital Democracy Observatory (ADDO)

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

Digital Equity Association

Global Project Against Hate and Extremism (GPAHE)

Media Monitoring Africa (MMA)

Fundación Multitudes

PolicyLab Africa

The Latin American and Caribbean Network for Democracy (REDLAD)
Red Latinoamericana y del Caribe para la Democracia

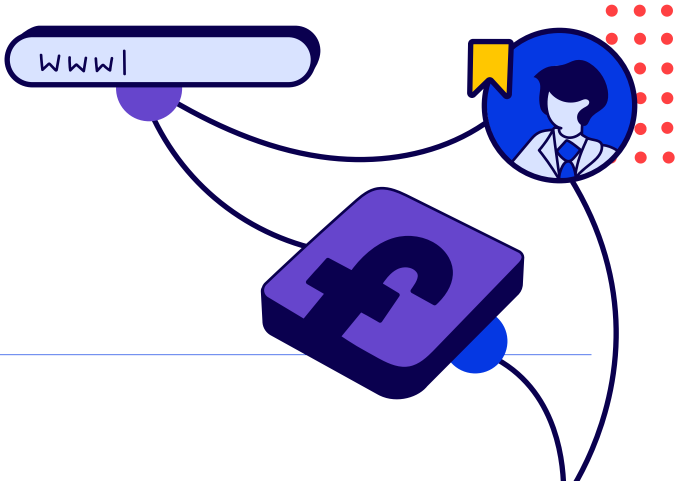
Siasa Place (SP)

Stiftung Neue Verantwortung e. V. (SNV), Dr. Julian Jaursch

Tactical Tech

Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA)

Table of Contents



Executive summary

Digital technology has revolutionized how political ads are delivered and consumed, giving political campaigns increased possibilities to target and tailor their messaging to specific audiences—a practice known as political microtargeting (PMT). While PMT has potential benefits for society, it also entails significant risks that have yet to be adequately addressed by regulators around the globe. This report offers fundamental guidance on PMT for policymakers, civil society, and other relevant stakeholders, providing recommendations for action and an overview of possible protective measures.

Public discourse has so far mostly focused on PMT cases in the Global North,[i] such as US elections or Brexit, whereas the practice is becoming increasingly adopted worldwide. In lower-income countries, the impact of PMT may be felt even more strongly due to context-specific factors such as lower levels of digital skills and media literacy, higher prevalence of political violence, weaker or non-existent legal and regulatory frameworks, and less resilient democratic institutions. This report contributes to balancing the global coverage by focusing on cases and examples from the Global South. Recent advances in artificial intelligence (AI) have added to the urgency of investigating PMT, as they amplify the capabilities of targeted messaging and intensify the risk of online disinformation though automated generation and manipulation of content.

What is political microtargeting? (Chapter 2)

The term political microtargeting (PMT) is often used to describe political messages that are strategically placed and tailored to appeal to specific individuals or groups by using personal data, but the phenomenon lacks a widely accepted definition. A nascent body of literature aims to describe central characteristics of PMT and map its various and evolving technical applications. Despite the significant interest and investment into PMT, its persuasive effects remain debatable, although PMT ads that are congruent with the preference and personality of the target individual have been found to positively affect the target's attitudes and voting intentions. The fairly recent emergence of PMT (the 2008 Obama presidential campaign is often referred to as its first appearance) explains why it is rarely included in the remit of national regulatory bodies, resulting in the activities related to PMT to go largely unchecked. Much is at stake to define PMT in a way that strikes the right balance between capturing enough political activity without being too cumbersome to implement or infringing on the right to free speech.

Promises and risks of political microtargeting (Chapter 3)

The evidence gathered to date suggests that PMT both offers potential benefits and poses a range of risks. Among the chief potential benefits of PMT are an increased informational value of political communication through (1) **ad relevance and diversification of content,** (2) **efficiency of campaign activity,** and (3) **ability to reach and activate specific population segments.** Better functioning political communication could in turn activate voters to become more interested in politics and participate in democratic processes. While these promises of PMT often surface in popular discourse, they are partially based on unrealistic assumptions and are only supported by limited scientific evidence.

PMT is also associated with manifold risks. Chief among them are (1) **voter manipulation and demobilization,** (2) **lack of transparency,** (3) **spread of disinformation,** (4) **unfair competition between political actors,** (5) **foreign influence into domestic affairs,** (6) **privacy violations,** (7) **difficulty of public scrutiny and counter speech,** (8) **distortion of voter model and political mandates,** (9) **discrimination,** and (10) **political polarization.** On an individual level, these risks may result in a violation of human autonomy and dignity. On the collective, societal level, the use of PMT may pose a threat to social cohesion, national sovereignty, fair and

[i] We are aware of the problematic nature of the terms *Global North* and *Global South* as well as the related dichotomy of *developed countries* and *developing countries*. However, given that much of the envisioned readership of this report are using the terms *Global South* and *Global North* in their work, we decided to employ them in this report in order to help the discoverability of our work. However, we would like to urge readers to make themselves familiar with the problematic nature of these terms and join us in actively seeking suitable substitutes. For anyone interested in further perspectives on this topic, we recommend the work of Kloß,[13] Hachani,[14] and Sud & Sánchez-Ancochea.[15]

informed public discourse, and the principle of free and fair elections, thus potentially undermining the foundations of democracy.

PMT cases in the Global South (Chapter 4)

Most of the literature on PMT draws from experiments and case studies in the Global North. Examples from the Global South have not yet received much coverage in the media and in international political forums. Therefore, Chapter 4 of this report presents brief reviews of PMT applications in Africa (Kenya, Nigeria), South & Southeast Asia (Philippines, India), and South America (Chile, Brazil, and Colombia). The examples illustrate that PMT is prevalent across all seven examined countries and is applied through diverse methods, including ethically questionable practices and illegal forms of data collection. Fairly short experiences with democratic regimes, widespread corruption, and nascent legal and policy frameworks governing the collection and use of personal data are challenges that appear repeatedly in the examined cases. The social media platforms and instant messengers used for the examined applications of PMT are mostly operated by Meta (including Facebook and WhatsApp) and X (formerly Twitter). TikTok had not yet attained the current level of prominence and political relevance in the country cases under consideration. As the platform has seen rapid growth over the last years and is increasingly being used by political actors, future investigations should also examine TikTok as a potential channel for PMT.

Context-specific factors (Chapter 5)

Efforts to investigate the role of PMT and any plans for regulation should consider certain context- and country-specific factors that may influence the impacts of PMT. In an attempt to understand which drivers influence the information environment around elections, we outlined five factors that are particularly relevant for low- and middle-income countries (LMICs):

1) **General education, digital skills, and critical media literacy** are crucial to be able to identify, interpret, and reflect on advertising content such as PMT. Where these skills are missing, it is challenging to distinguish between true, false, and deliberately misleading information.
2) **Societal cleavages, inequalities, and polarization** may be aggravated by the use of PMT. Existing tensions and violent conflict stemming from political divisions drawn across ethnic, cultural, or religious lines are particular risk factors for enhanced harmful effects of PMT.
3) **Connectivity** is rapidly rising in many countries and may result in large populations with minimal previous experience with digital technologies being exposed to PMT. On the other hand, improved connectivity can enable better access to fact-checking services and a diverse range of media, thus providing opportunities to exercise critical media literacy and scrutinize deceptive PMT campaigns.
4) **Legal and regulatory frameworks** largely shape how the potentially harmful effects of PMT can unfold. While there are major regulatory developments, for instance in the European Union, in many countries there is little to no regulation in place to govern data-driven political campaigning.
5) **Strength and resilience of democratic institutions** are key in determining the impact that PMT can deliver. Where democratic institutions are weak and media freedom is not guaranteed, accountability and independent oversight may be compromised, making a country vulnerable to misuse of PMT.

Regulating PMT (Chapter 6)

While most countries still have no comprehensive legislation in place to address PMT, efforts to regulate and legislate around the phenomenon are quickly emerging around the world. In order to define the material scope of any regulation on PMT, one fundamental question is how to legally define “political advertisement”. This is a delicate task, as all approaches have advantages and downsides (e.g., complexity in implementation, potential loopholes, level of subjectivity, adaptability to evolving technological landscape). Approaches to regulating PMT encompass a variety of options, including: (1) **rules for shaping PMT,** (2) **transparency obligations,** (3) **user control / consent,** (4) **partial restrictions or total bans.** Each approach has a range of implementation options as well as benefits and shortcomings which are discussed in detail.

Recommendations (Chapter 7)

We call on state and non-state actors around the world to devote attention to PMT and its impacts in their local contexts. Based on our research for this report, we have developed a set of recommendations that are specified for three groups of stakeholders: governments and political actors; users; and actors engaged in development cooperation.

Recommendations for governments and political actors

1. Make concrete efforts to regulate PMT
   1.1 *Set strong transparency obligations as a minimum requirement*
   1.2. *Adopt preliminary protective measures where suitable regulation of PMT is not in place*
   1.3. *Follow a multi-stakeholder approach in regulatory development*

   1.4. *Recognize the limitations of relying on transparency, industry self-regulation, and consumer education*
   1.5. *Account for local and contextual factors*
   1.6. *Monitor and reflect the advances in persuasive technologies*
   1.7. *Protect national sovereignty from foreign influence via PMT*
   1.8. *Carefully weigh the threats to free speech posed by a more stringent regulation of political ads*

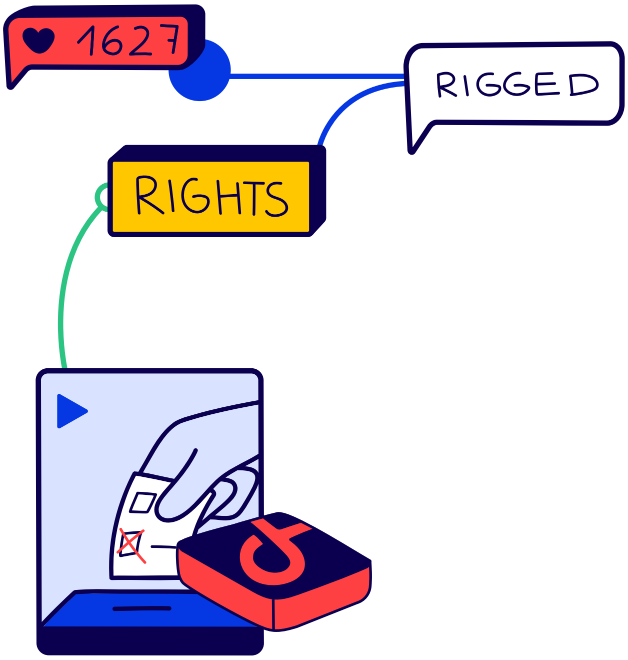
2. Oblige online platforms to allocate sufficient resources and personnel to content moderation
3. Act collectively or collaborate with other countries in devising PMT regulation and other strategies to manage its harmful impacts
4. Refrain from spreading false or misleading information
5. Bolster democratic resilience
   5.1. *Build public awareness of PMT*
   5.2. *Nurture public interest research on PMT and disinformation and support related public discourse*
   5.3. *Nurture media pluralism*
   5.4. *Develop and support capacity for fact-checking*

Recommendations for users

1. Protect your privacy
2. Block ads
3. Become an aware and critical consumer of information
   3.1. *Be vigilant when examining political messages*
   3.2. *Share information responsibly*
   3.3. *Use the information platforms give you*
   3.4. *Cross-check information by comparing alternative reliable sources*
   3.5. *Reflect on your personal biases—and look out for confirmation bias*
   3.6. *Report inappropriate political content*
   3.7. *Help others to navigate PMT and direct them towards trustworthy information*
   3.8. *Stay informed about political issues and the views of the electorate*
   3.9. *Review your information diet and expose yourself to opposing views*

Recommendations for development cooperation

1. Support capacity-building for informed policymaking
2. Strengthen the development of digital skills and critical media literacy
3. Facilitate research into digital political communication and foster civil society activity around the topic
4. Support representation and participation of Global South actors in relevant international networks, forums, and decision-making bodies



1 Introduction

Political advertising is an integral part of modern democratic discourse. It is a powerful tool that plays a pivotal role in shaping public opinion, mobilizing voters, and ultimately influencing the outcomes of elections. Over the last two decades, digital technology has brought about a revolutionary shift in how advertising is crafted, disseminated, and consumed, fundamentally altering the landscape of political communication. Among other things, technological advances have created new possibilities to target and tailor ads to specific groups or individuals. In the realm of political advertising, this approach is referred to as political microtargeting (PMT). It can include a broad range of methods and technologies.

The 2008 US presidential election marked a watershed moment in the advent of PMT, described by some observers as a "data war"[1] with social media platforms such as Facebook referred to as "election weapon[s]".[2] Recognizing the untapped potential of voter data, Barack Obama's campaign employed sophisticated analytics and targeting techniques to personalize its message and engage with voters on a granular level. Obama's chances appeared slim already during the 2008 primary campaign, as former First Lady Hillary Clinton enjoyed greater name recognition, deeper party connections, and a wealth of experience. However, harnessing the immense reach and influence of Facebook and Twitter and leveraging personal data from various sources, Obama's team managed to build a winning campaign, reaching out to specific voter segments with messages that resonated on an individual level.[3]

This pioneering approach set the stage for an era of data-driven strategies that continue to shape the landscape of political advertising today. The global PMT ecosystem has grown into a thriving "influence industry" which some estimate to number over 500 companies, including technology service providers, political strategists, data brokers, and platforms.[4] Organizations in this ecosystem often hold thousands of data points on individual voters.[5]

At best, PMT promises increased ad relevance and diversification of ad content, improved campaign efficiency, and new ways of connecting with population segments that are otherwise hard to reach. Thus, targeted political ads can be an opportunity for strengthening pluralism and voter engagement. On the other hand, however, PMT also carries a multitude of significant risks that range from voter manipulation and foreign election interference to discrimination and privacy violations. As PMT is often used to highlight topics based on individual voter preference rather than actual party priorities, it can lead to a distortion and polarization of public political debate and the creation of online echo chambers where prejudices are reinforced. The selective delivery of targeted political ads generally subverts the scrutiny of traditional democratic watchdogs who hold actors publicly accountable for political messaging, making PMT a convenient tool for spreading disinformation. Further criticism notes that political parties with large advertising budgets sometimes receive special services and privileged access to internal knowledge of online platforms and advertising networks.[6,7] According to several reports, employees of tech companies, such as Google, have worked inside political campaigns, "sometimes indistinguishable from campaign hands."[7] Ultimately, PMT can lead to unfair competition between political actors, distort political mandates, and threaten the integrity of elections. In extreme cases, online manipulation campaigns may even contribute to inflaming violence and armed conflicts.[8,9]

The risks of PMT first received widespread public attention worldwide in 2018, when a whistleblower exposed that the consulting firm Cambridge Analytica had exploited personal data from millions of Facebook users for political advertising and manipulation purposes. Undecided voters were presented with ads tailored to "target their inner demons", as described by whistleblower Christopher Wylie.[10] There are concerns that these illegitimate methods had an impact on Donald Trump's victory in the 2016 US presidential election. In a famous hidden-camera exposé, Cambridge Analytica executives were recorded boasting of their role in Trump's win and describing the stealthy methods used in the process.[11] Wylie, the former employee-turned-whistleblower, also believes that the UK would not have voted for Brexit without Cambridge Analytica's intervention.[12] Other industry insiders joined in on the criticism, with former elections integrity head at Facebook, Yael Eisenstat, stating that the social media platform earns "profit by manipulating us [and] can't avoid damaging democracy."[13] While Facebook has faced investigations and Cambridge Analytica went bankrupt in the aftermath of the 2018 revelations, given the industry's scale, it is likely that the scandal was only the tip of the iceberg.

PMT has gained public awareness primarily through investigative journalism, much of which has focused on the Global North, e.g., on the cases from the US and UK mentioned above. However, PMT techniques are applied globally and have also been used in attempts to skew election outcomes and destabilize political systems across the Global South.

PMT techniques are applied globally and have also been used in attempts to skew election outcomes and destabilize political systems across the Global South.

Cambridge Analytica's parent company, SCL Elections, for instance, has been active in many countries across Africa, Southeast Asia, and Latin America, including Gabon, Guyana, Indonesia, Mauritius, Nepal, Pakistan, Thailand, Uruguay, and Zambia.[14] PMT-related scandals and problems have also been reported in Brazil, Chile, Colombia, India, Nigeria, the Philippines, and Kenya,[ii] to name a few. According to a 2022 research report, online manipulation campaigns on X (formerly Twitter) have predominantly targeted non-English-speaking audiences, and 20 of the top 25 target territories of information manipulation on Facebook and Instagram were countries in the Global South.[15]

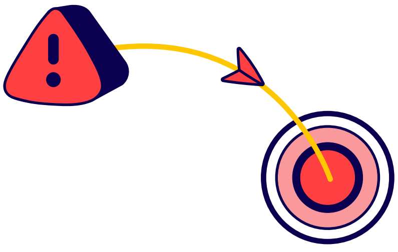
The impacts and risks of PMT are influenced by contextual factors such as local levels of media literacy, data protection standards, and the strength of democratic institutions. At the same time, technological advances, such as the rise of generative AI, offer potential for abuse in the context of political campaigning and may significantly impact the risks and benefits of PMT in the near-term future.[16] Addressing the complexities associated with PMT and implementing appropriate regulations presents a formidable task, especially for lower-income countries, which face unique challenges due to institutional and resource constraints. In some countries, significant segments of the population encountering PMT have only recently been introduced to digital technologies and thus have limited prior experience with the online environment. Furthermore, many countries in the Global South have a long history of religious or ethnical conflicts and election-related violence, which can be further aggravated by the polarizing impacts of PMT.

Addressing the complexities associated with PMT and implementing appropriate regulations presents a formidable task, especially for lower-income countries, which face unique challenges due to institutional and resource constraints.

With global Internet usage rapidly rising, especially in the Global South,[17] the prevalence of PMT will also continue to grow. According to the Reuters Institute Digital News Report 2023, audiences in Africa are most worried about misinformation worldwide, with 77% of the African population "concerned about what is real and what is fake on the Internet" compared to a global average of 56%.[18] Already in 2018, an article published by the MaxPlanckResearch magazine identified "[u]nregulated micro-targeting in elections" as a key factor contributing to the decline of democracy in Africa.[19]

A variety of reports and research articles has been published on the issue of political microtargeting. However, aside from a few notable examples,[iii] there is still a significant gap in the literature when it comes to exploring the prevalence and impacts of PMT in the Global South. This report contributes to addressing this gap.

The report will first introduce the reader to the topic of PMT and the existing evidence about its effects in Chapter 2. Chapter 3 will then discuss the potential benefits and risks of PMT. Country cases from Africa, South & Southeast Asia, and South America are presented in Chapter 4, while Chapter 5 discusses context-specific factors that can influence the impacts of PMT.. Chapter 6 outlines the regulatory environment for PMT and reviews a range of potential regulatory approaches, discussing their advantages and shortcomings. Chapter 7 presents a set of recommendations which are formulated towards three groups of stakeholders: governments and political actors, users, and actors engaged in development cooperation. Chapter 8 provides an outlook on possible advances in persuasive technologies that may impact PMT practices in the near-term future. Lastly, the Conclusion briefly summarizes the report's scope and achievements.



[ii] See Chapter 4

[iii] Notable examples include Tactical Tech's "Our Data Our Selves" project,[20] and reports and research articles on the use of PMT in individual countries, such as the 2022 report by Kitili et al,[21] the 2021 article by Mude,[22] and the 2019 report by Ong et al.[23]

References

1. Ambinder, M. (2009, October 5). Exclusive: How Democrats Won The Data War In 2008. The Atlantic. https://www.theatlantic.com/politics/archive/2009/10/exclusive-how-democrats-won-the-data-war-in-2008/27647/
2. Urbain, T. (2018). Facebook as an election weapon, from Obama to Trump. https://phys.org/news/2018-03-facebook-election-weapon-obama-trump.html
3. Issenberg, S. (2012). How Obama's Team Used Big Data to Rally Voters. MIT Technology Review. https://www.technologyreview.com/2012/12/19/114510/how-obamas-team-used-big-data-to-rally-voters/
4. Tactical Tech. (2022). The Influence Industry Explorer: A new online tool to explore 500 companies enabling political influence worldwide. https://tacticaltech.org/news/the-influence-industry-explorer/
5. Fowler, G. A. (2021). How politicians target you: 3,000 data points on every voter, including your phone number. Washington Post. https://www.washingtonpost.com/technology/2020/10/27/political-campaign-data-targeting/
6. Rennó, R. (2019). Search Result Influence: Reaching voters seeking answers. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/search-influence/
7. Campaign for Accountability. (2018). Partisan Programming: How Facebook and Google's Campaign Embeds Benefit Their Bottom Lines. https://campaignforaccountability.org/work/partisan-programming-how-facebook-and-googles-campaign-embeds-benefit-their-bottom-lines/
8. Miller, C. (2020). This Small Town Rioted Because Of Fake News And Rumors About The Coronavirus. BuzzFeed News. https://www.buzzfeednews.com/article/christopherm51/coronavirus-riots-social-media-ukraine
9. Aljazeera. (2022). Meta sued for $2bn over Facebook posts 'rousing hate' in Ethiopia. https://www.aljazeera.com/news/2022/12/14/meta-sued-for-2bn-over-facebook-posts-rousing-hate-in-ethiopia
10. Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
11. Neuman, S. (2018). In Hidden-Camera Exposé, Cambridge Analytica Executives Boast Of Role In Trump Win. NPR. https://www.npr.org/sections/thetwo-way/2018/03/21/595470164/in-hidden-camera-expose-cambridge-analytica-executives-boast-of-role-in-trump-wi
12. Martin, D. (2018). What role did Cambridge Analytica play in the Brexit vote? Deutsche Welle. https://www.dw.com/en/what-role-did-cambridge-analytica-play-in-the-brexit-vote/a-43151460
13. Eisenstat, Y. (2019). I worked on political ads at Facebook. They profit by manipulating us. Washington Post. https://www.washingtonpost.com/outlook/2019/11/04/i-worked-political-ads-facebook-they-profit-by-manipulating-us/
14. Ghoshal, D. (2018). Mapped: The breathtaking global reach of Cambridge Analytica's parent company. Quartz. https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/
15. Bailey, H., & Howard, P. N. (2022). The Instigators and Targets of Organised Social Media Manipulation: Global Index 2022. Oxford Internet Institute, University of Oxford. https://hannahlsbailey.github.io/docs/demtech_hannahbailey_memo.pdf
16. Simchon, A., Edwards, M., & Lewandowsky, S. (2023). The persuasive effects of political microtargeting in the age of generative AI [Preprint]. PsyArXiv. https://doi.org/10.31234/osf.io/62kxq
17. International Telecommunication Union. 2023. Share of the population using the Internet. Our World in Data. https://ourworldindata.org/grapher/share-of-individuals-using-the-internet
18. Reuters Institute. (2023). Digital News Report 2023. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf
19. Gadjanova, E. (2018). Democracy in decline in Africa. MaxPlanckResearch - Digital Society. https://www.mpg.de/12605295/W001_Viewpoint_012-017.pdf
20. Tactical Tech. (n.d.). Our Data Our Selves. Retrieved July 24, 2023, from https://ourdataourselves.tacticaltech.org/
21. Kitili, J., Theuri, G., & Badbess, K. (2022). Contextualising Political Advertising Policy to Political Micro-Targeting in Kenyan Elections. Center of Intellectual Property and Technology Law (CIPIT). https://cipit.org/wp-content/uploads/2023/03/Political-Advertising_compressed.pdf
22. Mude, H. (2021). Political Micro-Targeting in Kenya: An Analysis of the Legality of Data-Driven Campaign Strategies under the Data Protection Act. Journal of Intellectual Property and Information Technology Law (JIPIT). https://journal.strathmore.edu/index.php/jipit/article/view/61
23. Ong, J., Tapsell, R., & Curato, N. (2019). Tracking Digital Disinformation in the 2019 Philippine Midterm Election. New Mandala. https://www.newmandala.org/wp-content/uploads/2019/08/Digital-Disinformation-2019-Midterms.pdf

2 What is political microtargeting (PMT)

Political microtargeting (PMT), sometimes also referred to as data-driven campaigning, is a term frequently used to describe strategically placed and tailored political messages. Some prominent examples of PMT include ads that political actors fund, to appear for users on platforms such as Facebook, X, or LinkedIn or on search engines such as Google. Given that many of these activities have emerged and started to be adopted fairly recently, most of them are not in the remit of national regulatory bodies thus resulting in a definitional vacuum. Reflecting this complexity, no single universally accepted definition of PMT exists. Rather, actors who utilize or are affected by PMT tend to construct the concept from their viewpoint, leading to a multitude of definitions. Further, while the conceptual border around PMT is clear for some activities, it is much blurrier for others.[1] For instance, whereas a running political candidate paying for an ad to appear on the Facebook feed of a target voter presents a clear case of PMT, it is much less obvious whether an NGO communicating around a cause outside of an electoral period would constitute PMT.

Political microtargeting (PMT), sometimes also referred to as data-driven campaigning, is a term frequently used to describe strategically placed and tailored political messages.

The absence of a shared definition for PMT has prompted a nascent body of literature aiming to understand and analyze the phenomenon. While these contributions have not agreed on a single definition, they propose certain central characteristics of PMT. Jaursch describes PMT as targeting individuals with a goal to shape their opinions on political candidates, policies, ideas, and issues of public concern[1] while Papkyriakopoulos et al. highlight that such influence is achieved by presenting the individuals with stimuli that are derived through a consideration of the characteristics and preferences of the targeted individual.[2] Zuiderveen Borgesius et al. note PMT to consist of three main steps:

1) Collection of personal data about involved data subjects;
2) Use of the collected data to determine groups of data subjects who are susceptible to a certain political message; and
3) Sending the identified groups tailored messages through online avenues.[3]

An additional step includes analyzing the success and effectiveness of the sent messages, which in turn is used to optimize future targeting efforts.[4] A central tenet of all forms of PMT is the collection and use of personal data in order to formulate and send political messages to targets and exert political influence.[5] There is a growing interest in PMT and significant variation in the types of PMT content produced as well as the media spaces where it is deployed. The kind of data used for PMT, the statistical methods used to derive insights from the data, and the technical applications of PMT continue to evolve.

While this report focuses on PMT taking place online, similar practices take place offline, as robo calls, addressable TV, direct mail, and door-to-door canvassing are all increasingly data-driven and targeted. Despite not benefiting from the scale and efficiency of the online environment, targeted political ads deployed offline share many of the underpinning principles and risks of their digital counterparts. While PMT typically operates based on personal data collected online, in some cases the data can also be gathered offline.

Much is at stake to define PMT in a way that strikes the right balance between capturing enough political activity without being too cumbersome to implement. There are real risks of defining PMT too narrowly or excessively broadly: Whereas a too narrow definition may permit certain kinds of harmful PMT to be exercised without oversight, an overly broad definition including too many activities that may not be harmful might prove impossible to monitor. Chapter 6 of this report will discuss legal aspects concerning the definition of PMT.

2.1 Direct effects of PMT

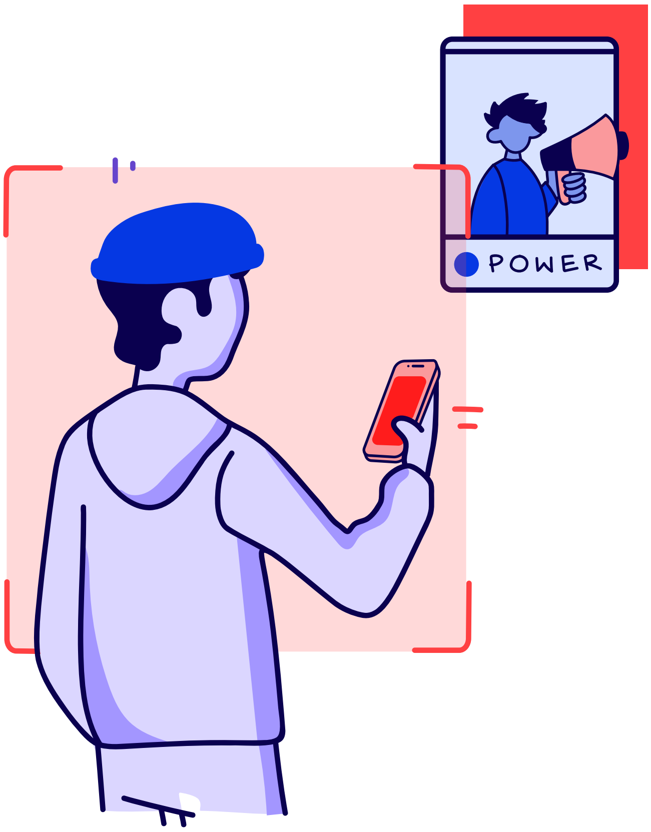
Despite the significant and growing interest and investment into PMT deployed through social media, its persuasive effects remain ambiguous. Experimental studies have started to investigate the phenomenon and have found no or negligible evidence for several effects of PMT, such as Facebook and Instagram ads on voter turnout,[6] the vote share for the US democratic party,[7,8] and candidate name identification or favourability.[9,10]

While these studies were carried out in the US, a modest impact was detected on vote share in Germany.[11,12] Instances where the targeted individual recognized being subject to PMT were found to lead to lower engagement in electronic word of mouth and to reduced perceived trustworthiness of the source of the PMT post.[13]

Direct effects of PMT on voters have been recorded in some instances where the ad is congruent with the personality or preferences of the targeted individual or in instances where the ad concerns a congruent issue (the issue stance of the target aligns with the political entity delivering the ad). PMT ads that are congruent with the preferences and personality of the target individual have been found to positively affect the target's attitudes and voting intentions toward political candidates,[14] political parties[15] and in terms of reinforcing party ties.[16] PMT ads including an issue that is congruent with the target's stance have been studied among cross-pressured partisan populations, where the partisan targets don't agree with the view of their own party's candidate but agree with the opposing party's candidate's stance on the issue. The study found that in this context, issue congruent PMT increased support for the candidate sending the message within the voters of the opposing party, increased abstention, and reduced the message recipient's support for their own party's candidate.[17]

The research investigating the effects of PMT seems to offer inconclusive findings. Crucially, detangling the effects of PMT is a challenging topic in research. PMT takes many forms and is used to target various demographic groups in diverse political and geographic contexts, but most of the PMT research is carried out in the US, or in Western countries and on a handful of social media platforms potentially limiting the external validity of these findings. Data is not easily accessible for research purposes, as it is held by various actors involved in the design and deployment of PMT, ranging from political entities to media platforms, and intermediary companies offering PMT services. The construction of adequate research designs to study causality in the context of potentially brief exposure to a political ad or a post in social media is difficult, and many of the methodological challenges related to wider research on political advertising beyond digital marketing apply (sample selection bias, confounding variables in observational studies, exaggerated compliance, experimenter effects, and unmeasured decay in experimental studies to mention a few).[7]

While a consensus on the persuasive effects of PMT is yet to emerge, the conflicting evidence and the well-acknowledged methodological challenges merit further attention. The political actors ramping up their investment into PMT certainly seem to expect it to deliver value for their money. There are many reasons why further research and policy attention on PMT is needed. As the developments over the last decade showcase, PMT is playing an increasing role in political communication around the world (the growing use of PMT in the Global South is discussed in more detail in Chapter 6), but many questions about its effects remain unanswered. The increasing technological capacities to profile citizens, target them, and automatically hone the ad content make PMT a fast-evolving set of practices. These reasons together with the widespread lack of regulation and the plethora of risks associated with PMT, which will be discussed in the following chapter, warrant policy action to address the phenomenon.



References

1. Jaursch, J. (2020). Defining Online Political Advertising. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/en/publication/defining-online-political-advertising
2. Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. C. M. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. Big Data & Society, 5(2), 2053951718811844. https://doi.org/10.1177/2053951718811844
3. Zuiderveen Borgesius, F. J. et al. (2018). Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, 14(1), 82–96. https://doi.org/10.18352/ulr.420
4. Baldwin-Philippi, J. (2017). The Myths of Data-Driven Campaigning. Political Communication, 34(4), 627–633. https://doi.org/10.1080/10584609.2017.1372999
5. Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R., & Wright, G. (2019). Personal Data: Political Persuasion Inside the Influence Industry. How it works. Tactical Tech. https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf
6. Collins, K., Kalla, J., & Keane, L. (2021). Youth Voter Mobilization Through Online Advertising: Evidence From Two GOTV Field Experiments. OSF Preprints. https://doi.org/10.31219/osf.io/6c9na
7. Aggarwal, M. et al. (2023). A 2 million-person, campaign-wide field experiment shows how digital advertising affects voter turnout. Nature Human Behaviour, 7(3), Article 3. https://doi.org/10.1038/s41562-022-01487-4
8. Coppock, A., Green, D. P., & Porter, E. (2022). Does digital advertising affect vote choice? Evidence from a randomized field experiment. Research & Politics, 9(1), 20531680221076901. https://doi.org/10.1177/20531680221076901
9. Broockman, D. E., & Green, D. P. (2014). Do Online Advertisements Increase Political Candidates' Name Recognition or Favorability? Evidence from Randomized Field Experiments. Political Behavior, 36(2), 263–289. https://doi.org/10.1007/s11109-013-9239-z
10. Shaw, D., Blunt, C., & Seaborn, B. (2018). Testing Overall and Synergistic Campaign Effects in a Partisan Statewide Election. Political Research Quarterly, 71(2), 361–379. https://doi.org/10.1177/1065912917738577
11. Errenst, E., Remoortere, A. V., Vermeer, S., & Kruikemeier, S. (2023). Instaworthy? Examining the Effects of (Targeted) Civic Education Ads on Instagram. Media and Communication, 11(3), 238–249. https://doi.org/10.17645/mac.v11i3.6614
12. Hager, A. (2019). Do Online Ads Influence Vote Choice? Political Communication, 36(3), 376–393. https://doi.org/10.1080/10584609.2018.1548529
13. Kruikemeier, S., Sezgin, M., & Boerman, S. C. (2016). Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses. Cyberpsychology, Behavior and Social Networking, 19(6), 367–372. https://doi.org/10.1089/cyber.2015.0652
14. Krotzek, L. J. (2019). Inside the Voter's Mind: The Effect of Psychometric Microtargeting on Feelings Toward and Propensity to Vote for a Candidate. International Journal of Communication, 13, 3609–3629. https://ijoc.org/index.php/ijoc/article/view/9605/2742
15. Zarouali, B., Dobber, T., De Pauw, G., & de Vreese, C. (2022). Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. Communication Research, 49(8), 1066–1091. https://doi.org/10.1177/0093650220961965
16. Lavigne, M. (2021). Strengthening ties: The influence of microtargeting on partisan attitudes and the vote. Party Politics, 27(5), 965–976. https://doi.org/10.1177/1354068820918387
17. Endres, K. (2020). Targeted Issue Messages and Voting Behavior. American Politics Research, 48(2), 317–328. https://doi.org/10.1177/1532673X19875694

3 Promises and risks of PMT

Given the fairly recent emergence of PMT around the world, the evidence base around its use and effects is still being developed. While the initial research evidence offers a conflicting view into the effectiveness of PMT, the promises and challenges of PMT have been discussed to some extent. On one hand, there are indications for benefits that the use of PMT may introduce, and on the other, research has identified potential risks that could follow from the use of PMT. Without regulatory intervention to bring these practices in line with the interest of society, the risks of PMT appear to outweigh the promises, based on current evidence.

3.1 Promises

Among the chief potential benefits of PMT are an increased informational value of political communication through ad relevance and diversification of content; efficiency of campaign activity; and the ability to reach and activate specific population segments, each of which will be discussed in more detail in this subchapter.[iv] Better functioning political communication could, in turn, activate voters to become interested in politics and participate in political activities—which seems particularly relevant in view of the declining voter turnout in democracies all over the world.[3] However, while the above-mentioned promises of PMT often surface in popular discourse, there is only limited scientific evidence to support them. Also, there are questionable assumptions underlying each of the three promises, which will be addressed below.

3.1.1 Relevance and diversification of ad content

By matching the content and style of political messages to the personalities and preferences of a targeted individual or group, PMT may deliver information that recipients find particularly relevant and interesting.[4] This could benefit the targeted citizens, as receiving meaningful information could raise their interest in political participation.[5,6] Targeted meaningful information could also save citizens time and avoid fatigue, as they may be able to access content they find relevant faster and avoid wading through political messages directed to a wider audience which may not address their particular interest.

PMT may also lead to more diverse political communication. Given the goal of PMT to communicate through messages that are congruent with the preferences and personalities of specific demographic groups, political campaigns and communication may diversify to cater to these varying voter profiles. This process may be further facilitated by the pressure of partisan competition directing parties to vie for the votes of particular groups or by the flexibility afforded by online PMT. Political communication through PMT may therefore extend the range of the addressed political issues beyond the scope of the messages communicated through major campaigns or traditional media such as television or radio.

These arguments assume an ideal situation where PMT does not contain disinformation.[v] Both arguments also only apply to citizens who are targeted with a relevant ad. It could be the case that others who could share the benefit were not adequately identified in the collected data and therefore miss out on any benefits that receiving the ad may have yielded.

3.1.2 Campaign efficiency

Political campaigning requires substantial financial and other resources. PMT may be able to deliver political messages at a lower cost and more effectively than traditional television or radio advertisements, therefore conserving resources.[4] This feature may be particularly appropriate in the context of restricted election campaigns and caps on campaign spending. Where these restrictions are strictly enforced, cheaper online PMT may have a significant impact. Owing to its cost efficiency, PMT may also enable smaller or financially weaker political entities to reach potential voters, funders, and supporters. The accessibility of PMT through intermediaries allows weaker political entities without the resources for dedicated in-house units to reach their target audience and bypass appearances in mass media outlets, which can be difficult to access. However, the "equalizing impact" of any efficiencies introduced by PMT may be called into question by the fact that such efficiencies can be equally derived by well-established powerful political entities. Bigger budgets, capacities for in-house technical units, and the likely role as first movers into applying PMT may result in more powerful

[iv] For a review, see for instance Matthes[1] and Zuiderveen Borgesius et al.[2] who discuss the promises of PMT as they pertain to citizens, politicians, and public opinion. This chapter draws examples from these two articles, please refer to them for further detail.

[v] In reality, PMT is often used as a vessel for disinformation—see Chapter 3.2.2 ("Spread of disinformation").

political entities reaping bigger benefits and leaving lower-resourced actors further behind.[vi]

3.1.3 Possibility to reach and activate specific population segments

Political entities around the world have a stake at reducing voter apathy within their country. With the increasing fragmentation of the global media spaces reducing the effectiveness of traditional political communication, PMT can succeed in connecting with particular demographic groups or niche audiences that are otherwise hard to reach.[7] Young voters may be particularly likely to be reached by online PMT. Politically disengaged citizens may be reachable through popular social media platforms and relevant targeted PMT could increase their interest in politics and encourage political participation.[4] However, to this date, empirical research finds conflicting evidence when it comes to voter mobilization.[8] Furthermore, these potential benefits assume that the PMT reaching the targeted individuals is used to activate them for instance through encouraging them to vote or through serving relevant ad content to vulnerable groups rather than any negative effects such as spreading disinformation or demobilizing voters.

3.2 Risks

This subchapter will provide an overview of the manifold risks associated with PMT. These risks can intersect and drive each other (e.g., lack of transparency facilitating disinformation; disinformation being used for voter manipulation). In sum, the examined risks can result in a violation of human autonomy and dignity by depriving individuals of the right to informed political decision-making and exposing them to hate, violence, and discrimination. On the collective, societal level, the use of PMT may pose a threat to social cohesion, national sovereignty, public discourse, and the principle of free and fair elections, thus potentially undermining the foundations of democracy.

3.2.1 Voter manipulation and demobilization

PMT has been used in numerous attempts to manipulate public opinion and sway the outcome of elections.[9] Despite inconclusive scientific evidence regarding the effects of PMT on actual voting behavior,[vii] one key concern with PMT is the technique's potential to interfere in voters' political will or actively dissuade specific population segments from voting and politically participating.[10,11] Through a growing base of granular profiling data and increasingly intelligent algorithms, political campaigns may get better at understanding which specific buttons they need to push in order to influence people's opinions and nudge their behavior in a particular direction, favoring the sender's interests. To increase persuasiveness, targeted political ads can be based on sensitive attributes, such as individuals' interests, biases, fears, and vulnerabilities.[4,12] As many elections are won by small margins,[13] even a relatively subtle manipulation of public opinion may have devastating consequences for democracy.

Of course, all forms of commercial and political advertising are persuasion attempts to some extent. The question is when they cross the boundary to undue manipulation. As defined by Susser et al., "manipulation is hidden influence—the covert subversion of another person's decision-making power" whereas persuasion "is the forthright appeal to another person's decision-making power".[14] Given its opaque nature,[viii] PMT could well fall under the above definition of manipulation. As Bayer observes, "Users have been deluded into believing that the encountered information is spontaneous, citizen generated, objective and universally encountered by other users, while in fact it may have been strategic, political and micro-targeted."[12] PMT has even been used to facilitate vote buying schemes and voter intimidation (e.g., in Nigeria).[15] If effective, PMT-based voter manipulation could violate individual autonomy and pose a severe threat to the functioning of democracy. Also, as an unintended side effect, when voters become aware of continued manipulation attempts via PMT, they "may lose trust in politicians, political parties and the democratic system overall" and therefore become demobilized.[9]

3.2.2 Spread of disinformation

Disinformation is on the rise worldwide[16] and has been identified as a "corrosive existential threat to democracy"[17] as it often contributes to social division, violence, and destabilization of elections.[18] Political ads can be used as a vessel for disinformation. Among other things, this can include false statements, manipulated media, and fake ads (i.e., ads made to appear to be from a particular party, but in fact aimed at demobilizing supporters of that party). For instance, in Colombia's 2022 presidential election, Facebook ads were used by so-called "disinformation for hire" marketing firms to spread hateful, misleading, and false content to discredit selected politicians.[19] PMT in particular, due to its opacity,[ix] can make it difficult to detect and expose disinformation campaigns. Along social bots, PMT has been a key channel for spreading disinformation.[12] When political ads are tailored to specific groups of voters, campaigns can selectively "share only those fragments of their political programs with the targeted voters these would be likely to support"[12] or even make contradicting electoral promises to different segments of the population.[20] As Zuiderveen Borgesius et al. state, "microtargeting enables a political party to, misleadingly, present itself as a different one-issue party to different people. (…) A risk for public opinion is that the priorities of political parties may become opaque."[4] Finally, based on information about people's fears, knowledge gaps and other vulnerabilities, PMT can also be used to target voter groups that are susceptible

[vi] See Chapter 3.2.5 ("Unfair competition between political actors")
[vii] See Chapter 2.1 ("Direct effects of PMT")
[viii] See Chapter 3.2.3 ("Lack of transparency")
[ix] See Chapter 3.2.3 ("Lack of transparency")

to certain types of disinformation.[21,22] Moving forward, it remains to be seen how increasingly advanced AI systems will continue to impact the spread of disinformation. Generative AI models, for instance, can facilitate disinformation campaigns through automated generation and manipulation of content.[23] In general, AI may enable malicious actors to disseminate disinformation in a much more efficient and tailored manner.[24]

3.2.3 Lack of transparency

There are multiple aspects that make PMT intangible, opaque and difficult to understand:

- **"Dark ads":** In contrast to conventional political ads (e.g., radio, television, newspaper, billboards), one central feature of PMT is that ads are only directly visible to the target audience, not to the general public.

- **Attribution problem:** It can be difficult to identify the ultimate source of online political influence campaigns.[25] This is exemplified by the complex investigation required to establish a connection between apparent Ghanaian NGO activities and the Russian interference in the 2016 US election.[26] In many cases, it is not possible to trace such connections. For instance, it remains unclear who paid the Israel-based political consultancy firm Archimedes Group for attacking local politicians with viral misinformation in the 2019 Nigeria election.[27]

- **Opaque collection of personal data:** For ad targeting purposes, political campaigns often gather vast amounts of personal data from various sources, including social media, campaign apps, voter registration records, and data brokers.[28] They are not always transparent about their data practices, and voters may not be aware of the data that is being collected about them or how it is being used. After PMT campaigns in Kenya, for instance, "[m]any people who did not consider themselves politically active wondered how politicians and candidates obtained their names and phone numbers."[29]

- **Proprietary algorithms and systems:** PMT often uses advanced algorithms to analyze and segment data. These algorithms can be complex and opaque, using hundreds or thousands of parameters, and are often treated as trade secrets (e.g., closed-source systems, non-disclosure agreements).[30,31] This makes it difficult to understand how exactly they work and how they influence the ads that people receive.

- **Number of ads:** When political ads are tailored to specific segments of the population, this increases the number of ad variations. For instance, Trump's 2016 presidential campaign placed tens of thousands of individual variations of microtargeted ads per day.[32] Even in the most transparent scenario where all targeted political ads are made available to the public through an ad library, it is "[h]ard for anyone to tell what's 'important', among thousands—or millions—of targeted ads."[30]

- **Opaque effects of PMT:** There is lack of evidence regarding the effects of PMT[x] which makes it difficult to assess the resulting benefits and damages in a precise and informed manner.

3.2.4 Privacy violations

As a form of "surveillance-based advertising",[33] PMT involves collecting and analyzing vast amounts of personal information, such as political affiliations, browsing history, and GPS location data.[9] This information can be used to create detailed profiles of individuals and target them with highly personalized political ads. Similar to commercial targeted advertising (the primary source of revenue in the Internet economy[34]), the flourishing political influence industry[35] creates economic incentives for "excessive data collection, particularly of privileged, highly personal data, on voters".[30] Online manipulation often involves the "irresponsible, illegal or unethical use of personal information."[36] Data collected for the purpose of PMT can also be leaked to third parties and be used for other potentially harmful purposes beyond political advertising.[21] The lack of transparency in PMT[xi] can make it difficult for voters to understand how their personal data is being used and to hold campaigns accountable for privacy violations. Personal information is often collected and inferred in intricate ways that are difficult to trace and fully comprehend, even for technical experts.[37] In general, due to the complexities involved, individual data subjects are typically not able to properly assess the risks of modern data practices, such as PMT, and make truly informed privacy choices.[38]

3.2.5 Unfair competition between political actors

By allowing campaigns to focus their messaging on specific groups of voters, PMT can create a situation where advertisers with greater resources and more sophisticated data analysis capabilities (e.g., larger parties with wealthy donors) can gain an unfair advantage over their competitors.[9] While the advantage of wealthier parties is a common factor across political advertising methods, the asymmetry may be accentuated in the case of PMT, as this technique heavily relies on access to detailed profiling data, analytical tools as well as know-how in data science and behavioral psychology. Considering the increasing global demand for these assets and skills, which also extends to the private sector, they can pose affordability challenges for smaller parties operating within limited financial means. This could amount to an entrance barrier for new opposition parties that lack the experience and expertise to "play the game" of data-driven campaigning.[30] India's 2019 election is an illustrative

[x] See Chapter 2.1 ("Direct effects of PMT")

[xi] See Chapter 3.2.3 ("Lack of transparency")

example of unequal access to digital campaigning tools: Out of all political ads on Google, YouTube and Google's partner properties, 60% were paid for by the ruling party, which spent a staggering 500% more than the main party in the opposition.[39] Political parties with large advertising budgets may even receive special services and privileged access to internal knowledge of online platforms and advertising networks.[40] It is well documented, for instance, that Google employees have worked inside political campaigns, "sometimes indistinguishable from campaign hands."[41]

3.2.6 Foreign influence into domestic affairs

While attempts to influence public opinion through PMT are often made by domestic actors, it is important to emphasize the threat posed by foreign influence. It is well documented that certain global powers aggressively try to influence media and politics in other countries.[42] According to a recent report, the top three countries instigating manipulation campaigns on Facebook, Instagram, and Twitter (now X) were China, Iran, and Russia.[43] Through its engagement and media offensive in Africa,[44] for instance, China is trying to "advance its interests across the continent [and] promote its model of state-led economic growth under one-party, authoritarian rule to African countries".[45] Beijing's media influence goes far beyond Africa and also affects—next to EU, US, and Australia—numerous countries in Asia and Latin America.[46] Propaganda by foreign entities often seeks to disguise its origin.[47] Through its opacity and targeted approach, PMT can allow foreign actors to "pursue anti-democratic goals in the shadows (...) [and] spread propaganda more effectively by introducing a customized propaganda narrative".[25] For instance, they could use PMT to harm the public's trust in the government, the media, and public institutions;[48] to advertise in favor of a political party that supports their geopolitical interests;[46,49] to improve their own image abroad;[50,51] to change the public's view on global events;[52] or to intentionally divide society.[53]

While attempts to influence public opinion through PMT are often made by domestic actors, it is important to emphasize the threat posed by foreign influence.

3.2.7 Difficulty of public scrutiny and counter speech

In the past, political campaigns had only few options to reach out to specific voter groups or individuals (e.g., door-to-door campaigning, political booths). As a result, most of their messaging had to be disseminated to the general public through mass media platforms like TV, radio, and billboards, allowing citizens, competing campaigns, and journalists to scrutinize and challenge them. When political messages are delivered through PMT, they are not directly visible to the public but only to the respective target audience. This makes it difficult to monitor and factcheck political messaging in real time[25,54] and can enable "an opaque campaign to which political competitors cannot respond".[11] It also fragments public discourse by hindering a shared information foundation that encompasses diverse opinions and perspectives, thus undermining the "marketplace of ideas" principle which is essential to a functioning democracy.[54]

When political messages are delivered through PMT, they are not directly visible to the public but only to the respective target audience. This makes it difficult to monitor and factcheck political messaging.

3.2.8 Distortion of voter model and political mandates

By relying on assumptions about voter behavior, incomplete data, and artificial categorizations, PMT can create a one-dimensional view of voters that fails to capture the complexity and diversity of their beliefs and experiences. Both the data and methods used for PMT typically contain a certain degree of error and bias.[55] This can lead to campaigns that are based on a constructed reality, where the messages and issues being discussed are not reflective of the real concerns and priorities of the electorate.[56] In particular, since people strongly vary in their level of social media use and online activity, there is a risk that political campaigns will focus on analyzing data from the more active Internet users, even if that group does not accurately represent the entire population.[57] This risk can be pronounced in economically disadvantaged countries where a significant proportion of the population is without Internet access. Additionally, PMT campaigns can be intentionally limited to targeting specific segments of the population (e.g., swing voters[xii]) while ignoring others, potentially "reduc[ing] the portion of the electorate that politicians need to campaign to and for, and ultimately care about after the election".[54] When one campaign sends conflicting messages and electoral promises to different groups of voters through PMT, this may lead to ambiguous political mandates for elected representatives.[59]

3.2.9 Discrimination

PMT can perpetuate existing inequalities in a society and contribute to discrimination and marginalization in multiple ways, including:

- **Limited access to information:** PMT can be used to exclude specific audiences from receiving ads and allow a prioritization of "who is considered a valuable voter and who is not".[9] For example, where not prohibited by law, targeting techniques can exclude people based on

[xii] The practice of limiting political campaigning to those voters that are most likely to be influenced is referred to as "political redlining".[58]

demographic attributes such as age, gender, income, level of education, ethnicity, religion, health status or sexual orientation.[60] This can lead to unequal access to information and lack of awareness in certain population segments (e.g., national minorities). As Bayer states, PMT “violates the fundamental right of the non-targeted electors to receive complete information about the candidates and parties in the electoral dispute”.[61]

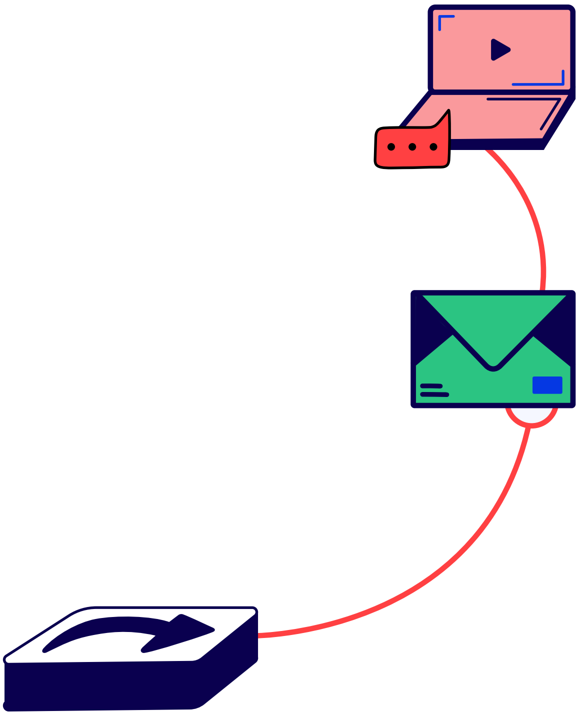
- **Reinforcement of prejudices:** Due to the lack of public scrutiny,[xiii] PMT may be more prone than other types of political advertising to contain discriminatory language or imagery. This can include, for example, scare campaigns about “migrant caravans”, anti LGBTQIA+ ads, or ads portraying a female candidate as weak or emotional to suggest that she is not qualified for the job.

- **Voter suppression of marginalized groups:** PMT can also be used to target already disenfranchised communities with (deceptive) messaging that promotes apathy towards voting.[62] For instance, this could include ads suggesting that their votes will not count or that the election is rigged, leading targeted voters to believe that it is not worth participating in the political process.

3.2.10 Political polarization

Political discussions may become fragmented when voter groups are exposed to different arguments and focus on different topics.[4] Thus, when political ads are being tailored to specific audiences based on their political leanings, this can entrench existing divisions in society and lead to a more toxic political environment. PMT may even contribute to the creation of online “echo chambers”, where individuals only receive information that confirms their existing beliefs and values, making it difficult for them to form opinions based on careful consideration of different viewpoints.[22] This problem is further compounded by the fact that PMT often addresses politically controversial topics or “wedge issues”, such as poverty, corruption, migration, race, gender, and neglected minorities.[9] Disinformation, which can be enabled through PMT,[xiv] can also contribute to polarization by amplifying false or misleading information that aligns with the targeted audience’s beliefs.[9] Ultimately, the polarizing effects of PMT can incite hatred and violence. Especially when paired with negative messages towards certain communities or individuals, which is often the case,[29,63] PMT can contribute to creating a hostile and dangerous political environment. This is well illustrated by a case where Facebook admitted to having played a role in inciting violence during the genocidal campaign against the Rohingya Muslim minority in Myanmar,[64] which involved targeted ads.[65]

Disinformation, which can be enabled through PMT, can also contribute to polarization by amplifying false or misleading information that aligns with the targeted audience’s beliefs.



[xiii] See Chapter 3.2.7 (“Difficulty of public scrutiny and fact-checking”)
[xiv] See Chapter 3.2.2 („Spread of disinformation”)

References

1. Matthes, J., Hirsch, M., Stubenvoll, M., Binder, A., Kruikemeier, S., Lecheler, S., & Otto, L. (2022). Understanding the democratic role of perceived online political micro-targeting: Longitudinal effects on trust in democracy and political interest. Journal of Information Technology & Politics, 19(4), 435–448. https://doi.org/10.1080/19331681.2021.2016542
2. Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, 14(1), 82–96. https://doi.org/10.18352/ulr.420
3. Kostelka, F., & Blais, A. (2021). The Generational and Institutional Sources of the Global Decline in Voter Turnout. World Politics, 73(4), 629–667. https://doi.org/10.1017/S0043887121000149
4. Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, 14(1). https://doi.org/10.18352/ulr.420
5. Murray, G. R., & Scime, A. (2010). Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies. Journal of Political Marketing, 9(3), 143–166. https://doi.org/10.1080/15377857.2010.497732
6. Kreiss, D. (2012). Yes We Can (Profile You). Stan. L. Rev. Online, 64, 70.
7. Hamel, B. (2013). Microtargeting: Politics of Participation, Politics of Polarization. American University Library. https://edspace.american.edu/atrium/portfolio-item/hamel-brian-microtargeting-politics-of-participation-politics-of-polarization/
8. Errenst, E., Remoortere, A. V., Vermeer, S., & Kruikemeier, S. (2023). Instaworthy? Examining the Effects of (Targeted) Civic Education Ads on Instagram. Media and Communication, 11(3), 238–249. https://doi.org/10.17645/mac.v11i3.6614
9. Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R., & Wright, G. (2019). Personal Data: Political Persuasion. Inside the Influence Industry. How it works. Tactical Tech. https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf
10. Jaursch, J. (2020). Defining Online Political Advertising. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/en/publication/defining-online-political-advertising
11. Panoptykon. (2020). Who (really) targets you? Fundacja Panoptykon. https://panoptykon.org/political-ads-report
12. Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs. https://www.ssrn.com/abstract=3409279
13. Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proceedings of the National Academy of Sciences, 112(33), E4512–E4521. https://doi.org/10.1073/pnas.1419828112
14. Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online Manipulation: Hidden Influences in a Digital World. Georgetown Law Technology Review, 4, 1.
15. Hassan, I., & Segun, T. (2020). Personal Data and the Influence Industry in Nigerian Elections. Tactical Tech. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Data-Politics-Nigeria-CDD-Tactical-Tech.pdf
16. Romeo, J. (2022). Disinformation is a growing crisis. Governments, business and individuals can help stem the tide. World Economic Forum. https://www.weforum.org/agenda/2022/10/how-to-address-disinformation/
17. Reglitz, M. (2022). 'Fake news' poses corrosive existential threat to democracy—Study. University of Birmingham. https://www.birmingham.ac.uk/news/2022/fake-news-poses-corrosive-existential-threat-to-democracy-study
18. Sanchez, C. (2019). Misinformation is a Threat to Democracy in the Developing World. Council on Foreign Relations. https://www.cfr.org/blog/misinformation-threat-democracy-developing-world
19. Pérez, D. S. (2022). Colombian PR firms used Facebook ads to spread disinfo on presidential candidates. https://medium.com/dfrlab/colombian-pr-firms-used-facebook-ads-to-spread-disinfo-on-presidential-candidates-c44e1ac18bba
20. Wong, J. C. (2018). "It might work too well": The dark art of political advertising online. The Guardian. https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy
21. Kröger, J. L., Miceli, M., & Müller, F. (2021). How Data Can Be Used Against People: A Classification of Personal Data Misuses (SSRN Scholarly Paper 3887097). https://doi.org/10.2139/ssrn.3887097
22. Simon, E. (2020). Solutions for Regulating Microtargeted Political Advertising. Civil Liberties Union for Europe. https://www.liberties.eu/f/fy69vA
23. Gregory, S. (2023). Fortify the Truth: How to Defend Human Rights in an Age of Deepfakes and Generative AI. Journal of Human Rights Practice, huad035. https://doi.org/10.1093/jhuman/huad035
24. Bontridder, N., & Poullet, Y. (2021). The role of artificial intelligence in disinformation. Data & Policy, 3, e32. https://doi.org/10.1017/dap.2021.20
25. Ó Fathaigh, R., Dobber, T., Zuiderveen Borgesius, F., & Shires, J. (2021). Microtargeted propaganda by foreign actors: An interdisciplinary exploration. Maastricht Journal of European and Comparative Law, 28(6), 856–877. https://doi.org/10.1177/1023263X211042471
26. Ward, C., Polglase, K., Shukla, S., Mezzofiore, G., & Lister, T. (2020). Russian election meddling is back—Via Ghana and Nigeria—And in your feeds. CNN. https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html
27. Bradshaw, S., Campbell-Smith, U., Henle, A., Perini, A., Shalev, S., Bailey, H., & Howard, P. N. (2020). Country Case Studies Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Programme on Democracy & Technology, University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/03/Case-Studies_FINAL.pdf
28. Bashyakarla, V., Hankey, S., Macintyre, A., Rennó, R., & Wright, G. (2019). Personal Data: Political Persuasion Inside the Influence Industry. How it works. Tactical Tech. https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf

29. Mutung'u, G. (2018). The Influence Industry Data and Digital Election Campaigning in Kenya. Tactical Tech. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf
30. Who Targets Me. (2020). What are we to do about microtargeting? Who Targets Me. https://whotargets.me/en/what-to-do-about-microtargeting/
31. Panoptykon Foundation. (n.d.). #WhoReallyTargetsYou: DSA and political microtargeting. European Digital Rights (EDRi). https://edri.org/our-work/whoreallytargetsyou-political-microtargeting-cant-be-ignored-by-the-dsa/
32. Navarria, G. (2019). The Networked Citizen: Power, Politics, and Resistance in the Internet Age (1st ed.). Palgrave Macmillan Singapore.
33. Becker Castellaro, S., & Penfrat, J. (2022). The DSA fails to reign in the most harmful digital platform businesses – but it is still useful. Verfassungsblog. https://verfassungsblog.de/dsa-fails/
34. Milano, S. (2021). Targeted ads aren't just annoying, they can be harmful. Here's how to fight back. Fast Company. https://www.fastcompany.com/90656170/targeted-ads-arent-just-annoying-they-can-be-harmful-heres-how-to-fight-back
35. Macintyre, A. (2021). The Influence Industry Long List: The Business of Your Data and Your Vote. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/the-influence-industry-long-list/
36. European Data Protection Supervisor (EDPS). (2018). Opinion 3/2018 on online manipulation and personal data. https://edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf
37. Kröger, J. L., Gellrich, L., Pape, S., Brause, S. R., & Ullrich, S. (2022). Personal information inference from voice recordings: User awareness and privacy concerns. Proceedings on Privacy Enhancing Technologies. https://petsymposium.org/popets/2022/popets-2022-0002.php
38. Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). The Myth of Individual Control: Mapping the Limitations of Privacy Self-management (SSRN Scholarly Paper 3881776). https://doi.org/10.2139/ssrn.3881776
39. Chaturvedi, A. (2019). BJP top spender on political ads on digital platforms. The Economic Times. https://economictimes.indiatimes.com/news/elections/lok-sabha/india/bjp-top-spender-on-political-ads-on-digital-platforms/articleshow/69351792.cms?from=mdr
40. Rennó, R. (2019). Search Result Influence: Reaching voters seeking answers. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/search-influence/
41. Partisan Programming: How Facebook and Google's Campaign Embeds Benefit Their Bottom Lines. (n.d.). Campaign for Accountability. https://campaignforaccountability.org/work/partisan-programming-how-facebook-and-googles-campaign-embeds-benefit-their-bottom-lines/
42. Madrid-Morales, D., Börekci, D., Löffler, D., & Birkevich, A. (2021). It is about their story—How China, Turkey and Russia influence the media in Africa. Konrad-Adenauer-Stiftung. https://www.kas.de/documents/285576/0/How+China%2C+Turkey+and+Russia+influence+media+in+Africa.pdf/6594fc3e-f240-6aea-342d-92c8f90dbf43?version=1.2&t=1611811364948
43. Bailey, H., & Howard, P. N. (2022). The Instigators and Targets of Organised Social Media Manipulation: Global Index 2022. DEM.TECH Working Paper. Oxford Internet Institute, University of Oxford. https://hannahlsbailey.github.io/docs/demtech_hannahbailey_memo.pdf
44. Grassi, S. (2014). Changing the narrative: China's media offensive in Africa. Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/iez/10700.pdf
45. Green, W., Nelson, L., & Washington, B. (2020). China's Engagement with Africa: Foundations for an Alternative Governance Regime. U.S.-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/2020-05/Chinas_Engagement_Africa.pdf
46. Cook, S. (2022). Beijing's Global Media Influence. Freedom House. https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience
47. Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.
48. Kaye, D. (2017). Statement by David Kaye, special rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations Human Rights, Office of the High Commissioner. https://www.ohchr.org/en/statements/2017/10/statement-david-kaye-special-rapporteur-promotion-and-protection-right-freedom
49. Manga, E., & Kenderdine, T. (2022). What Kenya's Presidential Election Means for China's Belt and Road Initiative. The Diplomat. https://thediplomat.com/2022/08/what-kenyas-presidential-election-means-for-chinas-belt-and-road-initiative/
50. Tambe, A. M., & Friedman, T. (2022). Chinese state media Facebook ads are linked to changes in news coverage of China worldwide. Harvard Kennedy School Misinformation Review. https://doi.org/10.37016/mr-2020-88
51. Kaiman, J. (2017, August 7). "China has conquered Kenya": Inside Beijing's new strategy to win African hearts and minds. Los Angeles Times. https://www.latimes.com/world/asia/la-fg-china-africa-kenya-20170807-htmlstory.html
52. Gold, A. (2022, March 9). China's state media buys Meta ads pushing Russia's line on war. Axios. https://www.axios.com/2022/03/09/chinas-state-media-meta-facebook-ads-russia
53. Meaker, M. (2023). Facebook Is Still Letting Russia Interfere in Politics. Wired. https://www.wired.com/story/facebook-is-still-letting-russia-interfere-in-politics/
54. Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1433
55. Hargittai, E. (2020). Potential Biases in Big Data: Omitted Voices on Social Media. Social Science Computer Review, 38(1), 10–24. https://doi.org/10.1177/0894439318788322
56. Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. C. M. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. Big Data & Society, 5(2). https://doi.org/10.1177/2053951718811844
57. Barberá, P., & Rivero, G. (2015). Understanding the Political Representativeness of Twitter Users. Social Science Computer Review, 33(6), 712–729. https://doi.org/10.1177/0894439314558836

58. Council of Europe. (2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes—Decl(13/02/2019)1. https://rm.coe.int/090000168092dd4b
59. Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. Proceedings of the First Edition Workshop on Politics, Elections and Data, 31–36. https://doi.org/10.1145/2389661.2389671
60. Holt, K. (2021). EU seeks to block political ads that target people's ethnicity or religion. Engadget. https://www.engadget.com/eu-targeted-political-ads-ethnicity-religion-sexual-orientation-transparency-233011048.html
61. Bayer, J. (2020). Double harm to voters: Data-driven micro-targeting and democratic public discourse. Internet Policy Review, 9(1). https://doi.org/10.14763/2020.1.1460
62. Stracqualursi, V. (2020). Trump campaign microtargeted Black Americans disproportionally "to deter" them from voting in 2016 election, Channel 4 reports. CNN. https://www.cnn.com/2020/09/29/politics/trump-2016-campaign-voter-deterrence/index.html
63. Hotham, T. (2019). We need to talk about A/B testing: Brexit, attack ads and the election campaign. LSE BREXIT. https://blogs.lse.ac.uk/brexit/2019/11/13/we-need-to-talk-about-a-b-testing-brexit-attack-ads-and-the-election-campaign/
64. Global Witness. (2022). Facebook approves adverts containing hate speech inciting violence and genocide against the Rohingya. https://www.globalwitness.org/en/campaigns/digital-threats/rohingya-facebook-hate-speech/
65. De Guzman, C. (2022). Report: Facebook Algorithms Promoted Anti-Rohingya Violence. Time. https://time.com/6217730/myanmar-meta-rohingya-facebook/

4 Example cases Global South

Most of the literature and media reports on PMT draw from experiments, examples, and case studies in the Global North. While detailed investigations with a focus on PMT in the Global South exist, these have not yet received much coverage on the international level. To help balance global coverage, this chapter presents brief reviews of PMT applications in Kenya, Nigeria, the Philippines, India, Chile, Brazil, and Colombia. We show that PMT is prevalent across all seven countries and is applied through a range of methods in diverse settings. There are some parallels between the cases as well: The social media platforms and instant-messengers used for PMT are often operated by Western companies such as Meta (Facebook, Instagram, and WhatsApp) and X (formerly Twitter), each of which offers fertile ground for the circulation of political messages which can deepen biases, exacerbate risks of already marginalized and vulnerable groups, multiply mis- or disinformation, amplify polarization, and induce hostility and violence.[xv] Fairly short experiences with democratic regimes, widespread corruption, and nascent legal and policy frameworks governing the collection and use of personal data are other challenges that the seven countries share. The example cases were chosen based on how extensively they had been discussed in academia and media already prior to the Summit for Democracy Year of Action, of which this report is a product. This approach aims to ensure that only well-documented cases are presented on the sensitive topic of PMT. The Chinese platform TikTok is not covered in this chapter because it had not yet attained the current level of prominence and political relevance in the country cases under consideration. However, the platform has seen rapid growth over the last years and is increasingly being used by political actors around the globe. Therefore, future investigations should also examine TikTok as a potential channel for PMT.

4.1. Example cases Africa

4.1.1. Kenya

(Socio-political) background

After gaining independence in 1963, Kenya enjoyed a period of remarkable stability, even in the face of shifts within its political landscape and turmoil in neighboring nations. Towards the end of the century, parliamentary reforms improved public freedoms and introduced a multi-party system in 1991. While characterised by a vibrant civil society and media landscape,[1] the country is also plagued by ethnically divided politics, election-related violence, and pervasive corruption. The Political Terror Scale, which measures levels of political violence that a country experiences, consistently shows high ratings for Kenya.[2] The disputed presidential election of 2007 was followed by a wave of violence leading to over 1,100 deaths[3] and around 600,000 people being displaced[4] in events that have been summarized in headlines as “Kenya on fire” and “Nairobi burning”.[5] Assessing the current condition of political rights and civil liberties, Freedom House rates Kenya a 52/100 on its ‘Freedom in the World’ index, classifying it as a “partly free” country.[6] In 2021, Kenya had an Internet penetration rate of 29%.[7]

Role of PMT

PMT has played a role in Kenyan elections at least since 2013, when Cambridge Analytica enabled messages leveraging for instance voters’ fears of tribal violence during the general election.[8] Three years prior to the company’s rise to the headlines after their involvement in the 2016 presidential election in the US, Cambridge Analytica, in the company’s own words, carried out “the largest political research project ever conducted in East Africa”[8] in Kenya. This involved building profiles that included information such as “key national and political issues, levels of trust in key politicians, voting behaviours/intentions, and preferred information channels”.[9] Collecting this information enabled the firm to “devise an online social media campaign to generate a hugely active online following”[9] and to design a campaign “based on the electorate’s real needs (jobs) and fears (tribal violence)”.[8]

By 2017, PMT was intertwined deeper into the country’s electoral processes with Cambridge Analytica improperly obtaining the personal data of 47,000 people through social media and complementing it with on-the-ground surveys.[10] In Kenya, ethnicity can often be discerned just based on an individual’s name, and with the information they collected, Cambridge Analytica was able to design targeted messages that were used to spread misinformation and potentially caused ethnically-based violence,[10] leading to accusations that the company engaged in “extreme scaremongering and fearmongering”.[11] Election-related violence remained a significant worry during the election[12] and at least

[xv] For a more comprehensive overview of risks of PMT, see Chapter 3.2.

37 people lost their lives during protests that took place after the election.[13] Data-driven methods were also used by tribal leaders and government officials to mobilize voters. Political aspirants and their supporters added people to groups on WhatsApp and channels on Telegram—often without their consent—in order to share personalized campaign messages.[10] In the absence of a data protection law,[xvi] a high volume of negative campaigning as well as false information circulated during the electoral period which is seen to have led to a deep polarization of the country.[10]

The introduction of the Kenyan data protection law in 2019 did not curtail PMT. Another form of PMT—paid influencers—was detected in 2021 when individuals were found to have been paid to create multiple accounts on Twitter (now X) to give the appearance of widespread support for an initiative seeking to introduce a controversial constitutional reform.[14] The initiative was later dismissed by the Supreme Court of Kenya, but many people were targeted on Twitter with political disinformation questioning the independence of the judiciary.[14] Such "disinformation-for-hire"[15] introduced a challenge for political communication given that influencers can earn an attractive level of pay and Twitter reportedly did little to curtail these disinformation campaigns.[16] By the general election of 2022, PMT was deployed on Facebook[17] and posts on Facebook and Instagram violated local election laws by failing to respect the ban on political advertising in the 48 hours before election day and by prematurely announcing election results.[18] Facebook was also criticized for approving ads calling for ethnically-based violence in the pre-electoral period.[19]

4.1.2 Nigeria

(Socio-political) background

Following three decades of military regimes, the general elections of 1999 marked the beginning of civilian rule in Nigeria. The transition to democratic rule saw improvements to the quality of civil liberties, press freedom, and the strengthening of Nigeria's civil society. However, challenges such as corruption, human rights abuses and criminal defamation laws remain, leading to a score of 43/100 and the label of "partly free" being assigned by Freedom House.[20] Further, the Political Terror Scale shows high ratings for Nigeria.[2] Over half of Nigerians are classified as multidimensionally poor and recently, economic challenges have been compounded by fuel and currency scarcity.[21] In early 2023, security challenges plagued the entire country resulting in the deployment of military troops.[21] While violence was feared to be widespread during the presidential and gubernatorial elections in February 2023, with 21 reported deaths,[22] the elections may have been the least violent in the country's recent history.[23] Regarding connectivity, infrastructural challenges hinder broad Internet access. As of January 2023, Nigeria had an Internet penetration rate of 55.4%.[24]

Role of PMT

During the general elections of 2011, politicians in Nigeria increasingly began to use online platforms, in particular social media, for political communication—a practice which was found to significantly impact the electorate's decision-making and participation.[25] In the 2015 election, Cambridge Analytica spread targeted disinformation in order to discourage votes from the opposition,[26,27] promoted ethnically and religiously-targeted violent content to intimidate voters,[28,29] and was found to be involved in an attempt to use hacked personal emails of a political candidate.[30,31] During the 2018 gubernatorial elections, a targeted vote buying scheme was deployed in Osun state, which involved linking people towards a WhatsApp contact, who would collect the voter's bank details and other information, promise an electronic transfer of money and ask for their contact information to be passed around by the bought voter.[26] During the 2019 election, PMT was used in particular to circulate disinformation, such as Facebook ads announcing Boko Haram's participation in the elections[32] or WhatsApp messages falsely announcing the death of the country's president Muhammadu Buhari.[33] Facebook removed 265 Facebook and Instagram assets created by an Israel-based group that Facebook deemed likely to interfere with elections.[34] Beyond mobile texting, other specific PMT techniques documented in Nigeria include bulk robocalls, recording of voters' browsing histories through tracking cookies, and geotargeting.[26] While regulations about data protection and fake news do exist, they are not effective and the regulatory setting in the country has been described as "porous", making it easy for political actors to assemble targeted voter databases.[35]

4.2 Example cases South & Southeast Asia

4.2.1 India

(Socio-political) background

Claiming the title of the world's largest democracy, India has a multi-party system, but single-party rule has been the electoral outcome over the last decade. Recently, political freedoms have declined and in 2021 Freedom House downgraded the country from "free" to "partly free".[36] Mobilizing such a sizeable electorate is not without its challenges and India has battled issues from voter fraud, corruption, and cybersecurity issues to managing public safety in areas that are vulnerable to electoral violence.[37] The Political Terror Scale records fairly high ratings for the country over the recent years.[2] Given its sizeable population, India is the biggest and fastest growing market for Western social media companies including Facebook and WhatsApp.[38] However, in light

[xvi] Without a data protection law, there was a lack of clear guidance on how data collected and processed in the country should be stored, retained, and protected.

of pervasive digital divides between urban and rural areas, only around 50% of the Indian population have Internet access.[39]

Role of PMT
Since 2014, the two largest Indian parties have incorporated digital campaigning. In the 2019 election, social media was used excessively to share political messages and mobilize voters but also to spread divisive messages focusing on caste and religion.[38] Parties were reported to use detailed profiles of voters to target them with messages that include misinformation and hateful language. An Indian news channel found that such divisive rhetoric among senior politicians had grown nearly fivefold in the four years after 2014[40] and the 2019 election became defined by increased social polarization[41] with fears of social media being used as "a weapon".[42] Messages that reflect mistrust and hate towards the Muslim community are particularly common in India.[38] WhatsApp is among the most popular media platforms for PMT and misinformation in the country owing to its userbase consisting of many individuals with limited exposure to other online information sources and a lack of digital skills.[43] Indian officials have even resorted to Internet shutdowns to stop harmful messages circulating on WhatsApp.[44] Prior to the 2019 election, PMT was used to target students and women who had been provided with low-cost smartphones in the state of Chhattisgarh.[45] These government-provided phones were targeted with robocalls containing political messages and collected data that was used by the campaign to steer on-the-ground activities.[45]

4.2.2 The Philippines

(Socio-political) background
The Republic of the Philippines is a multi-party electoral democracy where voter turnout is high despite corruption and lack of transparency. Multiple forms of electoral fraud are prevalent, and vote-buying and vote-selling are common practices.[46] Historically, elections have been overshadowed by intimidation and violence[47] and the Political Terror Scale is consistently very high for the country.[2] Freedom House rates the Philippines 58/100, making it a "partly free" country.[48] Known as one of the five Tiger Cub Economies, the Philippines show export-driven patterns of economic growth and stress the role of technology in achieving economic prosperity. In 2021, the Internet penetration rate was 53%,[49] and the prominent role of technology is reflected in the country's high levels of social media use. People in the Philippines spend an average 4.1 hours on social media every day—twice the global average of 2 hours.[50] Therefore, the country is often referred to as "the social media capital of the world".[51]

Role of PMT
The ubiquitous use of digital technologies makes the Philippines a fertile ground for online manipulation techniques. Orchestrated disinformation campaigns were first observed in the 2016 presidential elections which resulted in the victory of Rodrigo Duterte.[52] To illustrate the urgency of online manipulation in the country, the Philippines were described as "patient zero" in the so-called "global disinformation epidemic" by Facebook Executive Katie Harbarth.[53] PMT seems to have integrated into the political communication landscape during the 2019 elections. Whereas the traditional television, radio, and on-the-ground activities, such as rallies, formed the campaign budgets in previous elections, in 2019 significant funds were earmarked for social media. Digital campaigning took place on Facebook, Twitter, YouTube, and Instagram and the spread of disinformation was more camouflaged through micro- and nano-influencers.[54] Unlike celebrities or famous political pundits, these influencers have inconspicuous presence, which allows them to target smaller or niche audiences and build relationships that seem genuine. When a micro influencer cracks a joke about the election, includes a certain political hashtag in their message, or forwards a post from a candidate, the political opinion communicated seems authentic and remains very difficult to track as disinformation.[54,55] These strategies were used to elicit support for candidates and discourage votes for the competitors.[55] Target audiences included private groups or small communities that are moderated more loosely.[55]

4.3 Example cases South America

4.3.1 Brazil

(Socio-political) background
With a well-functioning multiparty system, strong protection of civil liberties and a vibrant media environment, Brazil has emerged as the world's fifth-largest democracy following its democratic transition in 1985 after decades of military dictatorship. Brazil scores 72/100 on the Global Freedom Index and therefore, qualifies as a "free" country.[56] However, over the past few years, the Political Terror Scale records fairly high ratings for the country.[2] Recently, Brazil's democracy has been challenged by political polarization, threats to freedom of speech and endemic corruption.[56] The 2022 presidential election between candidates Lula da Silva and Bolsonaro was characterised by high levels of polarization, disinformation and aggressive rhetoric and political violence on both sides. The country had an Internet penetration rate of 81% in 2022.[57] WhatsApp plays a significant role in Brazilians' social and political lives: It is estimated that more than 165 million people used the app in August 2022, representing over 75 percent of the population.[58] The app has previously functioned as a forum to organize political action. For instance, in 2018, truck drivers organizing a strike coordinated their protests and the blockage of key roads via WhatsApp.[59]

Role of PMT
Microtargeting and disinformation via WhatsApp chat groups had significant relevance in Brazil's 2018 presidential election, where campaigns built communication strategies that used Internet platforms and

messaging apps to communicate directly with different groups of voters. Researchers from the State University of Campinas and the Federal University of Rio de Janeiro found evidence of centralised management of WhatsApp chat groups, "built to manage and to stimulate members of discussion groups, which were treated as segmented audiences".[59] Targeted disinformation was spread via more than 1,500 WhatsApp groups that reflected specific religious, professional or regional interests.[59] While WhatsApp itself does not offer micro-segmentation as a service, marketing agencies filled that gap—sometimes based on information that was illegally obtained.[59] WhatsApp executives acknowledged that Brazilian accounts were the target of massive spamming operations before the election.[60] The intensive use of segmented WhatsApp groups for spreading political messages continued post-election, including false and misleading information as well as attacks on public figures, political opponents, news outlets and journalists, further contributing to a "hyperpolarized" political environment.[61] While Twitter, Facebook, YouTube, and blogs were also increasingly used to disseminate political messages, experts from Brazil have highlighted the role of WhatsApp as a "political weapon" and "tool for institutionalized computational propaganda", emphasizing that "[t]he origins and sources of messages are not easily traceable on WhatsApp, meaning that recipients tend to associate the information with a friend or family member who shared it."[61] Among other things, targeted disinformation in Brazil has helped political actors to downplay the COVID-19 crisis and justify the continued destruction of the Amazon Forest.[61]

4.3.2 Chile

(Socio-political) background

After the end of the military regime led by General Pinochet in 1990, Chile transitioned to democracy and underwent a significant expansion of political rights and civil liberties, most recently by the establishment of a new, progressive constitution. It is usually found at the top of democracy rankings in Latin America, evident in its score of 94/100 in the Global Freedom Index,[62] as well as its relatively low ratings on the Political Terror Scale.[2]

Chile is one of the most connected countries in Latin America,[63] with an Internet penetration rate of 90% in 2021,[64] and high levels of mobile phone usage, and social media adoption. Both WhatsApp and Facebook are used by over 80% of the population.[65,66] According to reports, nearly half (45%) of Internet users aged 55 years and over are using WhatsApp as a news source.[67] While Chile was the first country in Latin America to introduce a privacy law in 1999, the law does not cover personal data use in elections and is often not complied with.[66]

Role of PMT

According to the research center InternetLab, "Social media has played a central role in the electoral campaigns in Chile. (…) [I]n the last few elections, candidates have been using more targeted campaign strategies, with the help of data-driven agencies that use personal data to profile voters."[68] The privacy advocacy organization Datos Protegidos states in a report that "the high connectivity of the country together with the massive penetration of social networks in the Chilean population make it an ecosystem conducive to using social networks as tools for political propaganda."[69] A particularly interesting example is the geographical information system InstaGIS, also known in the local media as "big brother of political campaigning"[70] or "Chilean Cambridge Analytica".[71] Multiple political campaigns in national and municipal elections—many of them successful—worked with InstaGIS to enable targeted ads by analysing voters' comments and likes on social networks, socioeconomic status, geolocation, and political preferences (e.g., segmenting them based on their likeliness to vote for a certain candidate).[66] Besides targeted online ads, the services of InstaGIS were also used for data-driven telephone and door-to-door campaigning.[70] It has also been revealed that InstaGIS offered a "preferential price" to a major political campaign under the condition that the company could keep the results of this work, which it "may market without restriction for the purposes it deems appropriate"—essentially a carte blanche to sell sensitive personal data of thousands of unsuspecting citizens to third parties with unknown intentions.[70] Further, there is evidence to suggest that InstaGIS has used data from Chile's electoral register for voter profiling.[70] The register contains information on every Chilean who is eligible to vote, including their name, sex, unique identification number and electoral address. Chilean law does not permit the use of this data for commercial purposes. However, according to industry experts, there are diffuse boundaries between "research purposes" and "commercial uses".[66] According to experts in the field, data from the Chilean electoral register is widely used for data-driven campaigning (e.g., for profiling, segmentation of voters, geo-targeting) in combination with data from other sources.[66] It should be noted that through contracts with municipalities and public organizations, InstaGIS has access to citizens' data from projects in various other sectors (e.g., public procurement, prevention and rehabilitation of drug and alcohol consumption, citizen security, community development, school aid and scholarships).[70] In the field of data-driven campaigning, there are considerable legal and enforcement loopholes in Chile. In general, as a result of intensive lobbying of the marketing industry, Chile's aforementioned 1999 privacy law is rather geared towards regulating and enabling the business of personal data traffic than protecting the fundamental rights of people.[70] For instance, the law does not seek to protect individuals from the unwanted processing of their data by third parties, cross-border flows of personal data, or the use of their data for direct marketing without consent. There are neither effective sanctions for violating the law nor a public data protection authority.[70,72] Before the 2017 elections, there was a regulatory reform towards increased transparency on campaign spending and activities. These reforms, however, did not address the digital realm, leaving online political ads essentially unregulated.[66] Documents obtained by Datos Protegidos indicate that political parties in Chile have severely underdeclared their expenses for digital services, including InstaGIS.[69]

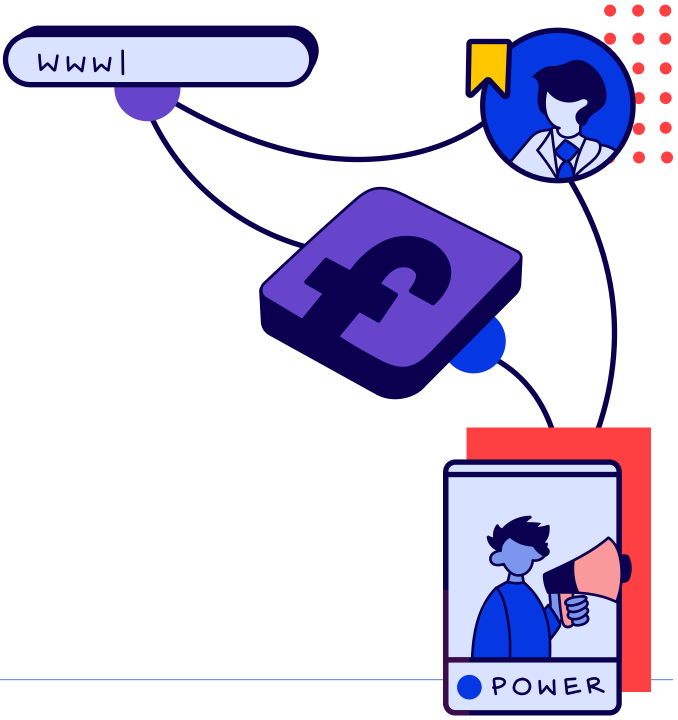
4.3.3 Colombia

(Socio-political) background

While being among the longest-standing democracies in Latin America, Colombia has a long history of political violence, rule-of-law violations, and lack of trust in public institutions. In 2016, a historic peace agreement ended the 50-year armed conflict between the Colombian government and the Revolutionary Armed Forces of Colombia (FARC).[73] Although a complete implementation of the accord remains difficult, Colombia has recently made important advances in counteracting political violence and strengthening democratic institutions. In 2023, Freedom House rated Colombia 70/100 on its 'Freedom in the World Index', updating its categorization to "free", whereas it was only rated as "partly free" in 2022.[73] Furthermore, the Political Terror Scale records moderate ratings for the country over the recent years.[2] Columbia had an Internet penetration rate of 73% in 2022,[74] and shows high levels of mobile use. With 64% of Colombians getting their news though social media in 2023, platforms such as X have become important tools in facilitating political discourse, especially since large areas of the country remain without local news coverage. However, trust in news on social media is low at around 35%.[75]

Role of PMT

At least since the 2018 national and the 2019 municipal elections, data protection and electoral advertising have been on the public agenda in Colombia. Researchers from Tactical Tech, an NGO focused on the impacts of technology on society, found that third-party tracking was employed during Colombia's 2018 national elections. An analysis of the leading parties' and candidates' websites revealed: "Of the leading 21 candidates' websites, eight had third-party Facebook trackers, 12 had Twitter trackers and 11 had some form of tracking on the donation page. Among 10 political party websites, five had Facebook trackers, seven from Twitter, and five had other trackers on the donation page."[76] As a result, searching for a particular candidate online and visiting their website often led to this candidate increasingly appearing in the user's social media feeds.[76] As a digital strategist explained: "At a marketing level, people (...) start 'sticking' cookies to you from when you turn on the computer to when you turn it off."[76] During the 2019 municipal elections, the so-called "Kontacto case" raised concerns over the irregular collection and processing of personal data to benefit election campaigns.[77] Cuestión Pública—a Colombian investigative media outlet—and Qurium—a Swedish civil society organization dedicated to safe hosting and defense of digital rights—investigated irregularities in the Colombian city of Pereira. They found that in 2019, city officials were caught entering citizens' data into an app called Kontacto, created specifically for the purpose of recording data on voters and their voting intention.[77] The data was used to benefit the incumbent's campaign in the mayoral election, who went on to win the election in October 2019. However, the following year the Risaralda Contentious Administrative Court partly rescinded the act declaring the candidate as a winner based on the information revealed about the Kontacto case.[68] They found that the influencing voters through the app had undermined their fundamental right to vote freely. The court furthermore referred the case for investigation by the data protection authority in Colombia.[68]



References

1. Kenya: Beijing's Global Media Influence 2022 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/kenya/beijings-global-media-influence/2022
2. Gibney, M., Cornett, L., Wood, R., Haschke, P., Arnon, D., Pisanò, A., Barrett, G., & Park, B. (2022). The Political Terror Scale 1976-2021. The Political Terror Scale. https://www.politicalterrorscale.org/
3. Human Rights Watch. (2017). Kenya: Post-Election Killings, Abuse. Human Rights Watch. https://www.hrw.org/news/2017/08/27/kenya-post-election-killings-abuse
4. The Associated Press. (2008). U.N.: 600,000 Displaced In Kenya Unrest. CBS News. https://web.archive.org/web/20110512055609/http:/www.cbsnews.com/stories/2008/02/11/world/main3815702.shtml
5. Jacobs, A. (2011). Nairobi burning: Kenya's post-election violence from the perspective of the urban poor. Peace Research Institute Frankfurt. https://www.ssoar.info/ssoar/handle/document/31995
6. Kenya: Freedom in the World 2023 Country Report. (n.d.). Freedom House. Retrieved November 7, 2023, from https://freedomhouse.org/country/kenya/freedom-world/2023
7. World Bank. (2024). Individuals using the Internet (% of population)—Kenya. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=KE
8. Crabtree, J. (2018). Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections. CNBC. https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html
9. BBC. (2018). Cambridge Analytica's Kenya election role "must be investigated." BBC News. https://www.bbc.com/news/world-africa-43471707
10. Mutung'u, G. & Tactical Technology Collective. (2018). The Influence Industry: Data and Digital Election Campaigning in Kenya. Tactical Technology Collective. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf
11. Privacy International. (2018). Voter profiling in the 2017 Kenyan election. Medium. https://medium.com/@privacyint/voter-profiling-in-the-2017-kenyan-election-8d9ac1e52877
12. Wafula, P. (n.d.). Election-related violence the biggest worry for kenyans in 2017. Standard Media. https://www.standardmedia.co.ke/article/2000228493/election-related-violence-the-biggest-worry-for-kenyans-in-2017
13. Amnesty International. (2017). Kenya: Police killed, beat post-election protesters. Amnesty International. https://www.amnesty.org/en/latest/press-release/2017/10/kenya-police-killed-beat-post-election-protesters/
14. McKay, G. (2022). Disinformation and Democratic Transition: A Kenyan Case Study. Stimson Center. https://www.stimson.org/2022/disinformation-and-democratic-transition-a-kenyan-case-study/
15. Ramadhan, S., & Murimi, B. (2022). Social media role in political disinformation, smear campaigns. The Star. https://www.the-star.co.ke/news/big-read/2022-01-18-social-media-role-in-political-disinformation-smear-campaigns/
16. Mozilla. (2021). Fellow Research: Inside the Shadowy World of Disinformation-for-hire in Kenya. Mozilla Foundation. https://foundation.mozilla.org/en/blog/fellow-research-inside-the-shadowy-world-of-disinformation-for-hire-in-kenya/
17. Kitili, J., Gitonga Theuri, & Badbess, K. (2022). Contextualising Political Advertising Policy to Political Micro-Targeting in Kenyan Elections. Center of Intellectual Property and Technology Law (CIPIT). https://cipit.org/wp-content/uploads/2023/03/Political-Advertising_compressed.pdf
18. Deck, A. (2022). Facebook and Instagram ran ads violating Kenyan election law, new report reveals. Rest of World. https://restofworld.org/2022/facebook-instagram-ads-kenya-election/
19. Global Witness. (2022). Facebook approves ads calling for ethnic violence in the lead up to a tense Kenyan election. Global Witness. https://www.globalwitness.org/en/press-releases/facebook-approves-ads-calling-ethnic-violence-lead-tense-kenyan-election/
20. Nigeria: Freedom in the World 2023 Country Report. (n.d.). Freedom House. Retrieved November 7, 2023, from https://freedomhouse.org/country/nigeria/freedom-world/2023
21. Premium Times. (2023). NigeriaDecides2023: How insecurity may affect elections - CDD. Premium Times Nigeria. https://www.premiumtimesng.com/news/top-news/583728-nigeriadecides2023-how-insecurity-may-affect-elections-cdd.html
22. Reuters. (2023). EU observers say 21 killed in Nigeria election violence. News24. https://www.news24.com/news24/africa/news/eu-observers-say-21-killed-in-nigeria-election-violence-20230320
23. Premium Times. (2023). Nigeria's 2023 elections least violent – Official. Premium Times. https://www.premiumtimesng.com/news/more-news/591965-nigerias-2023-elections-least-violent-official.html
24. Kemp, S. (2023). Digital 2023: Nigeria. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-nigeria
25. Chinedu-Okeke, C. F., & Obi, I. (2016). Social Media As A Political Platform In Nigeria: A Focus On Electorates In South-Eastern Nigeria. IOSR Journal of Humanities And Social Science, 21(11), 6–22. https://www.iosrjournals.org/iosr-jhss/papers/Vol.%2021%20Issue11/Version-1/B2111010622.pdf
26. Hassan, I., Segun, T., Tactical Tech, & Centre for Democracy and Development. (2020). Personal Data and the Influence Industry in Nigerian Elections: Data-Driven Campaigning by Formal and Informal Actors. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Data-Politics-Nigeria-CDD-Tactical-Tech.pdf
27. DCMS. (2018). Disinformation and 'fake news': Interim Report. House of Commons Digital, Culture, Media and Sport Committee. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36309.htm
28. Cadwalladr, C. (2018). Revealed: Graphic video used by Cambridge Analytica to influence Nigerian election. The Guardian. https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election
29. Ekdale, B., & Tully, M.. (2020). How the Nigerian and Kenyan media handled Cambridge Analytica. The Conversation. https://theconversation.com/how-the-nigerian-and-kenyan-media-handled-cambridge-analytica-128473

30. Cadwalladr, C. (2018). Cambridge Analytica was offered politicians' hacked emails, say witnesses. The Guardian. https://www.theguardian.com/uk-news/2018/mar/21/cambridge-analytica-offered-politicians-hacked-emails-witnesses-say
31. Kazeem, Y. (2018). Cambridge Analytica tried to sway Nigeria's last elections with Buhari's hacked emails. Quartz. https://qz.com/africa/1234916/cambridge-analytica-tried-to-sway-nigerias-last-elections-with-buharis-hacked-emails
32. Ritzen, Y. (2019). Exclusive: Facebook allowed fake news ads ahead of Nigeria vote. https://www.aljazeera.com/news/2019/2/14/exclusive-facebook-allowed-fake-news-ads-ahead-of-nigeria-vote
33. Hitchen, J., Fisher, J., Cheeseman, N., & Hassan, I. (2021). How WhatsApp influenced Nigeria's recent election—And what it taught us about 'fake news.' Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/
34. Aliyu, A., & Bankole, I. (2019). 2019 POLLS: How Israeli firm 'spread propaganda, manipulated voters on Facebook.' Vanguard News. https://www.vanguardngr.com/2019/05/2019-polls-how-israeli-firm-spread-propaganda-manipulated-voters-on-facebook-2/
35. Tactical Tech. (2023). Personal Data and the Influence Industry in Nigerian Elections. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/overview-nigeria/
36. India: Freedom in the World 2021 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/india/freedom-world/2021
37. Purohit, D. P., Kunal. (2019). Securing Democracy: Electoral Violence in India. ACLED. https://acleddata.com/2019/04/12/securing-democracy-electoral-violence-in-india/
38. Daxecker, U., & Milan, S. (2021). Political Microtargeting on Social Media in Diverse Democracies. Global Digital Cultures. https://globaldigitalcultures.org/2021/02/19/4677/
39. Majumdar, R. (2023). 52% of Indian population had internet access in 2022, says report. The Economic Times. https://economictimes.indiatimes.com/tech/technology/52-of-indian-population-had-internet-access-in-2022-says-report/articleshow/99964704.cms?from=mdr
40. Jaiswal, N., Jain, S., & Singh, P. (n.d.). Under Modi Government, VIP Hate Speech Skyrockets—By 500%. NDTV. https://www.ndtv.com/india-news/under-narendra-modi-government-vip-hate-speech-skyrockets-by-500-1838925
41. Sahoo, N. (2020). Mounting Majoritarianism and Political Polarization in India - Political Polarization in South and Southeast Asia: Old Divisions, New Dangers. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/08/18/mounting-majoritarianism-and-political-polarization-in-india-pub-82434
42. Iyengar, R. (2019). India's last election saw social media used as a tool. This one may make it a weapon. CNN Business. https://edition.cnn.com/2019/03/11/tech/india-election-whatsapp-twitter-facebook/index.html
43. Gowen, A., & Dwoskin, E. (2018). Why WhatsApp may present a greater challenge to democracy than Facebook—The Washington Post. The Washington Post. https://www.washingtonpost.com/world/asia_pacific/why-whatsapp-may-present-a-greater-challenge-to-democracy-than-facebook/2018/05/14/11124fea-5630-11e8-a6d4-ca1d035642ce_story.html?noredirect=on
44. Burgess, M. (2018). To fight fake news on WhatsApp, India is turning off the internet. Wired UK. https://www.wired.co.uk/article/whatsapp-web-internet-shutdown-india-turn-off
45. Wright, G. (2020). Robocalls and Mobile Texting: Automated campaign outreach. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/robocalls-texting/
46. You, J. (2015). Democracy, Inequality and Corruption. Cambridge University Press.
47. Hicken, A., Leider, S., Ravanilla, N., & Yang, D. (2015). Measuring Vote-Selling: Field Evidence from the Philippines. The American Economic Review, 105(5), 352–356. https://doi.org/10.1257/aer.p20151033
48. Philippines: Freedom in the World 2023 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/philippines/freedom-world/2023
49. World Bank. (2024). Individuals using the Internet (% of population)—Philippines. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=PH
50. OOSGA Analytics. (2023). Social Media in Philippines—2023 Stats & Platform Trends. https://oosga.com/social-media/phl/
51. Barredo, J. M. B., & Ardivilla, J. S. P. (2018). The Curious Case of Vox Populi 2.0: ASEAN's Complicated Romance with Social Media. Perspectives: Political Analyses and Commentary, 6. https://th.boell.org/sites/default/files/perspectives_-_asia_6_-_en.pdf
52. Lanuza, J. M., Ong, J. C., & Tapsell, R. (2019). Evolutions of "Fake News" from the South: Tracking Disinformation Innovations and Interventions between the 2016 and 2019 Philippines Elections. Harvard University Disinformation in Comparative Perspective Workshop. https://cyber.harvard.edu/sites/default/files/2019-11/Comparative%20Approaches%20to%20Disinformation%20-%20Jose%20Mari%20Hall%20Lanuza%20Slides.pdf
53. Elemia, C. (2022). In the Philippines, a Flourishing Ecosystem for Political Lies. The New York Times. https://www.nytimes.com/2022/05/06/business/philippines-election-disinformation.html
54. Ong, J., Tapsell, R., & Curato, N. (2019). Tracking Digital Disinformation in the 2019 Philippine Midterm Election. New Mandala. www.newmandala.org/disinformation
55. Silverman, C. (2019). "Patient Zero": The Philippines Offers A Preview Of The Disinformation Tactics The US Could See In 2020. BuzzFeed News. https://www.buzzfeed.com/craigsilverman/2020-philippines-disinformation
56. Brazil: Freedom in the World 2023 Country Report. (n.d.). Freedom House. Retrieved November 7, 2023, from https://freedomhouse.org/country/brazil/freedom-world/2023
57. World Bank. (2024). Individuals using the Internet (% of population)—Brazil. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BR
58. Mari, A. (2022). WhatsApp Picks Brazil To Launch In-App Business Directory And Shopping. Forbes. https://www.forbes.com/sites/angelicamarideoliveira/2022/11/17/whatsapp-picks-brazil-to-launch-in-app-business-directory-and-shopping/

59. Evangelista, R., & Bruno, F. (2019). WhatsApp and political instability in Brazil: Targeted messages and political radicalisation. Internet Policy Review, 8(4). https://policyreview.info/articles/analysis/whatsapp-and-political-instability-brazil-targeted-messages-and-political
60. Avelar, D. (2019). WhatsApp fake news during Brazil election 'favoured Bolsonaro.' The Guardian. https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests
61. Ozawa, J. V. S., Woolley, S. C., Straubhaar, J., Riedl, M. J., Joseff, K., & Gursky, J. (2023). How Disinformation on WhatsApp Went From Campaign Weapon to Governmental Propaganda in Brazil. Social Media + Society, 9(1). https://doi.org/10.1177/20563051231160632
62. Chile: Freedom in the World 2023 Country Report. (n.d.). Freedom House. Retrieved November 7, 2023, from https://freedomhouse.org/country/chile/freedom-world/2023
63. The World Bank. (2021). Individuals using the Internet (% of population)—Latin America & Caribbean. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZJ
64. World Bank. (2024). Individuals using the Internet (% of population)—Chile. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CL
65. NapoleonCat. (2021). Facebook users in Chile—January 2021. https://napoleoncat.com/stats/facebook-users-in-chile/2021/01/
66. Rennó, R. (2018). Chile: Voter Rolls and Geo-targeting. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/overview-chile/
67. Guttmann, A. (2023). Chile: Reliance on WhatsApp as news source 2022. Statista. https://www.statista.com/statistics/982032/whatsapp-usage-for-news-consumption-chile-age-group/
68. Monteiro, A. P. L., Tavares, C., Borges, E., Cruz, F. B., & Massaro, H. (2021). Missing Bridges—A comparative analysis of legal frameworks governing personal data in political campaigning in Latin America. InternetLab. https://internetlab.org.br/wp-content/uploads/2021/02/Missing-bridges-2.pdf
69. Garrido, R. (2018). Datos personales e influencia política en Chile. Fundación Datos Protegidos. https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf
70. CIPER Team. (2018). Instagis: El "gran hermano" de las campañas políticas es financiado por Corfo. piensaChile. https://piensachile.com/2018/01/09/instagis-gran-hermano-las-campanas-politicas-financiado-corfo/
71. Saleh, F. (2019). Instagis, la Cambrigde Analytica chilena: Empresa de big data favorita del Presidente Piñera opera al límite de la ley. El Mostrador. https://www.elmostrador.cl/destacado/2019/10/01/instagis-la-cambrigde-analytica-chilena-empresa-de-big-data-favorita-del-presidente-pinera-opera-al-limite-de-la-ley/
72. Rodríguez, D. (2021). Data protection and cybersecurity laws in Chile. CMS Legal Services. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/chile
73. Colombia: Freedom in the World 2023 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/colombia/freedom-world/2023
74. World Bank. (2024). Individuals using the Internet (% of population)—Colombia. World Bank Open Data. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CO
75. Reuters Institute. (n.d.). Colombia | Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023/colombia
76. Bashyakarla. (2019). Third-Party Tracking: Cookies, beacons, fingerprints and more. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/third-party-tracking/
77. Qurium Media Foundation. (2019). Kontacto—an insecure mobile app to track voters in Colombia. https://www.qurium.org/alerts/kontacto-an-insecure-mobile-app-to-track-voters-in-colombia/

5 Context-specific factors that may impact the effects of PMT

An analysis aiming to understand the role of PMT in a local context and any plans for regulation should consider certain context- and country-specific factors that can influence the impacts of PMT practices and the risks they may pose. Specifically, this Chapter will discuss the role of: 1) General education, digital skills, and critical media literacy; 2) Societal cleavages, inequalities, and polarization; 3) Connectivity and access to information; 4) Legal and regulatory frameworks; and 5) Strength and resilience of democratic institutions.

While these factors may be more pronounced in low- and middle-income countries, they can certainly be expected to play a role in high-income countries as well. For example, the US doesn't have a federal privacy law; critical media literacy is quite low in certain parts of societies across Europe;[1] and no country in the world is flawless in regard to media freedom.[2]

5.1 General education, digital skills, and critical media literacy

Education is crucial to be able to identify, interpret, and reflect on advertising content such as PMT. Various types of education or skills are relevant, and chief among them are digital skills and critical media literacy—with an increasing relevance of AI literacy, in particular. Incomplete understanding and insufficient voter education have been identified to constitute some of the key factors increasing vulnerability to disinformation and shaping the information environment around elections.[3] Accordingly, the OECD Development Co-operation Report 2021 states that the "negative impacts of persuasive technologies on individuals and societies are likely to be higher in contexts with lower digital skills".[4] Where critical thinking skills and media literacy skills are missing, it is very challenging for an individual to distinguish between true, false, and deliberately misleading information.[3] In fact, high-performing democracies tend to feature fewer instances of disinformation than those who perform around the middle of the range mainly owing to stronger command of digital literacy skills.[3]

Certain kinds of skills and knowledge can be particularly helpful for one to be able to recognize and make an informed decision on PMT. For instance, knowledge about politics and subjective persuasion knowledge[xvii] predicted scepticism toward PMT in a sample of voters from the US.[5] A study found that digital literacy predicted the ability to evaluate accuracy of headlines and the ability to distinguish between truth and fabrication.[6] Our review of PMT in India found that WhatsApp users in the country tend to command lower digital skills and therefore are more vulnerable to PMT (see Chapter 4.2.1)—a finding that also resonates in the Nigerian context.[7] Accordingly, the promotion of civic education (including media literacy) has been proposed as a measure to counter the risks of PMT.[8]

Education is crucial to be able to identify, interpret, and reflect on advertising content such as PMT. Various types of education or skills are relevant, and chief among them are digital skills and critical media literacy – with an increasing relevance of AI literacy, in particular.

Significant gaps exist in the attainment of general education, digital skills, and critical media literacy in many regions, countries, and demographic groups, especially in the Global South.[9,10] The increasingly fast pace of technological advance exacerbates the problem, as those with fewer skills struggle to catch up with new developments. While many African countries have ICT master plans and blueprints, for instance, they often don't focus on digital skills, tend to lack operational details, and fail to sufficiently steer policy development and investments, which has led to uncoordinated and ineffective initiatives.[11] To be able to grasp and address the risks of PMT and other forms of online manipulation, not only regular citizens, but also policymakers require training in these skills.

At the same time, it needs to be understood that, despite its importance, education alone is not a sufficient solution and should certainly not be thought of as a silver bullet. Given the opacities and complexities of PMT and human limitations (e.g., time constraints, cognitive biases, service dependence, limited bargaining power), education remains a key piece of the puzzle, but it is not sufficient on its own.

[xvii] Subjective persuasion knowledge refers to "an individual self-assessment or perception about how persuasion works". Please see Nelson et al.[5] for further detail.

5.2 Societal cleavages, inequalities, and polarization

As Chapter 3.2.10 has outlined, PMT can amplify and reinforce existing societal cleavages. When a country has pre-existing polarization, inequality, discrimination, or social tensions, the use of PMT may be more likely to aggravate such harmful tendencies. While a certain amount of polarization is part of a healthy democracy,[12] PMT may lead to a downwards spiral of polarization whereby voters reinforce their beliefs and become less likely to engage with contending views. Indeed, countries with a more polarized electorate may be more negatively affected by disinformation.[3]

Tensions and violent conflicts stemming from political divisions drawn across ethnic, cultural, or religious lines are particular risk factors for enhanced effects of PMT. Kenya[xviii] and Nigeria[xix], which were discussed in the previous chapter, offer examples where PMT has fuelled widespread protests and violence which often have an ethnic basis. In India, PMT campaigns often exploit pre-existing tensions between Hindus and Muslims.[13]

Political polarization may be further fuelled by economic inequality. Political polarization has been found to be higher in contexts of economic decline or increasing inequality,[14] in particular income inequality.[15] The Middle East and North Africa rank as the most unequal regions in the world,[16] and given that many countries in both regions feature significant social cleavages, it may be particularly important to aim to reduce the polarizing impacts of PMT in these regions.

Voter turnout may also affect political polarization. Where low voter turnout wipes away a significant share of the votes, political campaigns tend to adopt a more assertive tone, as they are not trying to convince undecided voters or voters of rival parties but will simply rally like-minded partisans to vote.[17] Turnout rates vary widely between countries,[18] but the global average started dropping in the 1990s and is not showing signs of recovery.[19]

Addressing economic inequality is a multidimensional and long-term process. While it is unrealistic to totally remove social cleavages, democracies stand to benefit from closer monitoring of political polarization and the implementation of countermeasures. Among other things, this will improve their resilience against deceptive and manipulative campaign practices.

5.3 Connectivity and access to information

Given that most forms of PMT are delivered through the Internet or mobile communication channels, the impacts of PMT are underpinned by the availability and quality of Internet/mobile connectivity and the penetration of digital devices. In countries where connectivity is high and digital devices are widely available, PMT can reach large audiences and utilize more data on citizens (i.e., collected through mobile apps, social media, and web tracking) for ad targeting.

Less reliable infrastructure, lower capacities within the electric grid, as well as lower levels of Internet and digital device penetration may explain why PMT has been adopted only recently in many countries, especially in the Global South. With global Internet usage rapidly rising, the prevalence of PMT will also likely continue to grow. In Sub-Saharan Africa, for instance, data-driven campaigning has played a smaller role vis-à-vis traditional rallies and billboards, but it is becoming more widespread.[20] These changes will result in large populations with minimal previous experience in using digital technologies being exposed to PMT—a prospect that warrants keen policy action.

With global Internet usage rapidly rising, the prevalence of PMT will also likely continue to grow.

At the same time, reduced access to the Internet (e.g., due to infrastructure constraints or politically motivated Internet shutdowns[xx]) signifies fewer opportunities to exercise critical media literacy as fact-checking services and consuming a diverse range of media may simply not be attainable. This is another factor making citizens of poorer countries more vulnerable to the negative effects of PMT. For example, in the Philippines, the Internet is often slow and unreliable, making social media sites—which are optimized for accessibility and low connectivity—“a prime platform for swaying public opinion”.[24]

Digital transformation and growing Internet penetration are largely positive trends, which should not be hampered for fears of PMT. However, an analysis of the role and influence of PMT in a Global South context and any processes to design context-appropriate measures for regulating PMT would benefit from considering the state of connectivity and access to digital devices.

[xviii] See Chapter 4.1.1

[xix] See Chapter 4.1.2

[xx] Repressive governments often use Internet shutdowns and the blocking or filtering of online services in the context of political instability, protests, and elections to make access to information more difficult, restrict the right to freedom of expression and assembly, and limit the scope of action of opposition parties and civil society – thus, ultimately, as a tool to evade accountability.[21] In 2022 alone, access to Internet services were restricted 187 times by a record number of 35 countries.[22] Since 2015, at least 71 countries worldwide have blocked or restricted access to social networks.[23]

5.4 Legal and regulatory frameworks

The regulatory framework governing political advertising largely shapes how the potentially harmful impacts of PMT will unfold. While there are major regulatory developments, for instance in the European Union, in many countries—especially in the Global South—there is little or no regulation in place to govern data-driven political campaigning (see Chapter 6.1).

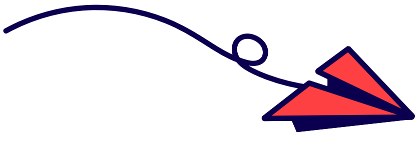
Beyond PMT-specific laws and policies, there are other types of regulation that may impact PMT, however most of these instruments do remain relatively underdeveloped in much of the Global South as well as in some parts of the Global North. Campaign finance laws govern the funding of political campaigns, including any funds used towards advertising and messaging. These laws may obligate political campaigns to share donor and expenditure information and may restrict the kinds of funding instruments that are permitted to be deployed. Ad content rules (see Chapter 6.4.1) regulate areas such as misinformation (see, for instance, Poynter's Global map of anti-misinformation actions[25]), hate speech (see, for instance, the Global Handbook on Hate Speech Laws[26]), and discrimination. Data protection laws govern the collection, use, and storage of personal data, including the kind of data that is used in PMT. These laws may obligate political campaigns to obtain consent from the voters before collecting their data and to share clear information on the use of the collected data. They may also require the introduction of appropriate security measures to safeguard the collected data from disclosure or unauthorized access. PMT can be restricted through strong data protection laws that make the practice challenging and costly. A prevalence of data leaks and a thriving black market for personal data, on the other hand, can undermine data protection efforts. Many countries, especially in the Global South, have weak or non-existent privacy laws,[27] meaning that political actors can access and use personal data of the electorate without much oversight or restriction.[28] For instance, cases from Sub-Saharan Africa have shown that there was little public scrutiny of how political candidates got access to phone numbers of individual voters.[20] Chapter 6.4 of this report will explore options to regulate PMT and their respective advantages and limitations. While the development of legal and regulatory frameworks is important, their effectiveness can only be secured by effective enforcement (see Chapter 6.5.3).

5.5 Strength and resilience of democratic institutions

The strength and resilience of the democratic institutions are key in determining the impact that PMT can deliver. Where democratic institutions are weak, and the media freedom and independence is not guaranteed, the level of oversight and accountability may be compromised making the country vulnerable to misuse of PMT and other forms of manipulation.[8] Indeed, disinformation cases have been found to deliver more harm to countries with weaker democratic institutions.[3] The democratic decline is making many countries more vulnerable and a cynical, resigned, and apathetic electorate is ripe ground for PMT.[29] There is much diversity between the democratic regimes around the world, and many countries in the Global South are more correctly classified electoral autocracies than liberal democracies, meaning that the democratic institutions are rather imitative and violate liberal democratic norms.[30]

Where democratic institutions are weak, and the media freedom and independence is not guaranteed, the level of oversight and accountability may be compromised making the country vulnerable to misuse of PMT.

As noted in the previous subchapter, for the legal and regulatory frameworks to be effective, enforcement is required. Where a country has a high rule of law, they also have high capacity to enforce legal instruments, such as anti-disinformation laws.[31] On the other hand, electoral manipulation and fraud are more likely to take place in countries with a weak rule of law.[32–34] Indeed, the lack of punitive consequences and lack of enforcement have been found to be a factor driving disinformation.[3] The Rule of Law Index—which incorporates estimates on government powers, corruption, and regulatory enforcement—shows that there are significant differences in these capacities between the Global North and the Global South.[35] An example for insufficient enforcement capacity is the Kenyan Data Protection Authority, which has been criticized as underfunded, understaffed, inefficient and not truly independent.[36]



References

1. Feldman, S. (2019). Infographic: Media Literacy Is Not a Given in Europe. Statista Daily Data. https://www.statista.com/chart/18117/media-literacy-in-europe
2. Reporters Without Borders. (2023). RSF's World Press Freedom Index. https://rsf.org/en/index
3. International IDEA. (2022). The Information Environment around Elections. https://www.idea.int/our-work/what-we-do/elections/information-environment-around-elections
4. Kumpf, B., & Hanson, A. (2021). Reshaping social media: From persuasive technology to collective intelligence. In Development Co-operation Report 2021: Shaping a Just Digital Transformation. OECD. https://doi.org/10.1787/ce08832f-en
5. Nelson, M. R., Ham, C. D., & Haley, E. (2021). What Do We Know about Political Advertising? Not Much! Political Persuasion Knowledge and Advertising Skepticism in the United States. Journal of Current Issues & Research in Advertising, 42(4), 329–353. https://doi.org/10.1080/10641734.2021.1925179
6. Sirlin, N., Epstein, Z., Arechar, A. A., & Rand, D. G. (2021). Digital literacy is associated with more discerning accuracy judgments but not sharing intentions. Harvard Kennedy School Misinformation Review. https://misinforeview.hks.harvard.edu/wp-content/uploads/2021/12/sirlin_digital_literacy_20211206.pdf
7. Hitchen, J., Fisher, J., Cheeseman, N., & Hassan, I. (2021). How WhatsApp influenced Nigeria's recent election—And what it taught us about 'fake news.' Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/
8. Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs. https://www.ssrn.com/abstract=3409279
9. Roser, M., & Ortiz-Ospina, E. (2016). Global Education. Our World in Data. https://ourworldindata.org/global-education
10. Wiley. (2021). Global Rankings for Digital Skills. Wiley. https://dsgi.wiley.com/global-rankings/
11. World Bank. (2021). Digital Skills: The Why, the What and the How—Methodological Guidebook V 2.0. World Bank.
12. Milačić, F. (2021). The Negative Impact of Polarization on Society. Friedrich Ebert Stiftung. https://library.fes.de/pdf-files/bueros/wien/18175.pdf
13. Daxecker, U., & Milan, S. (2021). Political Microtargeting on Social Media in Diverse Democracies. Global Digital Cultures - University of Amsterdam. https://globaldigitalcultures.uva.nl/projects/daxecker.html
14. Stewart, A. J., McCarty, N., & Bryson, J. J. (2020). Polarization under rising inequality and economic decline. Science Advances, 6(50), eabd4201. https://doi.org/10.1126/sciadv.abd4201
15. Gu, Y., & Wang, Z. (2022). Income Inequality and Global Political Polarization: The Economic Origin of Political Polarization in the World. Journal of Chinese Political Science, 27(2), 375–398. https://doi.org/10.1007/s11366-021-09772-1
16. World Inequality Lab. (2021). The World Inequality Report 2022 presents the most up-to-date & complete data on inequality worldwide. World Inequality Report 2022. https://wir2022.wid.world/
17. Rosenberg, M. (2019). The root causes of political polarization—Doing Business on the Earth. IESE Business School. https://blog.iese.edu/doing-business/2019/11/25/the-root-causes-of-political-polarization/
18. Our World in Data. (2023). Voter turnout. Our World in Data. https://ourworldindata.org/grapher/voter-turnout
19. Solijonov, A. (2016). Voter Turnout Trends around the World. International Institute for Democracy and Electoral Assistance. https://www.idea.int/sites/default/files/publications/voter-turnout-trends-around-the-world.pdf
20. Macintyre, A. (2020). The Imports and Exports of Sub-Saharan Africa's Influence Industry. https://medium.com/@Info_Activism/the-imports-and-exports-of-sub-saharan-africas-influence-industry-d189a7bb9edf
21. Global Partners Digital & Access Now. (2023). Evading accountability through internet shutdowns: Trends in Africa and the Middle East. https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf
22. Skok, Z. R., Felicia Anthonio, Sage Cheng, Carolyn Tackett, Alexia. (2023). Internet shutdowns in 2022: The #KeepItOn Report. Access Now. https://www.accessnow.org/internet-shutdowns-2022/
23. Armstrong, M. (2022). Infographic: Where Social Media is Suppressed. Statista Daily Data. https://www.statista.com/chart/23804/countries-blocking-social-media
24. Azeez, W. (2021). Google bans political ads ahead of elections in the Philippines | CNN Business. CNN. https://www.cnn.com/2021/12/01/tech/google-political-ad-ban-philippines/index.html
25. Poynter. (2023). Global map of anti-misinformation actions. https://www.poynter.org/ifcn/anti-misinformation-actions/
26. The Future of Free Speech. (2020, November 20). Global Handbook on Hate Speech Laws. The Future of Free Speech. https://futurefreespeech.com/global-handbook-on-hate-speech-laws/
27. UNCTAD. (2021). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
28. DLA Piper. (2023). DLA Piper Global Data Protection Laws of the World: Compare data protection laws around the world. DLA Piper. https://www.dlapiperdataprotection.com/
29. Gadjanova, E. (2018). Democracy in decline in Africa (MaxPlanckResearch - Digital Society). https://www.mpg.de/12605295/W001_Viewpoint_012-017.pdf
30. Our World in Data. (2023). Political regime. Our World in Data. https://ourworldindata.org/grapher/political-regime
31. Tan, N. (2020). Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia. Election Law Journal: Rules, Politics, and Policy, 19(2), 214–239. https://doi.org/10.1089/elj.2019.0599
32. Birch, S., & Carlson, J. (2012). Electoral Integrity Framework Project. Creative Associates International. https://aceproject.org/electoral-advice/archive/questions/replies/531723839/52093951/Creative-Electoral-Integrity-Framework-Project.pdf

33. Fortin-Rittberger, J. (2014). The role of infrastructural and coercive state capacity in explaining different types of electoral fraud. Democratization, 21(1), 95–117. https://doi.org/10.1080/13510347.2012.724064
34. Simpser, A. (2013). Why Governments and Parties Manipulate Elections: Theory, Practice, and Implications. Cambridge University Press. https://doi.org/10.1017/CBO9781139343824
35. World Justice Project. (2023). WJP Rule of Law Index. World Justice Project. https://worldjusticeproject.org/rule-of-law-index
36. Andere, B. (2021). Data Protection in Kenya: How is this Right protected?. Access Now. https://www.accessnow.org/wp-content/uploads/2021/10/Data-Protection-in-Kenya.pdf

6 Regulating PMT

Previous chapters of this report have underlined that PMT increasingly demands policy attention. While most countries still have no comprehensive legislation in place to address PMT, efforts to regulate and legislate around the phenomenon are fast emerging around the world. This chapter first provides examples of recent regulatory developments both in the Global South and the Global North. It then offers an overview of policy options for regulating PMT and discusses their respective advantages, limitations, and challenges. The chapter concludes with considerations on key issues affecting the policy options to manage PMT.

6.1 Recent regulatory developments

The regulation of political ads and PMT in particular is gaining a lot of traction globally. As discussed in Chapter 5.4, many kinds of laws have the potential to bear an impact on PMT. However, currently, across most jurisdictions, there is a clear lack of suitable regulation to address PMT. Existing regulations largely focus on political advertising taking place in traditional media outlets and have not been sufficiently adapted to the online media environment, where political ads can be delivered in a highly personalized manner and algorithms show users prioritized content that they predict will keep them engaged on social media platforms.[1,2]

Yet, the challenges are even more fundamental. For instance, many jurisdictions do not have a functioning data protection regime. According to UNCTAD, less than half of the least developed countries have laws in place that protect data and privacy.[3] Even where privacy laws have been implemented, enforcement is often deficient, including in the electoral context.[4] For instance, the US also do not have a federal privacy law, leaving companies relatively free to decide how they collect and use personal data.[5]

Despite a widespread lack of comprehensive regulation to govern PMT, there are promising regulatory developments in both the Global South and the Global North, some of which will be highlighted in the following for illustration purposes.

South Africa: General law that applies to PMT through sections on direct marketing and unsolicited electronic communications
The South African Information Regulator has produced a legal document entitled "Guidance note on the processing of personal information of a voter by a political party in terms of the Protection of Personal Information Act", which offers guidance around the scope and way in which the Protection of Personal Information Act of 2013 (POPIA) applies in relation to political parties.[6] For instance, the guidance note decrees that political parties must respond to voters enquiring whether their personal information is being processed upon request, and that political parties cannot process personal information about voters if voters object.

Philippines: Partial ban on PMT
In light of the 2022 elections, the Philippine's Commission on Elections (COMELEC) banned electoral candidates from using microtargeted electoral ads. It further required electoral posts to display a disclosure that identifies the ad as having been paid for an electoral purpose and discloses the political actor who paid for the ad within its Resolution No. 10730.[7] In another set of guidelines, the Philippine Privacy Commission prohibits the processing of personal data that exceeds the data subjects' reasonable expectations.[8]

Panama: Political campaigning limited to certain time periods and introduction of a monitoring unit
In 2019, Panama adopted a law limiting the campaigning actions of political parties outside the electoral period.[9] In the same year, the Electoral Tribunal of Panama established a special unit to monitor political parties' online activities in particular on X (formerly Twitter) and Facebook.[9] Where the unit detected a breach of electoral legislation (for instance campaigning outside the electoral period), it cooperated with the respective platform to take action. The unit also engaged citizens by creating channels to detect disinformation, for instance through a designated WhatsApp chat. During the 2019 national election, the unit detected various foreign-based malicious operations which intended to manipulate the political debate.[9]

Kenya: Bulk messaging ban
In 2017, the Communications Authority of Kenya adopted guidelines preventing bulk messaging by political actors,[10] intending to limit hate speech and

incitement of violence. While these guidelines do not specifically address or define PMT, some aspects help with regulating the practice.[11] With the implementation of the Data Protection Act in 2019, Kenya became the third country in East Africa to implement significant data protection legislation.[12] While creating a substantial legal framework for data protection that requires the data subject's consent for the practices involved in PMT, an analysis of the Act finds that it provides for several exceptions that create loopholes for data collection and processing. Therefore, its efficacy in curtailing PMT depends on the interpretation of the parties involved and thus, does not constitute a safeguard for voter protection.[13] However, areas such as the use of personal data in PMT are not covered in any legislation and need to be addressed.[11]

United States: First Amendment as an obstacle to regulating PMT

Owing to the First Amendment, which guarantees the protection of free speech, the government is generally not able to regulate speech based on its content. Consequently, without a substantial change to the Bill of Rights, regulating PMT would be very difficult.[14] In 2021, the Banning Microtargeted Political Ads Act (BMPAA) was proposed by a Representative of the Democratic Party in the US Congress. Applying to all forms of electioneering communication and advocacy, the bill aims to prohibit the use of demographic or behavioral data use for political advertisement on online platforms. However, even in the unlikely scenario of Congress passing this bill, the Supreme Court is expected to strike it down as unconstitutional.[15]

European Union (EU): Regulation on political ads and a Code of Practice on disinformation

As part of the European Democracy Action Plan (EDAP), the European Commission published a legislative proposal in 2021 directed towards "transparency and targeting of political advertising". In November 2023, EU Parliament, Council and Commission reached an agreement on the proposal. It encompasses a legal definition of political ads, and institutes transparency requirements such as mandatory labels and reporting obligations that are backed by possible sanctions. It also includes a ban on targeting techniques that use sensitive personal data (cf. Article 9 GDPR).[16] Additionally, a rule is foreseen that prohibits all political advertising from third country entities in the three months before an election or referendum.[17] In November 2023, EU Parliament, Council and Commission reached an agreement on the proposal. However, some experts doubt the results' overall impact and demand further reaching rules.[18]

The 2022 Code of Practice on Disinformation offers a rulebook of "commitments" to address the harms of disinformation which was initially introduced in 2018 as a form of voluntary self-regulation. Signatories included Big Tech firms such as Google, Meta, Microsoft, Twitch, and TikTok.[19] In May 2023, the Commissioner for Internal Market, Thierry Breton, announced that X withdrew from the Code of Practice following Elon Musk's takeover.[20] Acting on disinformation is now mandatory under the EU's Digital Services Act (DSA), which entered into effect in August 2023 for very large online platforms.[21]

Other examples

In Canada, the Elections Modernization Act of 2018 introduced new transparency rules such as spending caps and disclosure requirements that apply to elections and regulate electoral ads by third parties on platforms including Facebook, Google and X.[11] Furthermore, in the same year, added provisions to the Canada Elections Act (CEA) introduced a publicly available online database that includes all political ads published on online platforms.[22,23]

In Singapore, the Code of Practice for Transparency of Online Political Advertisements (2019) requires digital advertising and Internet intermediaries to enhance transparency of online political ads.[11] Additionally, according to Singapore's Protection from Online Falsehoods and Manipulation Act (2019), it is an offense to spread a false statement that is "likely" to impact the results of an election or a referendum, instigate enmity, hatred, or ill-will among population groups, or undermine public trust in the Singapore government or its agencies.[24]

In Australia, it has been criticized that there are "very few restrictions on political advertising", especially when it comes to the content of political ads: truth is not a requirement.[25] However, the concept of truth is hard to grasp or even legally define, and the latter poses the risk of misuse by authoritarian regimes.[26] This complicates the regulation of disinformation and PMT, as Chapter 6.5.1 describes in more detail.

6.2 Scope of regulation

Political advertising regulation can be designed as content-based or content-neutral. Content-neutral legislation refers to rules that apply to all types of advertising regardless of their content or message. This can include, for example, general transparency obligations or general data protection rules. Content-based legislation, on the other hand, applies only to specific types of advertising, for instance, exclusively to political advertising or even specifically to PMT. The advantage of this approach is that rules can be tailored to the specific risks and requirements of regulating political campaigning. The main challenge introduced by this approach is defining the material scope: What should legally qualify as political advertising and what not?

Legally defining "political advertising"

In many cases, it is evident that an ad is political (e.g., a campaign ad of a political party in a national election).

In other cases, however, this is much less clear (e.g., an influencer promoting a political party; an NGO advocating a political stance or social cause; an online post by a political party that is shared by social media users). Choosing a definition is ultimately also a political decision and intense debates have erupted over recent proposals.[27] We suggest considering the aspects described below when legally defining a "political ad":[xxi]

- **Media:** Messages can be classified based on the media channels used for dissemination (e.g., TV, radio, streaming service, social media).
- **Timing:** Messages can be classified based on when they are posted (e.g., around an election period, around other key political events, anytime).
- **Content/purpose:** Messages can be classified based on their purpose or content (e.g., electoral advertising directly promoting a political party or candidate; messages on pending legislation; corporate social responsibility; ads on social issues, such as abortion, environmental protection, gun laws, and LGBTQIA+).
- **Advertiser:** Messages can be classified based on the individual or organization trying to disseminate them (e.g., political party, social media influencer, private individual).
- **(Expected) effect:** Messages can be classified based on the effect they have—or are expected to have—on individuals and society (e.g., potential to influence the outcome of an election).
- **Paid vs. unpaid:** Messages can be classified based on the cost they incur for the advertiser, if any.

Legally defining "political advertising" is a delicate task.

Importantly, any legal definition of political advertising as well as the associated rules and enforcement structures need to be carefully weighed against threats to freedom of expression.

To build a legal definition, it is possible and appropriate to combine multiple of the above criteria. For instance, an upcoming EU regulation includes the following definition:[29]

> *'political advertising' means the preparation, placement, promotion, publication, delivery or dissemination, by any means, of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign: (a) by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or (b) which is liable and designed to influence the outcome of an election or referendum, a voting behaviour or a legislative or regulatory process, at Union, national, regional or local level.*
>
> *It shall not include: (a) messages from official sources of Member States or the Union that are strictly limited to the organisation and modalities for participation in elections or referendums, including the announcement of candidacies or the question put to the referendum, or for promoting participation in elections or referendums; (b) public communication aiming to provide official information to the public by, for or on behalf of any public authority of a Member State or of the Union, including members of Government, provided they are not liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process; (c) presentation of candidates in specified public spaces or in the media which is explicitly provided by law and allocated free of charge while ensuring equal treatment.*

Legally defining "political advertising" is a delicate task. All approaches have advantages and downsides (e.g., level of subjectivity, complexity in implementation, potential loopholes, adaptability to evolving technological landscape). Importantly, any legal definition of political advertising as well as the associated rules and enforcement structures need to be carefully weighed against threats to freedom of expression. As will be discussed in Chapter 6.5.1, content-based rules have the potential to be (and are often) exploited by authoritarian governments as a tool for censorship and to silence political opposition.

6.2.1 Actor-specific rules

Legal rules can also be designed to differ between categories of actors. As suggested in the UN Guiding Principles on Business and Human Rights, "the scale and complexity of the means through which enterprises meet [their] responsibility may vary according to [their size and] the severity of the enterprise's adverse human rights impacts."[30] For instance, big online platforms and core political advertisers (e.g., political parties, candidates, lobby associations) could face heightened scrutiny and more restrictions than smaller platforms and political advertisers on the periphery (e.g., social media influencers, non-party campaigns).[31] The EU's Digital Services Act (DSA), for example, thus makes use of a system of tiered responsibilities to spare small platforms from excessive compliance costs. Very large online platforms, on the other hand, are expected to be able to handle this financial burden and are assessed to have the most significant impact on society.[21]

To address threats to national sovereignty—especially in countries that experience aggressive outside interference in elections—a distinction can further be made between domestic and foreign advertisers. In some cases, social media platforms have decided to ban foreign-funded political ads (e.g., Facebook in Thailand, Ireland, Nigeria, and Ukraine).[32] However, such a ban can also be imposed by law. In February 2023, the European

[xxi] Discussing all these criteria in detail is beyond the scope of this report. For a more in-depth discussion of some of the above definition approaches, see, for example, Cipers and Meyer (2022),[28] or Jaursch's 2020 report.[1]

Parliament voted in favor of banning foreign funding for political ads as part of its position on the political advertising regulation.[33]

6.3 State regulation versus corporate self-regulation

Besides the content and scope of possible regulatory responses to PMT, their form and legal bindingness can also differ. Online platforms have long been met with a liberal legal approach across the globe.[34] In some industrialized nations such as the US, this is still the case today, whereas the EU for instance is slowly starting to introduce more legal restraints to the power of Big Tech. Pioneering initiatives such as the EU's Digital Services Act (DSA) and the upcoming regulation of political advertising could serve as inspiration or even become blueprints for other regions in drawing up appropriate responses while balancing free speech considerations. It is crucial to recognize that the EU's socio-political context differs from many other regions, for example in terms of rule of law, institutional checks and balances, as well as independent journalism and civil society. Any regulation of the digital sphere must consider possible impacts on democracy and human rights with due regard to local contextual factors (see also Chapter 6.5.1).

The multifaceted risks of PMT will require a nuanced policy mix.

In the EU, the challenges faced or generated by online platforms were long addressed mainly through voluntary action by platforms. As these issues became increasingly clear and more impactful to society, self-regulatory efforts were further incentivized and formalized, for instance through the voluntary Code of Practice on Disinformation: In the form of non-binding self-commitments, pledges were made by a number of key companies to tackle disinformation.[19] When these measures turned out to be insufficient (for a discussion of the limitations of corporate self-regulation, see Chapter 6.5.2), the DSA was drafted which, in large part, makes use of a co-regulatory approach.[21] This means that, while there are certain top-down obligations such as requiring platforms to publish Terms of Service that explain how content is moderated, there are also paragraphs that prescribe an outcome but give addressees leeway in how to get there. For example, very large online platforms are required to assess and mitigate systemic risks, yet there are no specifics on the way this must be achieved. Although there will be supervision mechanisms of state actors and, in some cases, third parties, the delegation of tasks can and should be publicly scrutinized.[35]

Most of the available policy options only address a fraction of the risks associated with PMT.

One of the aims behind this approach is to adequately balance the roles and responsibilities of public versus private actors. In an area as sensitive as the regulation of speech acts, neither full control of states (risk of state censorship and abuse for political power gains, see Chapter 6.5.1) nor private actors (risk of private censorship and abuse for financial gains, see Chapter 6.5.2) are desirable outcomes. Therefore, a regulatory framework involving several stakeholders, including neutral auditors or supervisors, is advisable.[36] This is particularly relevant in face of the current state of play where platforms guard their core functionalities, including algorithms and content moderation practices, hindering full situation awareness for policymakers, users and other stakeholders.[37]

Similarly, in most contexts, when it comes to the content of regulatory measures, the multifaceted risks of PMT will require a nuanced policy mix, for which the following chapter presents several options.

6.4 Overview of policy options

This subchapter provides an overview of possible approaches to regulating PMT, including (1) **rules for shaping PMT,** (2) **transparency obligations,** (3 **user control / consent,** (4) **partial restrictions,** and (5) **a total ban.** The options are presented with their respective advantages and shortcomings. The proposed policy measures are mostly not mutually exclusive, meaning that they can be combined (e.g., it is possible to use a combination of transparency obligations, user consent, and partial restrictions of PMT).

An overview of the policy options is provided in **Table 1**. Importantly, as can be seen from the table, most of the available policy options only address a fraction of the risks associated with PMT. For instance, ensuring equal access to PMT addresses the risk of unfair competition between political actors, but nothing else. Transparency obligations may improve public scrutiny but will not fundamentally alleviate concerns around voter manipulation, discrimination, and political polarization. A legal restriction or complete ban of PMT are probably most effective in removing risks, but if not carefully designed, such measures can pose a significant threat to freedom of expression (see Chapter 6.5.1). In regulating PMT, policymakers need to strike a delicate balance between public interest and different fundamental rights.

6.4.1 Rules for shaping PMT

In countries where the practice of PMT is permitted, legal rules can be amended to ensure fair political campaigning in the online domain.

Table 1.

Regulation approach	Advantages	PMT Risks Addressed	Limitations & Challenges
Ensuring equal access to PMT → see Chapter 6.4.1.1	Can help to promote **fair competition between political actors**	**R4**	**Defining boundaries:** Challenge of defining equal access
Rules regarding ad content → see Chapter 6.4.1.2	Can help to **curb disinformation, hate speech and discrimination**	**R3, R9, R10**	**Defining boundaries:** Challenge of defining mis- and disinformation, hate speech, and discriminatory content **Balancing free speech:** Challenge of striking the right balance between regulating harmful content and preserving the principles of freedom of expression
Identity verification → see Chapter 6.4.1.3	Can help to swiftly **remove fake accounts** and **inauthentic online content**	**R2, R3**	**Enforcement:** Challenge of identifying fake accounts and inauthentic content
User-facing transparency → see Chapter 6.4.2.1	Can strengthen users' **rights awareness and basic understanding of PMT** and **help hold advertisers accountable for their messaging**	**R2** Possibly also: **R1, R3, R5**	Typically **insufficient for informed decision-making** due to complex/opaque language and information overload May instill a **false sense of security** in users Challenging for users to **verify the accuracy and completeness of the provided information** Malicious advertisers can try to **evade transparency obligations**
Public-facing transparency → see Chapter 6.4.2.2	Can **improve accountability and oversight** by enabling political opponents, the media, and civil society to engage in **fact-checking, critical analysis, and remedial counter speech**	**R2, R7** Possibly also: **R3, R5**	**Underfunded civil society** organizations have limited resources to curate and analyze publicly available data Challenge to **verify the accuracy and completeness of the provided information** Malicious advertisers can try to **evade transparency obligations** Ad libraries have been criticized for **functional limitations and usability issues** which impede the work of journalists and watchdog organizations
User control / consent → see Chapter 6.4.3	**May strengthen individual self-determination** with regard to political ads and personal data processing (Attention: this **claim is contested**),[xxii] potentially **disincentivizing privacy-intrusive advertising practices**	**R6**	Practical limitations of user control (user **decisions often not truly "free" and "informed"**) Individual privacy choices often **ignore potential impacts on overall society** **Compliance with data protection laws is typically limited**

[xxii] Due to practical limitations of this approach, it is questionable whether autonomy is really strengthened—see, for example, Kröger et al. (2021).[48]

Partial PMT restrictions (e.g., spending caps, quiet periods, limitations on types of personal data that can be used) → see Chapter 6.4.1	**Can remove part of the risks associated with PMT** (see Chapter 3.2), depending on the extent of restriction	**All risks** (to the extent of restriction)	**Limits potential benefits of PMT** (see chapter 3.1) Partial restriction **leaves room for risks of PMT** A ban of PMT **can be misused by (would-be) authoritarian governments to suppress dissent**—thus needs to be carefully designed and implemented to safeguard freedom of expression
Total PMT ban → see Chapter 6.4.4.2	**Removes all risks associated with PMT** (see Chapter 3.2)	**All risks**	**Removes potential benefits of PMT** (see chapter 3.1) A ban of PMT **can be misused by (would-be) authoritarian governments to suppress dissent**—thus needs to be carefully designed and implemented to safeguard freedom of expression

Risks:
R1) Voter manipulation and demobilization, **R2)** Lack of transparency, **R3)** Spread of disinformation, **R4)** Unfair competition between political actors, **R5)** Foreign influence, **R6)** Privacy violations, **R7)** Difficulty of public scrutiny and counter speech, **R8)** Distortion of voter model and political mandates, **R9)** Discrimination, **R10)** Political polarization

6.4.1.1 RULES TO ENSURE EQUAL ACCESS TO PMT

Regulation can be used to ensure that campaigns across the political spectrum receive equal access to PMT. This can include, for example, ensuring that platforms do not charge political parties different prices to target voters or charge higher prices to reach out to voters that have not traditionally engaged with their messages.[38] For instance, similar to the "equal time rule" that requires US radio and television broadcast stations to provide competing political candidates with equivalent access, namely the same amount of time on the same terms, commentators have proposed an "equal time rule for social media" that would require social media companies to provide opposing candidates with an option to reach the same audience.[39] To ensure that the information provided is reliable, delivering corrective information through fact-checking is a suitable option.[39]

6.4.1.2 RULES REGARDING AD CONTENT

To reduce harmful impacts of PMT, laws can regulate ad content, for example by addressing hate speech or disinformation. Many countries already have legislation that aims to restrict public speech containing harmful language, such as expressions hate or encouragement of violence towards a group or an individual, in place.[40] The UN Strategy and Plan of Action on Hate Speech defines hate speech as any kind of communication "that attacks or uses pejorative or discriminatory language with reference to a person or a group (…) based on [identity factors, such as] their religion, ethnicity, nationality, race, color, descent, gender, (…) language, economic or social origin, disability, health status, or sexual orientation".[41] In one instance, Kenya even threatened to ban Facebook because it "has been reluctant to take action to combat the spread of hate speech, propaganda and disinformation, escalating the risk of violence ahead of the elections."[42]

Across the globe, there have also been various regulatory responses to disinformation, reaching from task forces and investigations to specific bills and laws.[43,44] However, in many places, despite the risks involved, spreading disinformation in a political campaign is still legal. In the US for instance, political campaigns can intentionally misrepresent facts and mislead voters without violating any law as long as it remains domestic.[45] Regulatory responses to disinformation and investments in fact-checking capacity have several advantages—however, it is equally important to pay due regard to threats that they can pose to free speech (see Chapter 6.5.1).

Beyond general rules against hate speech and discrimination, specific rules for PMT can be put in place. Guidelines proposed by Bayer (2019), for instance, include that political ads should be "based on true information and real social needs; not based on fear, social tensions or instincts; [avoid] inciting hatred or hostility; [and avoid] ad hominem arguments (character assassination)".[46] Given the elusive nature of the concept of truth and the challenges in its legal definition, one could also evaluate political ads based on other legal criteria, such as their potential for harm.[26]

6.4.1.3 RULES REGARDING IDENTITY VERIFICATION

Platform operators can be obliged to carefully verify the identity of both political advertisers and social media accounts that reach large audiences with political or issue-based content (e.g., political candidates, political parties, NGOs, and influencers), and to swiftly remove fake accounts and inauthentic online content. Here, again, impacts on free speech need to be taken into consideration (see Chapter 6.5.1).

Advantages of using rules for shaping PMT

- **Combating disinformation:** Rules can help address the spread of disinformation by setting standards for the accuracy and truthfulness of political advertisements, reducing the potential for false or misleading information to be targeted at specific individuals or groups.
- **Curbing hate speech:** Regulations can tackle hate speech by establishing guidelines that prevent the dissemination of inflammatory, abusive or threatening content, fostering a more respectful and constructive political discourse.
- **Addressing discrimination:** Regulations can hamper certain individuals or groups from being disproportionately targeted or excluded from political campaigns, thus fostering a more democratic and inclusive political landscape.
- **Promoting fair competition:** Regulations can promote fair competition among political actors by fostering a level playing field and ensuring that campaigns compete based on ideas and policies rather than manipulative tactics.

Limitations & challenges of using rules for shaping PMT

- **Defining boundaries:** Determining what constitutes disinformation, hate speech, or fair access to ad space can be subjective and open to interpretation, leading to potential disagreements and challenges in implementation.
- **Balancing free speech:** In particular, striking an appropriate balance between regulating harmful content such as disinformation and hate speech while preserving the principles of free speech is a complex challenge. Rules will likely face criticism for potential infringements on freedom of expression. Considerations regarding freedom of expression are addressed in more depth in Chapter 6.5.1.
- **Enforcement difficulties:** Enforcing rules on political microtargeting can be challenging, especially in the digital realm, where boundaries and jurisdictional issues can arise, making it difficult to hold violators accountable. The challenge of enforcement will be addressed in more depth in Chapter 6.5.3.

6.4.2 Transparency obligations

Requiring online platforms to publish or display information about political ads can help individual users, opposing campaigns and the broader public (e.g., journalists, watchdog organizations) better understand data-driven campaigning, detect unsavory targeting tactics, and engage in remedial counter speech. The following subchapters will individually examine measures for user-facing transparency and public-facing transparency.

6.4.2.1 USER-FACING TRANSPARENCY

Platform operators can be obliged to clearly designate paid political ads and distinguish them from other content (e.g., editorial content, news, or user posts), and to provide clickable ad transparency notices containing information such as:[xxiii]

- Who paid for the ad
- Reasons why the user has qualified for the targeted audience, including personal data that were relevant in this process
- Source of user's data (e.g., web tracking, mobile app, or loyalty card) including, where applicable, information indicating whether the personal data was derived, inferred, and/or uploaded by the advertiser or obtained from a third party
- Legal basis for data processing
- How the user can exercise their data subject rights
- Furthermore, social media platforms can be required to clearly signal the "influencer status" of users or sites that regularly reach large audiences with political or issue-based content.

Advantages of user-facing transparency

- **Basic situational awareness:** While transparency notices are typically too compact and simplistic to capture the full complexity of the PMT ecosystem, they can help interested users gain a basic understanding about the mechanisms, actors, and risks involved in PMT.
- **Rights awareness:** Notices play a vital role in making users aware of their data subject rights (e.g., data access, rectification, deletion) and alerting them to assert those rights.
- **Accountability:** Transparent advertising holds advertisers accountable for their messaging and actions. When users are aware of who is behind an ad, they can provide feedback, report issues, or seek clarification directly from the advertiser. In the best-case scenario, this accountability promotes responsible advertising practices and encourages advertisers to maintain ethical standards.

[xxiii] Examples were adapted from Panoptykon Foundation's 2020 report "Who (really) targets you?"[47]

Limitations & challenges of user-facing transparency

- **Insufficient for informed decision-making:** Transparency notices often rely on complex and opaque language and contain too much information to realistically digest. Paired with people's everyday time constraints and the limited awareness and understanding of the average user, the information provided via notices typically does not suffice for truly informed decision-making.[48]
- **False sense of security:** The presence of transparency notices can give the impression of legal compliance and comprehensive data protection but, by itself, does not guarantee either. Thus, without additional protective measures required by law, notices can lead users to falsely believe they are adequately protected from PMT-related harms.
- **Challenge of verification:** Notices can contain inadequate or incomplete information, and it can be challenging for users to verify the accuracy and completeness of the provided details. Furthermore, as long as online platforms can decide themselves which information to include in transparency notices, there is a risk of relevant data points being omitted entirely.

6.4.2.2 PUBLIC-FACING TRANSPARENCY

For addressing the risks of PMT through public-facing transparency, there are two main approaches, namely ad libraries and campaign finance laws.

Ad libraries

Platform operators can be obliged to publish an "ad library", i.e., a searchable repository of all active and historical ads that have been posted through their website(s). This can be limited to political and issue-based ads, or even include non-political ads. The latter option provides more comprehensive transparency and avoids ads remaining under the radar when they are falsely labelled as non-political. For each advertisement, an ad library can provide information such as:[xxiv]

- Ad content (text, image and/or video content), including ad variations
- Period when the ad was active
- Ad placement (e.g., sidebar, newsfeed)
- Detailed description of selected targeting criteria (e.g. demographics, location, interests, and behaviors)
- The source(s) of the personal data used, where applicable including information whether the personal data was derived, inferred, and uploaded by the advertiser or obtained from a third party
- Information on ad spending (incl. aggregated information such as the total spend on ads by country and by advertiser)
- Estimated reach that the ad received within specific geographic and demographic criteria, optionally broken down by paid vs. unpaid reach
- The number of views and engagements that the ad received (incl. shares, likes, and comments)
- Optimization criteria used in the targeting process (e.g., improved awareness, engagement, and traffic)

Users should be able to filter the information in the ad library based on all these criteria.

Campaign finance

Political finance laws can be updated for the digital era to protect the integrity of elections online. As Bayer (2019) states, "campaign financing has long been a pressing, overlooked issue in democracies, and the problem [has only] grown more severe."[46] To increase trust in the democratic process, political campaigns can be obliged to disclose details on their spending (including social media ads and other types of online campaigns) and their sources of funding (domestic and abroad) in a searchable public database. Existing non-profit initiatives, such as the OpenSecrets platform[49] tracking the flow of money in U.S. politics, provide inspiration on how such databases could be structured in a clean and transparent way. Online platforms and communication agencies can be required to retain their contracts with political campaigns for validation purposes.

Advantages of public-facing transparency

- **Fact-checking and remedial counter speech:** Political ads often contain false or misleading claims. Ad libraries enable fact-checkers, researchers, and journalists to analyze political ads for accuracy and inform the public about potential manipulation attempts. This also gives political opponents, the media, and civil society the opportunity to engage in fact-checking.
- **Accountability and oversight:** By providing a transparent record of political ads and their sponsors, ad libraries allow regulatory bodies, journalists, and the public to monitor and hold advertisers accountable for their messaging. Such public scrutiny can discourage harmful practices, such as hate speech, disinformation, and astroturfing.[xxv] Public information on campaign finances helps identify potential conflicts of interest between candidates and their donors and can discourage illegal activities, such as improper contributions or illicit use of funds.

[xxiv] Examples were adapted from Panoptykon Foundation's 2020 report "Who (really) targets you?"[47]

[xxv] Astroturfing refers to the practice of artificially simulating grassroots support for a cause, idea, product, or political movement. It involves the use of fake online personas, social media accounts, comments, reviews, or other forms of online engagement to give the impression of widespread public backing.

- **Empowering watchdog organizations:** Disclosures about political ads and campaign finances can provide valuable information to organizations advocating for civil rights, helping them to strengthen privacy protections and influence policy.
- **Research and analysis:** Ad libraries serve as valuable resources for researchers, journalists, and policymakers studying the impact of political advertising, enabling comprehensive analyses of trends, strategies, and their effects on democratic processes. These insights can underpin policy discussions and regulatory efforts aimed at addressing the risks associated with PMT and ensuring fair and transparent advertising practices.

Limitations & challenges of public-facing transparency

- **Underfunded civil society:** The effectiveness of public disclosures in promoting transparency and accountability in political advertising relies heavily on the efforts of civil society organizations. These organizations play a crucial role in curating, maintaining, and analyzing the vast amount of data on campaign finance and political ads, despite being hindered by chronic underfunding. Much like open-source initiatives, where community efforts cannot eliminate all security breaches, and like fact-checkers, who cannot catch all instances of disinformation, limited funding and resources available to civil society organizations can hamper their ability to uncover unfair, dangerous, and illegal practices based on publicly available data.
- **Incomplete or inaccurate information:** Public disclosures of political ads and campaign finance frequently fall short of providing comprehensive and precise information—for instance, because advertisers do not properly declare political ads[50] or political parties underdeclare their online campaign spending.[51] If political parties and online platforms can decide which information to include in their disclosures, there is a risk that relevant data points are omitted entirely. As long as transparency measures are not subject to clear rules and appropriate supervision, their output should be treated with reservations. Independent ad collections by watchdogs such as the Persuasion Lab's *Ad.Watch* project,[52] which pioneered in creating a visual database of Facebook ads in 34 countries, are therefore critical.
- **Functional limitations and usability issues:** If not enforced by law, ad libraries and other public disclosure tools can be flawed in their design and implementation that degrade their usability and functionality. Such flaws, which can of course be intentional, may impede the work of journalists and watchdog organizations, hindering their ability to access relevant data, analyze political advertising trends, and hold political actors accountable for misleading or manipulative practices. Research has shown, for example, that journalists were highly critical of the Meta Ad library and its many limitations (e.g., low data granularity, lack of reliability, difficulty of tracking overall campaign spending, potentially misleading labels, and the user-unfriendly and time-consuming design).[53]
- **Evasion techniques:** Even if an online platform or a political campaign makes an honest effort to implement disclosure tools for enhanced transparency, there is a potential for downstream actors (e.g., malicious advertisers on the platform, or corrupt political candidates) to evade monitoring and detection. For instance, investigations have revealed that weaknesses in the Meta Ad Library enabled malicious advertisers to avoid accurate disclosure of coordinated activities and political ads worth millions of dollars.[50]

6.4.3 User control / consent

Another approach to regulate PMT is giving voters (more) control over the ways they can be targeted with political ads. As PMT typically involves the processing of personal data, such rules can be rooted in data protection regulation. In many places, such as in the EU, existing privacy laws already make it harder for companies and political campaigns to gather and process the fine-grained personal information required for PMT.[54] However, in other places, including most countries of the Global South, data protection rules are weaker or non-existent.[55]

For instance, using personal data for PMT could require informed, explicit, and freely given consent of the data subject. Additional measures can further strengthen privacy protection, such as outlawing "tracking walls" (i.e., barriers that website visitors can only pass if they consent to third-party tracking), ensuring that users can easily move their data between online services ("data portability") or giving users the right to manage consent automatically for all websites through browser settings.

Advantages of user control / consent

- **User autonomy:** The implementation of user controls can empower individuals, reinforcing their autonomy and self-determination by granting them greater authority over their own personal data and online experience. It is important to note, however, that this outcome assumes that people's privacy choices are free and informed, which is often not the case (see limitations below).

- **Can discourage privacy-intrusive advertising practices:** By allowing individuals to exert greater control over their personal information and online activities, user controls can hamper and disincentivize excessive tracking and surveillance-based advertising.

Limitations & challenges of user control / consent

- **In practice, most privacy choices are neither free nor informed:** One major shortcoming with the notice-and-consent approach is that people's everyday choices about their personal data can hardly be described as free and informed. As Kröger et al. (2021) state, "people's privacy choices are typically irrational, involuntary and/or circumventable due to human limitations, corporate tricks, legal loopholes, [people's dependence on certain services,] and the complexities of modern data processing."[48] The way user controls are implemented in practice often leaves users with little choice but to either sacrifice essential services or compromise their privacy.[48] Accordingly, surveys indicate that most people feel that they have lost control over their personal data.[56]
- **Ignorance of collective harms:** The risks associated with PMT can go beyond the individual and affect other people and society at large. The privacy choices of individuals typically do not consider these types of collective consequences.[48]
- **Low compliance rates:** Data companies' compliance with data protection rules is typically limited—even in countries with relatively strong rule of law such as EU member states.[57] Thus, even if privacy regulation is in place, there is still a high risk that data may be mishandled or misused, including for intrusive tracking and undue online manipulation.

6.4.4 Restricting PMT

Legal rules can impose certain limits or even a total ban on PMT. The scope of ads affected by a restriction depends on the specific legal definition of PMT (see Chapter 6.2).

6.4.4.1 PARTIAL RESTRICTIONS

There are many ways in which PMT practices can be partially restricted by law, e.g., by limiting one of the following (or any of these in combination):

- **Number of ads campaigns can run**
- **PMT methods that can be used** (e.g., automated accounts, artificial intelligence, bulk messaging)
- **Use of PMT in certain time periods** (restricting PMT during "quiet periods" or in the run-up to elections)
- **Types of data that can be used for PMT** (e.g., prohibition of using "sensitive" attributes such as ethnicity, religion, political affiliation, and health information)
- **Amount that campaigns can spend on PMT** (e.g., 20 times the monthly national minimum wage per candidate)

6.4.4.2 TOTAL BAN

PMT can be legally prohibited, for example by imposing interdictions on political advertisers, preventing online platforms from displaying political ads, or by banning the utilization of personal data for political advertising purposes.

Advantages of restricting PMT

- **Removing risks:** By implementing restrictions on PMT, the associated risks—which include significant threats to individual privacy and autonomy, social cohesion, and the functioning of democracy (see Chapter 3.2)—can be mitigated or even completely avoided. The degree of prohibition imposed determines the extent of protection: A total ban can remove all risks, while a partial restriction only removes part of the risks.

Limitations & challenges of restricting PMT

- **Giving up benefits:** Imposing strong restrictions on PMT will eliminate or diminish the possibility of reaping the benefits that PMT can offer (e.g., relevance and diversification of ad content, campaign efficiency, possibility of connecting with specific population segments that are otherwise hard to reach). It should be noted, however, that the stated benefits of PMT lack empirical evidence are partly based on unrealistic assumptions (see Chapter 3.1). Based on current knowledge, the risks of PMT appear to outweigh the promises regarding their impact on the common good.
- **Balancing free speech:** Political ads are considered a form of political speech. When contemplating a ban on political microtargeting, careful consideration must be given to striking a balance between addressing potential harms and avoiding unintended limitations on political discourse. Considerations regarding freedom of expression are addressed in more depth in Chapter 6.5.1.

6.5 Further considerations

6.5.1 Considerations regarding freedom of expression

When regulating PMT, it is of utmost importance to consider and safeguard freedom of expression. Regulation on political advertising and disinformation, if not carefully designed, can be easily misused by authoritarian governments as a means to suppress dissent and consolidate their power.[58,59] Authorities can use vague definitions of "propaganda", "hate speech", or "fake news" to censor political opponents, independent media outlets, and civil society organizations critical of the government. Rather than effectively addressing disinformation, these regulations serve as a tool for authoritarian regimes to control narratives and manipulate public opinion, ultimately undermining the principles of democracy and human rights.

When regulating PMT, it is of utmost importance to consider and safeguard freedom of expression. Regulation on political advertising and disinformation, if not carefully designed, can be easily misused by authoritarian governments as a means to suppress dissent and consolidate their power.

A particularly striking example of this is Russia, where a new law ensures that people can be heavily fined or even jailed for up to 15 years for spreading what the Kremlin would consider "false information" (e.g., basic facts about Russia's war on Ukraine).[60] Human rights watchdogs have also warned about potentially repressive fake-news laws in many other countries, including Algeria, Azerbaijan, Cambodia, Malaysia, Nigeria, Hungary, and Thailand.[58,61]

While protecting citizens from misinformation and undue influence is important, any regulatory measure must strike a delicate balance to avoid infringing upon the fundamental right to free speech. A nuanced approach to regulating PMT should focus on transparency, accountability, and preventing malicious practices while preserving the open exchange of ideas and diverse perspectives necessary for a thriving democratic society.

If not carefully designed, a PMT ban could also be exploited by competing political parties. As has been argued, "political opponents could flag each other's content online, turning the online spaces people depend on to obtain their information into void and barren places. The focus in our democracies must be on promoting a high-quality, informed debate, not creating legislation that pushes us towards a culture of fear of removal when expressing our views."[62]

Clear and fair standards should be established by policymakers and platforms for determining what is false information, hate speech, undue manipulation, etc. during content moderation.

Where the law mandates the filtering of content, clear and fair standards should be established by policymakers and platforms for determining what is false information, hate speech, undue manipulation, etc. during content moderation. This should include redress options for users who feel they were treated unfairly in this process. There should be checks and balances in place to ensure that rules cannot be exploited by neither powerful private actors, nor governments to introduce censorship and suppress opposition voices. For instance, independent nonpartisan committees can be formed for tasks such as screening political ads in social media. These bodies could include civil society actors like NGOs and researchers but also partnerships with public actors to protect election integrity and independence. Such initiatives are already being piloted, for example in South Africa, where these bodies not only enable research and build ad repositories, but also might be used to help guiding possible future regulation.[63]

Finally, it is also important to consider that not only regulation on political advertising but also PMT itself can harm freedom of expression. As Bennett and Lyon state, "The opaqueness of much contemporary political messaging [such as PMT] blocks the presumed self-correcting benefits of rights to freedom of expression."[64] In other words, PMT fragments public discourse by hindering a shared information foundation that encompasses diverse opinions and perspectives, thus undermining the "marketplace of ideas" principle which is essential to a functioning democracy.[64] Bayer (2020) argues that PMT "impacts the fundamental right of the non-targeted citizens to receive information, and consequently, the democratic public discourse. The right to information is the passive side of freedom of expression (…) Freedom of political expression is also an instrument to create a diverse and free public debate; therefore, expressions that counteract this goal cannot avail of the protection."[65]

6.5.2 Limitations of corporate self-regulation

Corporate self-regulation is often touted as a potential solution to address various ethical concerns and risks associated with emerging technologies and practices, including PMT. For instance, under pressure following the Cambridge Analytica scandal, Facebook made several promises, including researching the role of social media in elections, disclosing more information on advertisers, and ending some types of targeted advertising;[66] Twitter temporarily banned political ads from its platform;[67] and Google barred political advertisers from targeting voters based on affiliation and tightened its ban on "demonstrably false claims".[68]

Corporate self-regulation can be an important element in addressing the risks of PMT (see Chapter 3.2). However, relying solely on self-regulation does not seem sufficient to safeguard democratic processes and protect individuals' rights—for several reasons:

- **Big Tech's lack of trustworthiness:** Over the last few years, a multitude of privacy scandals,[69] lies,[70] antitrust lawsuits,[71] and cases where online platforms neglected their own content rules[72] have shown that Big Tech companies often engage in reckless practices to pursue their business interests and lack the motivation to effectively scrutinize their own behavior. Seen in the context of a highly competitive market where voluntary ethical behavior may amount to a competitive disadvantage, Big Tech companies do not seem suited to reliably police their own business practices. A recent survey conducted across 18 international markets revealed that two-thirds of consumers express high levels of distrust in social media platforms' handling of their data.[73] Big Tech companies have also been criticized for their "shady" lobbying against platform regulation[74] and for undermining independent research into their data practices and measures on disinformation.[75]

Over the last few years, a multitude of privacy scandals, lies, antitrust lawsuits, and cases where online platforms neglected their own content rules have shown that Big Tech companies often engage in reckless practices to pursue their business interests and lack the motivation to effectively scrutinize their own behavior.

- **Question of legitimacy:** As Jaursch (2020) states, "On a more fundamental level, it is problematic that private, profit-driven corporations reliant on behavioral advertising to make money decide on the limits to (paid) political speech. This contrasts with broadcasting rules set by elected officials or their democratically instituted regulatory bodies, for example, or to industry-wide self-regulation in print media."[31] Given these significant conflicts of interest and the impacts that PMT can have not only on individuals, but also on society at large (see Chapter 3.2), the approach of corporate self-regulation in this area is questionable. Furthermore, allowing private entities to control speech and impose penalties raises concerns, as protecting fundamental rights is a core responsibility of governments.[36]

Self-regulatory measures are not sufficient to regulate PMT in the best interest of society and should therefore not replace enforceable regulation.

- **Self-regulatory measures do not go far enough:** Research has shown that, in practice, the voluntary measures implemented by certain social media platforms with regard to political advertising (e.g., transparency commitments) are insufficient.[31] Similarly, for instance, it is questionable how valuable a platform's commitment to "research[ing] the role of social media in elections"[66] is when business-damaging findings of internal studies are kept secret and are not acted upon by Big Tech, as the case of Facebook whistleblower Frances Haugen has demonstrated.[76]

- **Self-imposed measures vary between companies and can be changed anytime:** As the examples mentioned in the beginning of this chapter illustrate, self-regulatory measures typically vary from platform to platform, which can cause confusion and inconsistencies in fighting undue online manipulation and disinformation. This may even include significant differences in how political ads are defined in the first place, which "makes independent monitoring from academics, regulators and civil society experts difficult".[31] Also, self-imposed rules can change anytime, as illustrated by Twitter (now X) lifting its ban on political ads in early 2023.[77] Binding regulation can bring much-needed clarity and standardization to this process.

- **Lack of enforcement:** Rules—including self-imposed ones—need to be properly enforced to have a real impact. However, self-regulation typically does not involve sanctions in case of non-compliance[65] or meaningful openings for independent auditing and oversight.[31] While even binding legal rules are often not adhered to by Big Tech,[69] compliance with non-binding self-imposed rules is even more questionable. The same applies to journalistic ethical codes and media self-regulation: Most disinformation is distributed by actors that would arguably not adhere to self-imposed rules anyways.[46]

In conclusion, self-regulatory measures are not sufficient to regulate PMT in the best interest of society and should therefore not replace enforceable regulation. As explained in Chapter 6.3, under current circumstances, a combination of state regulation and self-regulation would seem appropriate to address the risks of PMT.

6.5.3 Challenges to regulating PMT

Political efforts to regulate PMT can face numerous challenges that need to be considered and dealt with, including:

- **Conflicts of interest within political parties:** Governments themselves often engage in PMT to gain a competitive advantage in elections. They leverage the power of data and targeted messaging to shape public opinion, mobilize supporters, and influence electoral outcomes. Therefore, regulating PMT could potentially undermine their own ability to employ these tactics effectively. For example, the European Commission currently faces a legal complaint for its alleged use of PMT to garner support for a controversial regulation proposal, which may have violated the EU's General Data Protection Regulation.[78] Despite the risks associated with PMT, governments may be reluctant to introduce stringent regulations that limit their own campaign strategies or hinder their chances of staying in power.[65,79]

Despite the risks associated with PMT, governments may be reluctant to introduce stringent regulations that limit their own campaign strategies or hinder their chances of staying in power.

- **Lack of public awareness / political momentum:** Regulating PMT can present a significant challenge due to a lack of awareness about the risks involved, resulting in a dearth of political momentum. The complexity and technicality of this issue make it less accessible to the public, leading to limited understanding and awareness among policymakers and citizens alike. This includes the various risks associated with PMT (see Chapter 3.2). Consequently, there is often a lack of political will to address the regulation of PMT effectively.

- **Political lobbying by the PMT industry:** The challenge of regulating political microtargeting is compounded by the influence and lobbying power exerted by Big Tech companies and other actors of the PMT ecosystem. They have a vested interest in maintaining the status quo and resisting stringent regulations that could curtail their access to user data or restrict the lucrative advertising revenue generated from political campaigns. The substantial financial resources, extensive networks, and lobbying prowess of Big Tech companies make it challenging for policymakers to enact meaningful regulatory measures, as they often face significant pushback and resistance from these industry giants. Striking a balance between protecting democratic processes and user privacy, safeguarding free speech, and countering the lobbying power of Big Tech remains a critical hurdle in regulating political microtargeting effectively.

A lack of economic and political power of individual countries can make it difficult for them to effectively regulate the business practices of major corporations, especially when these are backed by powerful countries, such as the US or China.

- **Effective power to govern:** A lack of economic and political power of individual countries can make it difficult for them to effectively regulate the business practices of major corporations, especially when these are backed by powerful countries, such as the US or China. As Takhshid (2021) argues, "the current power asymmetry between major social media companies and countries in the Global South limits the ability of many of such countries to have any meaningful bargaining power to advocate for their citizens' consumer rights and their ability to manage misinformation campaigns in their sovereign territories. (…) [U]nless countries in the Global South act collectively, they should not expect any major change from powerful social media companies (…) Regional treaties among countries as a form of collective action could push social media companies to be more attentive to their actions outside the Global North and bear responsibility in a transnational space."[80] While there are supranational political and economic unions in the Global South (e.g., AU, ECOWAS, MERCOSUR, ASEAN), most of these unions currently do not have the same level of integration and bargaining power as the EU, for example. Building stronger regional alliances will be key not only to regulating PMT but also to responding to digital colonialism in general.

- **Challenge of enforcement:** In modern platform regulation, enforcement has emerged as a crucial bottleneck. Even the EU's General Data Protection Regulation (GDPR) has been criticized as "toothless" due to a lack of effective enforcement.[81] For poorer countries, which often lack the expertise and resources to build and properly staff effective supervisory bodies (e.g., data protection authorities), it may be particularly difficult to ensure compliance with existing laws.[82,83] Some possible solutions to this problem are to narrow the focus of laws, for instance on large platforms (e.g., special requirements for large online platforms under the EU's DSA[21]); to put a focus on efficient and standardized processes; and to implement rules that are easier to supervise (e.g., total or temporal ban of PMT vs. fine-grained rules about ad spending, which can be difficult to trace). When designing enforcement regimes, it should also be considered that foreign actors—which pose a particular risk with regard to PMT (see Chapter 3.2.6)—typically have less incentive to conform to domestic regulation.[24] Where PMT is not banned, the companies that benefit financially from the practice can be obliged to play a role in enforcement (e.g., establish mechanisms to prevent unlawful targeted ads; immediately report violations to authorities; ensure that adequately trained staff is available for content moderation, especially in non-English-speaking contexts; respond to user complaints within a specific period of time). In contrast to traditional advertising (e.g., newspaper, TV), which is mostly bound to specific national markets, "online political ads can transcend borders and thus political, cultural

In modern platform regulation, enforcement has emerged as a crucial bottleneck.

and language differences”,[31] adding to the difficulty of enforcing legal rules. There may even be types and aspects of PMT that are impossible to supervise (e.g., PMT via end-to-end encrypted messengers[46]). These limitations must be understood and taken into consideration when designing a legal and enforcement regime for dealing with PMT.

- **Evolving tactics:** The rapidly evolving nature of technology and tactics in PMT can make it difficult for rules to keep up. Adapting regulations to address emerging strategies and platforms becomes a continuous challenge. As rules are established, malicious actors may find ways to circumvent or exploit loopholes in the regulations, necessitating constant vigilance and updating of rules to stay ahead.

Algorithms employed by online platforms wield a significant influence over the dissemination of political content on the internet, including political ads, and much of modern media consumption, which can all impact the formation of political will.

6.5.4 Content filtering and algorithmic amplification

In today’s online media environment, search engines, social media and video platforms act as information intermediaries or gatekeepers that “decide which messages are displayed to which people and in which order”.[84] While content filtering algorithms are presumed to be designed with the goal of maximizing user engagement and profits for online platforms, their intricate workings often remain shrouded in secrecy. According to platforms themselves, this is due to the protection of trade secrets. There are ongoing discussions whether these algorithms inadvertently promote extreme viewpoints and polarize online political discourse.[85] For instance, it has long been known that making social media users angry can increase their online engagement,[86] leading Facebook to push emotional and provocative content into users’ news feed.[87] Similarly, Facebook has been criticized for conducting a secret experiment to influence the emotions of nearly 700,000 users for opaque purposes by filtering their friends’ postings.[88] Logically, filtering what people see online can also have an impact on their convictions and political views,[89] making it a relevant topic for democracy protection. In 2015, an experimental study found that “Google’s search algorithm can easily shift the voting preferences of undecided voters by 20 percent or more—up to 80 percent in some demographic groups—with virtually no one knowing they are being manipulated”.[90] These findings were dubbed by the authors as the Search Engine Manipulation Effect (SEME).[91] Content filtering algorithms can also contribute to fueling hate and political division. For example, Meta has been sued for two billion dollars over Facebook’s recommendations systems which “amplified violent posts” in Ethiopia, “inflaming the country’s bloody civil war”.[92] Recent changes at X (formerly Twitter) even made it easier for authoritarian governments “to attract new followers and broadcast propaganda and disinformation to a larger audience.”[93]

Letting platform owners and algorithms decide what people see online raises concerns about voter manipulation and distortion of political discourse.

To understand the role that platform algorithms can play in political campaigning, it is important to distinguish between paid reach and what is commonly referred to as “organic” or unpaid reach:

Unpaid reach of online content refers to the number of people who see the content without paid distribution (e.g., unpaid listings that appear on a search engine results page, social media posts that appear in people’s news feed because their friends have shared or interacted with them). This content is, however, still typically ranked by algorithms and sorted artificially, making the frequently used term “organic” somewhat misleading. Political campaigns often use Search Engine Optimization (SEO) techniques—sometimes even underhanded “Black Hat” techniques[xxvi]—to improve the search rankings and maximize the unpaid reach of their websites and online content.[95]

Paid reach, on the other hand, refers to the number of people who see a piece of online content through paid advertising efforts (e.g., paid search results, banner ads, boosted posts). While political campaigns can define targeting criteria and strategies for paid online ads, the actual ad targeting is typically conducted by online platforms and their algorithms.[47] They decide to whom specifically an ad is shown (or not shown). Some platforms even offer advertisers features to automate their advertising campaigns (e.g., automatic ad placement, automatic audience selection, automatic personalization).[47]

In sum, algorithms employed by online platforms wield a significant influence over the dissemination of political content on the Internet, including political ads, and much of modern media consumption, which can all impact the formation of political will.

Why is it problematic that online platforms and their algorithms have political influence?

Letting platform owners and algorithms decide what people see online raises similar concerns about voter manipulation and distortion of political discourse—

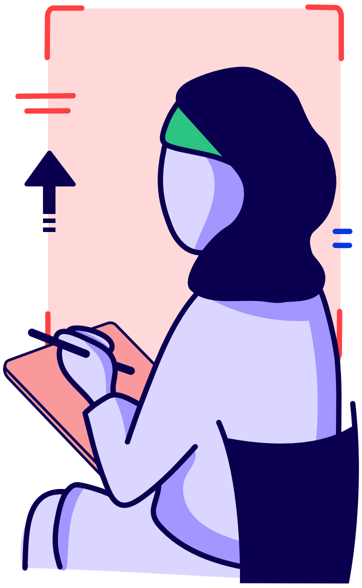
[xxvi] Although algorithms can penalize such behavior, it is well-documented, for example, that political actors have used bots and trolls to manipulate the recommendation algorithms of social media platforms and artificially boost their content.[94]

and thus similar risks for democracy—as the ones described in Chapter 3.2 for PMT in general. A key difference is that this subchapter focuses on entire platforms that underpin much of modern global information exchange with greater reach and the potential to inflict more substantial harm than individual political parties. The following points are worth highlighting with regard to platform algorithms:

- **Lack of transparency:** Shielded by trade secrets, platform algorithms essentially operate as black boxes, which limits public understanding and scrutiny of their inner workings. Research has shown that biased ranking of online content "can be masked so that people show no awareness of the manipulation."[91]
- **Concentration of power:** As online platforms have become the main source of information for many Internet users,[95] their content filtering algorithms wield immense influence over what information reaches people, potentially shaping opinions, beliefs, and behaviors. A small number of tech giants is controlling these platforms and algorithms. This concentration of power not only stifles competition but also raises questions about democratic values and the need for greater transparency and accountability in the digital realm (see also "Question of legitimacy" in Chapter 6.5.2).
- **Biases / conflicts of interest:** Online platforms are typically profit-driven and can exhibit political biases, raising questions about their apparent neutrality, especially given the substantial lobbying efforts by Big Tech (see also "Big Tech's lack of trustworthiness" in Chapter 6.5.2). For instance, independent tests of algorithmic recommender systems have found a significant bias towards right-leaning content on platforms such as YouTube[89] and X.[96]

Should platform algorithms be regulated?
Considering the problematic aspects highlighted above, it is important to address platform algorithms when regulating the information environment around elections and other democratic processes. While a detailed discussion on the regulation of algorithms goes beyond the scope of this report, it is generally advisable to implement measures that ensure transparency and accountability in algorithmic systems (see, for example, the due diligence and transparency obligations regarding algorithmic decision-making by online platforms introduced by the EU's DSA[97]). Where possible, steps should be taken to oblige platforms to maintain ideologically neutral services and avoid platforms and their algorithms being used for political influence. Social media algorithms have already been criticized for amplifying extreme views[98] and showing a bias towards a specific political camp.[99] Safeguarding the integrity of the digital information ecosystem is paramount to fostering informed and unbiased political discourse.

Social media companies increasingly make use of Artificial Intelligence (AI) systems, which can contribute to biases and lack of transparency in their content filtering and thus introduce additional risks. These developments require an adequate political response. There is a need for regulatory frameworks and legitimate institutions to govern the use of AI. The EU will soon release the world's first comprehensive regulatory approach, the AI Act, aiming at balancing the risks and opportunities of these technologies. While numerous countries in the Global South have developed—or are currently developing—national AI strategies[100] and are moving toward legislative action,[101] AI governance has been described as a "regulatory bottleneck" in the Global South.[102] Many countries, especially in Africa, are still lacking regulatory initiatives to implement dedicated AI legislation.[103,104] As an unprecedented technological challenge with major implications for all aspects of society, the regulation of AI should be addressed with high priority—both at the national and multilateral level.



References

1. Jaursch, J. (2020). Defining Online Political Advertising. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/en/publication/defining-online-political-advertising
2. The Civil Liberties Union for Europe. (2022). Uneven Regulation of Political Ads Across EU Threatens Free & Fair Elections. Liberties. https://www.liberties.eu/en/stories/political-advertising-regulation-in-five-eu-countries-liberties-report/44478
3. UNCTAD. (2021). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
4. Monteiro, A. P. L., Tavares, C., Borges, E., Cruz, F. B., & Massaro, H. (2021). Missing Bridges—A comparative analysis of legal frameworks governing personal data in political campaigning in Latin America. InternetLab. https://internetlab.org.br/wp-content/uploads/2021/02/Missing-bridges-2.pdf
5. Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Wirecutter. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/
6. Information Regulator (South Africa). (2019). Guidance Note on the Processing of Personal Information of a Voter by a Political Party in Terms of the Protection of Personal Information Act, 4 OF 2013. https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-PolParties-1.pdf
7. Republic of the Philippines Commission on Elections. (2021). RESOLUTION NO. 10730. https://namfrel.org.ph/news/reslaws/comelec_res_10730%20IRR%20for%20Fair%20Election%20Act%20for%202022%20NLE.pdf
8. Republic of the Philippines National Privacy Commission. (2021). Guidelines on the processing of personal data for election campaign or partisan political activity. https://www.dataguidance.com/sites/default/files/advisory_election_campaigning_03-nov-21-final_1.pdf
9. International IDEA. (2020). Protecting Political Campaigns from Digital Threats Insights from Tunisia, Panama and Bolivia. https://www.idea.int/sites/default/files/publications/protecting-political-campaigns-from-digital-threats.pdf
10. Communications Authority of Kenya. (2017). Guidelines on prevention of dissemination of undesirable bulk and premium rate political messages and political social media content via electronic communications network. http://www.knchr.org/Portals/0/DOC-20170630-WA0061.pdf?ver=2017-06-30-225539-533
11. Kitili, J., Gitonga Theuri, & Badbess, K. (2022). Contextualising Political Advertising Policy to Political Micro-Targeting in Kenyan Elections. Center of Intellectual Property and Technology Law (CIPIT). https://cipit.org/wp-content/uploads/2023/03/Political-Advertising_compressed.pdf
12. Deloitte. (2021). Kenya Data Protection Act Quick Guide. https://www.deloitte.com/content/dam/Deloitte/ke/Documents/risk/Kenya%20Data%20Protection%20Act%20-%20Quick%20Guide%202021.pdf
13. Mude, H. (2021). Political Micro-Targeting in Kenya: An Analysis of the Legality of Data-Driven Campaign Strategies under the Data Protection Act. Journal of Intellectual Property and Information Technology Law (JIPIT). https://journal.strathmore.edu/index.php/jipit/article/view/61
14. King, J. (2022). Microtargeted Political Ads: An Intractable Problem. Boston University Law Review, 102(3), 1129–1167. https://www.bu.edu/bulawreview/files/2022/04/KING.pdf
15. Bulka, T. (2022). Algorithms and Misinformation: The Constitutional Implications of Regulating Microtargeting. Fordham Intellectual Property, Media and Entertainment Law Journal, 32(4). https://ir.lawnet.fordham.edu/iplj/vol32/iss4/6/
16. European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising, 2021/0381 (COD). https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0001.02/DOC_1&format=PDF
17. Chee, F. Y., & Chee, F. Y. (2023). Big Tech to face tougher rules on targeted political ads in EU. Reuters. https://www.reuters.com/technology/big-tech-face-tougher-rules-targeted-political-ads-eu-2023-11-07/
18. Moraht, F. (2023). Mehr Transparenz erst nach den EU-Wahlen. Tagesspiegel. [German]. https://background.tagesspiegel.de/digitalisierung/mehr-transparenz-erst-nach-den-eu-wahlen
19. Vincent, J. (2022). Facebook, Twitter, TikTok, Google and others agree to new EU rules to fight disinformation. The Verge. https://www.theverge.com/2022/6/16/23168987/eu-code-disinformation-online-propaganda-facebook-twitter-tiktok
20. Lomas, N. (2023). Elon Musk takes Twitter out of the EU's Disinformation Code of Practice. TechCrunch. https://techcrunch.com/2023/05/27/elon-musk-twitter-eu-disinformation-code/
21. European Commission. (2022). The Digital Services Act: Ensuring a safe and accountable online environment. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en
22. Cavaliere, P., Mude, H., Bonaventura, I., & Sanchez, M. G. (2021). Micro-Targeting in Political Campaigns: A comparative analysis of legal frameworks. The University of Edinburgh. https://privacyinternational.org/sites/default/files/2021-01/UoE_PI%20Micro-targeting%20in%20policital%20campaigns%20comparative%20analysis%202021.pdf
23. Digital Advertising Alliance of Canada. (n.d.). Political Ad Registries. https://politicalads.ca/en/registries
24. Ó Fathaigh, R., Dobber, T., Zuiderveen Borgesius, F., & Shires, J. (2021). Microtargeted propaganda by foreign actors: An interdisciplinary exploration. Maastricht Journal of European and Comparative Law, 28(6), 856–877. https://doi.org/10.1177/1023263X211042471
25. Stobart, A., & Griffiths, K. (2022). Explainer: The rules (or lack thereof) for political advertising. Grattan Institute. https://grattan.edu.au/news/the-rules-or-lack-thereof-for-political-advertising/
26. Appelman, N., Dreyer, S., Bidare, P. M., & Potthast, K. C. (2022). Truth, intention and harm: Conceptual challenges for disinformation-targeted governance. Internet Policy Review. https://policyreview.info/articles/news/truth-intention-and-harm-conceptual-challenges-disinformation-targeted-governance/1668

27. van Drunen, M., Helberger, N., Schulz, W., & de Vreese, C. (2023). The EU is going too far with political advertising! - DSA Observatory. https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/
28. Cipers, S., & Meyer, T. (2022). What is political? The uncoordinated efforts of social media platforms on political advertising. https://researchportal.vub.be/en/publications/what-is-political-the-uncoordinated-efforts-of-social-media-platf
29. General Secretariat of the Council. (2023). Proposal for a regulation of the European Parliament and of the Council on the transparency and targeting of political advertising—Offer letter sent to the Chair of the European Parliament's Committee on Internal Market and Consumer Protection. https://www.consilium.europa.eu/media/69097/st17037-en23.pdf
30. United Nations Human Rights. (2011). Guiding Princpiles on Business and Human Rights. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
31. Jaursch, J. (2020). Defining Online Political Advertising. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/en/publication/defining-online-political-advertising
32. Today. (2019). Facebook blocks foreign ads before Thai election amid fears junta will benefit. https://www.todayonline.com/world/facebook-blocks-foreign-ads-thai-election-amid-fears-junta-will-benefit
33. Agence France Presse. (2023). EU Lawmakers Back Ban On Foreign Funding Of Political Ads. https://www.barrons.com/news/eu-lawmakers-back-ban-on-foreign-funding-of-political-ads-01675356007
34. De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law, 19(1), 41–70. https://doi.org/10.1093/icon/moab001
35. Bayer, J., Holznagel, B., Korpisaari, P., & Woods, L. (Eds.). (2021). Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe. Nomos. https://doi.org/10.5771/9783748929789
36. Bontcheva et al. (2020). Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression. International Telecommunication Union (ITU) and UNESCO. https://www.broadbandcommission.org/Documents/working-groups/ExecSum_FoE_disinfo_report.pdf
37. Meyer-Resende, M., & Straub, M. (2022). The Rule of Law versus the Rule of the Algorithm. Verfassungsblog. https://doi.org/10.17176/20220328-131300-0
38. van Drunen, M. Z., Helberger, N., & Ó Fathaigh, R. (2022). The beginning of EU political advertising law: Unifying democratic visions through the internal market. International Journal of Law and Information Technology, 30(2), 181–199. https://doi.org/10.1093/ijlit/eaac017
39. MacCarthy, M. (2020). An 'Equal Time' Rule for Social Media. Forbes. https://www.forbes.com/sites/washingtonbytes/2020/01/21/an-equal-time-rule-for-social-media/
40. Hate speech laws by country. (2023). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Hate_speech_laws_by_country&oldid=1146830275
41. United Nations. (n.d.). What is hate speech? Retrieved July 11, 2023, from https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech
42. Owino, V. (202). Kenya threatens ban on Facebook over hate speech. The East African. https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-threatens-ban-on-facebook-over-hate-speech-3896380
43. Tan, N. (2020). Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia. Election Law Journal: Rules, Politics, and Policy, 19(2), 214–239. https://doi.org/10.1089/elj.2019.0599
44. Bhagyanagar, V. S. (2021). Lessons from the Global Responses to Misinformation. Social & Political Research Foundation. https://sprf.in/wp-content/uploads/2021/11/SPRF-2021_Comm_Global-Responses-to-Misinformation.pdf
45. Westby, J. R. (2023). It Is Time To Pass Laws To Protect Voters Against Disinformation. Forbes. https://www.forbes.com/sites/jodywestby/2023/02/16/it-is-time-to-pass-laws-to-protect-voters-against-disinformation/
46. Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs. Social Science Research Network (SSRN). https://www.ssrn.com/abstract=3409279
47. Panoptykon. (2020). Who (really) targets you? Fundacja Panoptykon. https://panoptykon.org/political-ads-report
48. Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). The myth of individual control: Mapping the limitations of privacy self-management. Social Science Research Network (SSRN). https://doi.org/10.2139/ssrn.3881776
49. OpenSecrets. (2023). We Are OpenSecrets. https://www.opensecrets.org/
50. Edelson, L., Lauinger, T., & McCoy, D. (2020). A Security Analysis of the Facebook Ad Library. 2020 IEEE Symposium on Security and Privacy (SP), 661–678. https://ieeexplore.ieee.org/document/9152626
51. Rennó, R. (2018). Chile: Voter Rolls and Geo-targeting. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/overview-chile/
52. Sathe, G. (2019). Ad.Watch Is Everything The Facebook Ad Library Fails To Be. (2019). HuffPost. https://www.huffpost.com/archive/in/entry/ad-watch-facebook-ads-library-political-advertising-fake-news_in_5d41ab92e4b0db8affb1df0d
53. Leerssen, P., Dobber, T., Helberger, N., & de Vreese, C. (2023). News from the ad archive: How journalists use the Facebook Ad Library to hold online advertising accountable. Information, Communication & Society, 26(7), 1381–1400. https://doi.org/10.1080/1369118X.2021.2009002
54. Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. C. M. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. Big Data & Society, 5(2). https://doi.org/10.1177/2053951718811844
55. DLA Piper. (2023). Global Data Protection Laws of the World. https://www.dlapiperdataprotection.com/
56. The Harris Poll. (2022). Cyber Safety Insights Report. Norton. https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2022_NLCSIR_Global_Report.pdf

57. Kröger, J. L., Lindemann, J., & Herrmann, D. (2020). How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps. Proceedings of the 15th International Conference on Availability, Reliability and Security, 1–10. https://doi.org/10.1145/3407023.3407057
58. Wiseman, J. (2020, October 3). Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges. International Press Institute. https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/
59. Amnesty International. (2022, October 13). Turkey: "Dark day for online free expression" as new 'disinformation law' is passed. https://www.amnesty.org/en/latest/news/2022/10/turkey-dark-day-for-online-free-expression-as-new-disinformation-law-is-passed/
60. The Committee to Protect Journalists, Thomson Reuters Foundation, & Hogan Lovells. (2022). Understanding the laws relating to "fake news" in Russia. https://www.trust.org/publications/i/?id=ff07f978-3aae-4f4d-a7aa-7a505de138dd
61. Davison, L. (2022). Addressing Disinformation In The Global South. Tech Policy Press. https://techpolicy.press/addressing-disinformation-in-the-global-south/
62. Rodríguez, S. et al. (2023). The EU will deplatform political content and millions of citizens. Euractiv. https://www.euractiv.com/section/digital/opinion/the-eu-will-deplatform-political-content-and-millions-of-citizens/
63. Media Monitoring Africa. (n.d.). About Us. Retrieved November 8, 2023, from https://www.mediamonitoringafrica.org/about-us/
64. Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1433
65. Bayer, J. (2020). Double harm to voters: Data-driven micro-targeting and democratic public discourse. Internet Policy Review, 9(1). https://doi.org/10.14763/2020.1.1460
66. Ivanova, I. (2018). 8 promises from Facebook after Cambridge Analytica. CBS News. https://www.cbsnews.com/news/facebooks-promises-for-protecting-your-information-after-data-breach-scandal/
67. Demony, C. (2019). Twitter political ads ban no sure fix to voter manipulation: Kaiser. Reuters. https://www.reuters.com/article/instant-article/idUSKBN1XF29L/
68. Wong, J. C. (2019). Google latest tech giant to crack down on political ads as pressure on Facebook grows. The Guardian. https://www.theguardian.com/technology/2019/nov/20/google-political-ad-policy-facebook-twitter
69. Hill, M. (2022). The 12 biggest data breach fines, penalties, and settlements so far. CSO Online. https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html
70. Smith, C. (2017). Facebook's WhatsApp privacy lie cost it $122 million in European fines. BGR. https://bgr.com/tech/facebook-whatsapp-privacy-fine/
71. Lasarte, D. (2023). The ongoing big tech antitrust cases to watch in 2023. Quartz. https://qz.com/antitrust-cases-big-tech-2023-guide-1849995493
72. Global Witness. (2022). Facebook approves adverts containing hate speech inciting violence and genocide against the Rohingya. https://www.globalwitness.org/en/campaigns/digital-threats/rohingya-facebook-hate-speech/
73. Shah, K. (2023). Social media companies least trusted to handle personal data responsibly. YouGov. https://business.yougov.com/content/8258-global-social-media-companies-least-trusted-to-handle-personal-data-responsibly
74. Goujard, C. (2022). Big Tech accused of shady lobbying in EU Parliament. POLITICO. https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban/
75. Edelson, L., & McCoy, D. (2021). Facebook is obstructing our work on disinformation. Other researchers could be next. The Guardian. https://www.theguardian.com/technology/2021/aug/14/facebook-research-disinformation-politics
76. Allyn, B. (2021). Here are 4 key points from the Facebook whistleblower's testimony on Capitol Hill. NPR. https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress
77. Dang, S. (2023). Elon Musk's Twitter lifts ban on political ads. Reuters. https://www.reuters.com/business/media-telecom/twitter-expand-permitted-political-advertising-2023-01-03/
78. Tar, J. (2023). EU Commission's microtargeting ads on controversial law faces fresh complaint. https://www.euractiv.com/section/law-enforcement/news/eu-commissions-microtargeting-ads-on-controversial-law-faces-fresh-complaint/
79. Who Targets Me. (2020). What are we to do about microtargeting? https://whotargets.me/en/what-to-do-about-microtargeting/
80. Takhshid, Z. (2021). Regulating Social Media in the Global South. Social Science Research Network (SSRN Scholarly Paper 3836986). https://papers.ssrn.com/abstract=3836986
81. Venkataramakrishnan, S. (2020). GDPR accused of being toothless because of lack of resources. Financial Times. https://www.ft.com/content/a915ae62-034e-4b13-b787-4b0ac2aaff7e
82. Andere, B. (2021). Data Protection in Kenya: How is this Right Protected? Access Now. https://www.accessnow.org/wp-content/uploads/2021/10/Data-Protection-in-Kenya.pdf
83. World Justice Project. (2023). WJP Rule of Law Index. https://worldjusticeproject.org/rule-of-law-index
84. Oertel, B., Dametto, D., Kluge, J., & Todt, J. (2022). Algorithms in digital media and their influence on opinion formation. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). https://doi.org/10.5445/IR/1000154070
85. AlgorithmWatch. (2023). Social media algorithms are harmless, or are they? https://algorithmwatch.org/en/are-social-media-algorithms-harmless/
86. Brandon, J. (2021). Are You Angry? Facebook Loves You. Forbes. https://www.forbes.com/sites/johnbbrandon/2021/10/28/are-you-angry-facebook-loves-you/
87. Merrill, J. B., & Oremus, W. (2021, October 26). Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation. Washington Post. https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/
88. Booth, R. (2014). Facebook reveals news feed experiment to control emotions. The Guardian. https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

89. Bryant, L. V. (2020). The YouTube Algorithm and the Alt-Right Filter Bubble. Open Information Science, 4(1), 85–90. https://doi.org/10.1515/opis-2020-0007
90. Epstein, R. (2015). How Google Could Rig the 2016 Election. POLITICO Magazine. https://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548
91. Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proceedings of the National Academy of Sciences, 112(33), E4512–E4521. https://doi.org/10.1073/pnas.1419828112
92. Aljazeera. (2022). Meta sued for $2bn over Facebook posts 'rousing hate' in Ethiopia. https://www.aljazeera.com/news/2022/12/14/meta-sued-for-2bn-over-facebook-posts-rousing-hate-in-ethiopia
93. Klepper, D. (2023, April 24). Twitter changes stoke Russian, Chinese propaganda surge. AP News. https://apnews.com/article/twitter-russia-china-elon-musk-ukraine-2eedeabf7d555dc1d0a68b3724cfdd55
94. Williams, E. M., & Carley, K. M. (2023). Search engine manipulation to spread pro-Kremlin propaganda. Harvard Kennedy School Misinformation Review. https://doi.org/10.37016/mr-2020-112
95. Rennó, R. (2019). Search Result Influence: Reaching voters seeking answers. Tactical Tech. https://ourdataourselves.tacticaltech.org/posts/search-influence/
96. Huszár, F., Ktena, S. I., O'Brien, C., Belli, L., Schlaikjer, A., & Hardt, M. (2022). Algorithmic amplification of politics on Twitter. Proceedings of the National Academy of Sciences, 119(1), e2025334119. https://doi.org/10.1073/pnas.2025334119
97. Beck, B., & Worm, U. (2023). EU Digital Services Act's Effects on Algorithmic Transparency and Accountability. https://www.mayerbrown.com/en/perspectives-events/publications/2023/03/eu-digital-services-acts-effects-on-algorithmic-transparency-and-accountability
98. Conversation, T. (2023). The science behind why social media algorithms warp our view of the world. Fast Company. https://www.fastcompany.com/90943919/the-science-behind-why-social-media-algorithms-warp-our-view-of-the-world
99. Milmo, D., & editor, D. M. G. technology. (2021). Twitter admits bias in algorithm for rightwing politicians and news outlets. The Guardian. https://www.theguardian.com/technology/2021/oct/22/twitter-admits-bias-in-algorithm-for-rightwing-politicians-and-news-outlets
100. Diplo. (2023). Nationa AI policies in Africa. https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-national-policies/
101. Maffioli, D. R. (2023). AI regulation in Latin America: Balancing global trends with local realities. https://iapp.org/news/a/ai-regulation-in-latin-america-balancing-global-trends-with-local-realities/
102. Sharma, G. (2022). AI Governance: The 'regulatory bottleneck' in the Global South. Hertie School. https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/ai-governance-the-regulatory-bottleneck-in-the-global-south
103. Applied Law & Technology Ltd. (n.d.). AI Governance in Africa. https://ai.altadvisory.africa/governance/
104. Lewis Silkin. (n.d.). AI regulation around the world. https://www.lewissilkin.com/en/insights/ai-regulation-around-the-world

7 Recommendations

Understanding PMT and persuasive technologies better is important to encourage benevolent uses and regulate against harmful applications. However, countries seem to be taking quite disparate steps towards achieving this. We strongly encourage policymakers around the world to begin devoting attention to the matter now, if not already the case. Based on our research for this report, we have developed a set of fairly universal recommendations that are specified for three groups of stakeholders: governments and political actors; users; and actors engaged in development cooperation. As PMT intertwines closely with the social media platforms on which much of it is distributed, and since it often contains disinformation, many of the recommendations can be equally applied more widely to platform regulation and towards tackling polarization and disinformation in general. We have attempted to formulate these recommendations so that they are practical and actionable, and it is our hope that they will encourage readers to take action.

7.1 Recommendations for governments and political actors

Persuasive technologies and PMT in particular are starting to receive policy attention in countries around the world. Given the many gaps in identifying and understanding the various forms of PMT, taking note of the efforts trying to grasp their impacts, and in order to curtail their harmful effects, governments and political actors are advised to consider the following set of recommendations.

7.1.1 Make concrete efforts to regulate PMT

PMT poses serious risks and harms for individuals and governments alike. As discussed in Chapter 3.2 of this report, PMT can threaten the autonomy and privacy of individuals as well as jeopardize national sovereignty and endanger the very foundations of democratic processes and institutions. Given the growing presence of PMT in the online media landscape, it is crucial that lawmakers around the world earnestly investigate PMT and ensure the transparency and accountability of political advertising through appropriate regulatory action. Countries have made varying levels of progress in terms of identifying the various forms of PMT and developing regulatory responses, which has led to the emergence of a range of policy options. These policy options have their respective benefits and challenges, the impact of which also often depends on the specific country context (see Chapter 6.4 for a detailed review of existing policy options.)

7.1.1.1 SET STRONG TRANSPARENCY OBLIGATIONS AS A MINIMUM REQUIREMENT

Transparency underpins the accountability of any media space or political actor. Both the identification and collection of necessary evidence to regulate PMT and the ability to carry out informed public discourse on PMT hinge on transparency. Requiring online media platforms to exhibit user-facing transparency notices and reforming campaign finance laws to command full transparency are areas where transparency obligations would be particularly impactful (see Chapter 3.2.3 for a discussion of the many processes where transparency plays a central role.)

7.1.1.2 ADOPT PRELIMINARY PROTECTIVE MEASURES WHERE SUITABLE REGULATION OF PMT IS NOT IN PLACE

In sight of the substantial and urgent risks that PMT introduces and owing to the often lengthy time horizons involved in developing regulatory solutions, preliminary protective measures (such as strong transparency obligations or restrictions in the use of PMT) should be adopted while a regulatory response is being developed.

7.1.1.3 FOLLOW A MULTI-STAKEHOLDER APPROACH IN REGULATORY DEVELOPMENT

The development of regulatory responses to PMT should involve diverse stakeholders, especially academia and civil society, to ensure sustainability. While firms such as online platforms tend to be active in developing their own responses to PMT, their influence in the regulatory processes related to PMT should be curtailed owing to their vested interests in profiting from PMT.

7.1.1.4 RECOGNIZE THE LIMITATIONS OF RELYING ON TRANSPARENCY, INDUSTRY SELF-REGULATION, AND CONSUMER EDUCATION

The complexity and seriousness of PMT warrants governments to take action beyond transparency obligations and consumer awareness campaigns. The capacity or interest of companies to self-regulate around PMT should not be relied upon either, as recent experience with the digital advertising industry failing to ensure ethical data practices has shown (see Chapter 6.5.2 for a more detailed discussion of this topic).

7.1.1.5 ACCOUNT FOR LOCAL AND CONTEXTUAL FACTORS

Local situations as well as contextual factors and limitations should be considered in the regulatory approaches related to PMT (see Chapter 5 for a more detailed discussion on local factors). Regulatory instruments or tools developed within a certain jurisdiction may not readily apply to another where local and contextual factors differ. For example, where regulatory authorities have limited enforcement capacity for intricate regulatory instruments (common in structurally disadvantaged countries), a temporal or complete ban on PMT may be more likely to have an effect than spending caps or limits on the quantity of political ads within a campaign.

7.1.1.6 MONITOR AND REFLECT THE ADVANCES IN PERSUASIVE TECHNOLOGIES

The regulatory efforts and their underpinning frameworks need to stay abreast of the developments in persuasive technologies to remain effective. Novel persuasive technologies and tools, such as generative Artificial Intelligence, should be subjected to fundamental rights impact assessments before being deployed (see Chapter 8 for a more detailed discussion of the relevant technological trends that are likely to influence the opportunities and challenges related to PMT in the short term.)

7.1.1.7 PROTECT NATIONAL SOVEREIGNTY FROM FOREIGN INFLUENCE VIA PMT

Where PMT is not banned, the threat of foreign influence through PMT could be addressed through adopting clear rules for foreign actors, such as forbidding funding of PMT by foreign actors. This may be particularly important in political environments that experience significant disruption from external influence.

7.1.1.8 CAREFULLY WEIGH THE THREATS TO FREE SPEECH POSED BY A MORE STRINGENT REGULATION OF POLITICAL ADS

More stringent regulatory approaches to political communication to curtail the negative effects of PMT should be codified and implemented in a way that reduces the potential for abuse by authoritarian actors. This may be particularly relevant in fragile political contexts, in countries where anti-democratic tendencies are present, and in situations where the use of PMT contributes to an uneven playing field between political parties (see Chapter 3.2.5 for a more detailed discussion of this topic). To minimize the potential for abuse, proposals for regulatory legislation should be consulted among diverse stakeholders to ensure that regulations conform with national and international standards, laws, and fundamental rights, including free speech.

7.1.2 Oblige online platforms to allocate sufficient resources and personnel to appropriate content moderation

Social media platforms' tendency to neglect proper content moderation poses a challenge, which can be particularly prevalent in the Global South and in the context of minority languages.[1] Even where content moderation is in place, the capabilities for it may not be sufficient. Posts that violate the rules set by the platform have ended up being approved, for instance in the context of the recent Kenyan election, in both English and Swahili,[2,3] as well as during the genocidal campaign against the Rohingya Muslim minority in Myanmar.[4] Governments could thus require platforms to dedicate requisite resources towards appropriate content moderation, with quality criteria such as the existence of redress options for users whose content was unjustly removed (overblocking) or whose reports of illegal content were disregarded (underblocking).

7.1.3 Secure platform data access to independent, vetted researchers

In order to open up the "black box" that social media platforms frequently resemble and improve oversight, it is crucial for independent researchers to gain insights into their inner workings.[5] This includes how the respective companies conduct content moderation, but also how they rank the content to be displayed on their websites by delving into their algorithms.[6] In the past, however, major players have shown disinterest towards granting such access, or even open hostility: In the case of Berlin-based NGO AlgorithmWatch's Instagram research project, Meta threatened to take legal action which led to the project's discontinuation. Platforms argue that such investigations could threaten trade secrets.[7] To account for this concern, a suitable solution is to introduce a researcher vetting system by neutral third parties. Then, only trustworthy experts from academia, civil society, and journalism can analyse how algorithms function. This would also end platforms' quasi-monopoly over relevant data and allow for better situational awareness through research into the scale and social impact of digital issues such as disinformation and hate speech. Therefore, we recommend a regulation which clearly mandates access, without legal loopholes (cf. Leerssen 2021),[5] for independent, vetted researchers—so that their important work can later on inform tailor-made policy responses.

7.1.4 Act collectively/collaborate with other countries in devising PMT regulation and other strategies to manage its harmful impacts

Social media platforms and the Big Tech companies behind them are powerful and impactful economic entities capable of repressing critical discourse and regulatory efforts. It is challenging for a single country to muster the legal and economic resources for developing regulatory action and the issue is compounded for poorer countries with even scarcer resources (see Chapter 6.5.3 for a discussion of the challenges of regulating PMT). Governments could forge or turn to existing regional alliances or governance frameworks to build an understanding of PMT and to develop regulation that addresses the issues raised by PMT. Collectively generated approaches such as country alliances or regional harmonization efforts,[8] or even regional treaties,[9] have been proposed as potentially effective ways to address the issues posed by PMT. Some suggest that only approaches concerted at the regional or international level can tackle some of the policy challenges introduced by PMT, considering the transnational nature of social media.[10]

7.1.5 Refrain from spreading false or misleading information

PMT is closely associated with misinformation and disinformation. Political actors should be mindful of these as well as of the potential problems in using PMT within their campaigns, to avoid harming democracy and damaging their own credibility and reputation. Specifically, political actors should not disseminate false or otherwise misleading information, neither through PMT, nor other avenues.

7.1.6 Bolster democratic resilience

The resilience of democratic institutions and processes can alleviate the ill effects of PMT on citizens and the political system (see Chapter 5.5 for a review of democratic resilience and its relation to PMT). As previously discussed, suitable legislation to curtail harmful applications of PMT is a central safeguard, but efforts to nurture democratic resilience are important complementary measures. Even where a total ban exists on PMT, some forms of PMT (e.g., political ads spread through encrypted messaging apps) will be difficult to completely eradicate. Measures to support democratic resilience such as the ones elaborated on below can help mitigate the negative impacts of PMT.

7.1.6.1 BUILD PUBLIC AWARENESS OF PMT

Given the increasingly fractionalized media landscape and the growing prevalence of PMT, citizens are likely to encounter its multiple forms regardless of the regulatory efforts by government actors. Public awareness campaigns about PMT and investments into digital, media, and information literacy skills of the citizenry will provide them with the skills and capacities to recognize PMT and critically evaluate the veracity of the political messages. These measures would address both consumption and sharing of PMT and could be delivered by political actors, civil society organizations, or media actors. Older demographics may be a particularly central constituency whose critical online media skills require improvement.[11] Besides education on persuasive technologies, awareness campaigns should also improve peoples' ability to identify and prevent the spread of misinformation.

7.1.6.2 NURTURE PUBLIC INTEREST RESEARCH ON PMT AND DISINFORMATION AND SUPPORT RELATED PUBLIC DISCOURSE

Independent research efforts can shed light onto areas relevant for public interest, such as the extent of PMT use and its impacts, disinformation campaigns, and the use of AI-based technologies in political campaigning. Such research projects should be coupled with effective ways to publicly disseminate their findings and effort should be made to foster public discourse around them. There are many research gaps about the potential positive and negative impacts of PMT as well as regarding the extent of the phenomenon in fields related to development, including education, health, climate change, and gender equality,[12] which independent research could address. Many of the existing research institutes working on technology policy are not independent of leading tech companies such as Google, Meta, Microsoft, and Amazon, underlining the importance of continued efforts to protect the independence and impartiality of public interest research.[13,14]

7.1.6.3 NURTURE MEDIA PLURALISM

Nurturing a plurality of media outlets may limit the impact of PMT through encouraging diversified perspectives and reducing the ability of PMT to be calibrated for use around a single dominant platform or media outlet. In fact, using multiple social media platforms has been linked to lower political polarization.[15] A more diverse media landscape could be achieved, for instance through ensuring sustainable investment in high-quality public broadcasting and promoting a variety of independent media outlets. Introducing services that deliver fact-checking and publish credibility indices, or a media service that assists citizens in navigating among the various media outlets have been suggested as potentially helpful options, especially when organized by actors outside the public sector.[15]

7.1.6.4 DEVELOP AND SUPPORT CAPACITY FOR FACT-CHECKING

Independent fact-checking services verifying the accuracy of messages posted on media platforms have become increasingly available over the last few years. In the Global South, some of the most prominent fact-checking media organizations include AfricaCheck, operating in various countries in the region, Chequeado working in Argentina, Aos Fatos in Brazil, and BOOM with presence in India, Bangladesh, and Myanmar.[16] While these organizations' work can be made more effective with strong links to social media platforms resulting in flagged content being deleted from the platforms, strong financial dependencies from the platform companies are problematic. Such organizations often struggle with funding. While substantial funds may be available from platform or AI companies, it is important to be aware of the potential conflict of interest and rather aim for a secure sustainable funding that ensures the organizations' independence.

7.2 Recommendations for users

While governments are making headway with regulation of persuasive technologies, there are many forms of PMT and disinformation that users of digital platforms, search engines, and other digital tools encounter frequently. To limit the ill effects of those encounters, individuals are advised to take an active role in educating themselves about PMT and follow the recommended actions below.

7.2.1 Protect your privacy

Be aware and mindful of your information seeking and sharing activities online as your demographic data and your behaviour related to your interests and political views can be used for PMT. To avoid falling victim of surveillance, manipulation, and other abuses of the digital traces created by your online presence, you should protect your privacy, for instance through the use of privacy-enhancing tools (such as a browser extension to prevent unwanted tracking of your activities); adjusting your privacy settings across the devices, apps, and services you use; and choosing messaging apps, search engines, web-browsers, social platforms, and email providers that focus on privacy.[xxvii]

7.2.2 Block ads[xxviii]

You can limit your exposure to unwanted ads, including personalized political ads, through adopting ad-blocking tools. These tools (e.g., browser extensions) can automatically block ads on search engines, web browsers, and social media platforms, among other websites. However, the functionality of services may be reduced.

7.2.3 Become a critical consumer of information

Given the complexity of today's communications and media landscape, and the presence of misinformation, disinformation, and powerful manipulation efforts including harmful forms of PMT, individuals are advised to develop strong skills and abilities to critically evaluate information, whether text-, image-, or audio-based. There are several steps you can take towards developing critical media literacy:

7.2.3.1 BE VIGILANT WHEN EXAMINING POLITICAL MESSAGES

Approach messages that address social, political, or election-related issues critically, regardless if the content is paid or unpaid. Try to think what motivation the producer of the content may have and evaluate how reliable it may be. Where you notice that the content raises strong emotions within yourself, whether positive or negative, be particularly mindful of your reaction, as disinformation often aims to elicit a strong emotional response from the receiver. Educate yourself about PMT and disinformation so that you are better equipped to spot these phenomena and be aware of their potential harms.

7.2.3.2 SHARE INFORMATION RESPONSIBLY

Make sure to only share information that is truthful. If you share misinformation or disinformation, you contribute to the prevalence of this challenging phenomenon and risk others to view your future content as less genuine. If you notice that you have shared misinformation or disinformation in error, it is good practice to remove the associated post and publish another message explaining why you removed it, encouraging others to disregard the content of that message.

7.2.3.3 USE THE INFORMATION PLATFORMS GIVE YOU

Make use of the labels and contextualization of political posts and messages that platforms provide. A number of social media platforms have started to display a warning symbol or disclaimer next to content that is likely false or misleading. Some messaging services label shared messages according to whether the sender typed it themselves or whether it was forwarded by another user. They may also indicate the number of times the message has been forwarded. In many countries, progress is underway to identify political ads on platforms and explain who targeted the ad towards the user and on what basis.

7.2.3.4 CROSS-CHECK INFORMATION BY COMPARING ALTERNATIVE SOURCES

Where you are unsure of the correctness of a political message, cross-check it from a trusted source or across multiple sources where you may not be familiar with how trustworthy a particular source is. When multiple trustworthy media report the same message, it is more likely to be truthful, whereas conflictual views indicate that you may want to question the message. Fact-checking services and tools can help you to verify the trustworthiness of messages.

7.2.3.5 REFLECT ON YOUR PERSONAL BIASES—AND LOOK OUT FOR CONFIRMATION BIAS

All of us have biases which involve tendencies to favor and dislike certain people, things, and phenomena. While we hold some of our biases consciously (conscious or explicit biases), others are unconscious assumptions or perceptions that we are often unaware of (unconscious or inherent biases), which may even be in direct contradiction with our beliefs and values, and which impact our opinions and behavior. Confirmation bias is a name for the tendency to navigate towards evidence that confirms our pre-existing beliefs and expectations. Many of us are additionally susceptible to social bias, whereby most of our social interactions take place with others who hold similar values and therefore risk creating "echo chambers", which are particularly vulnerable for being influenced intentionally or unintentionally.[18] Part of being a critical consumer of information is to be aware and reflect on one's personal biases, beliefs and attitudes, as well as on socially created biases.[xxix]

7.2.3.6 REPORT INAPPROPRIATE POLITICAL CONTENT

If you come across political messages or other political content that infringes your personal integrity, standards, or expectations, that violates rules set by platforms, or that is unlawful, make sure to contact the platform in question. All major platforms (including Facebook, X,

[xxvii] For more concrete examples, see the Tactical Tech's Resource Center.[17]

[xxviii] While blocking ads can help avert the risks of PMT and provide individual users with a more streamlined online experience, it can have repercussions for those who are dependent on digital ads as a source of income (e.g., journalists and online content creators). Policymakers should consider the broader implications of ad blocking on the ecosystem of content creation and distribution. Alternative funding models may need to be explored to sustain quality journalism.

[xxix] A helpful resource to identify confirmation bias and other logical fallacies can be found at https://yourlogicalfallacyis.com

YouTube, and WhatsApp) have mechanisms for users to report issues related to various types of content such as ads, posts, messages, pages, videos, or images.

7.2.3.7 HELP OTHERS TO NAVIGATE PMT AND DIRECT THEM TOWARDS TRUSTWORTHY INFORMATION

Given the prevalence of PMT, misinformation, and disinformation, you will likely come across a friend or relative sharing a problematic post. When this happens, do let the person know that you suspect the message to not be trustworthy and refer them to a reliable source. Be prepared that strong feelings may be involved, try to take a kind and positive attitude, and make sure to not make the person feel belittled.

7.2.3.8 STAY INFORMED ABOUT POLITICAL ISSUES AND THE VIEWS OF THE ELECTORATE

To meaningfully participate in the democratic processes and to know whether information about social, political, or election-related topics is true or misleading, one must stay informed about key events and, ideally, have a sense of the values, beliefs, and attitudes held by other constituents or groups of citizens.

7.2.3.9 REVIEW YOUR INFORMATION DIET AND EXPOSE YOURSELF TO OPPOSING VIEWS

Related to reflecting on your personal and social bias, review whether your information diet may also be affected by machine bias, i.e., the way in which the algorithms built into social media platforms and increasingly into major news platforms shape the information you view and consume. Try to diversify the sources from which you access your content and include generalist or traditional media outlets to reduce the influence of content prioritizing algorithms. Examine whether you may be caught in a filter bubble and try bursting it by seeking information from sources that hold different values to yours.[xxx]

7.3 Recommendations for development cooperation

Through development cooperation and multi-sectoral collaboration and learning, industrialized democracies could support low- and middle-income countries to bolster resilience against disinformation and persuasive technologies.

7.3.1 Support capacity-building for informed policymaking

Development actors could support their partner countries in the Global South by allocating funding for these countries to organize capacity-building efforts. These could aim to devise evidence-based digital policy positions on data-driven and personalized political communications as well as on disinformation, taking into consideration the impacts of generative AI and other emerging technologies. Such capacity building could involve trainings tailored to policymakers and other political actors.

7.3.2 Strengthen the development of digital skills and critical media literacy

Development actors could support their partner countries in the Global South in terms of developing digital skills, to strengthen the general population's capacities to navigate the Internet and social media platforms safely, especially while trying to stay abreast of political issues. Development actors could also offer support towards improving the general critical media literacy to enhance people's ability to critically evaluate political communication.

7.3.3 Facilitate research into digital political communication and foster civil society activity around the topic

Development actors could allocate funding towards institutions and initiatives that produce research investigating the impacts of persuasive technologies in the Global South. Development actors could also support the work of civil society organizations around related topics, such as digital rights, platform regulation, and promotion of democracy, for instance through nurturing a diverse media landscape and supporting fact-checking services and efforts to monitor disinformation.

7.3.4 Support representation and participation of the Global South in relevant international networks, fora, and decision-making bodies

Development actors could offer the necessary support to enable representatives from countries in the Global South to more actively participate in discussions about efforts to regulate persuasive technologies and share their perspectives. The harmful impacts of persuasive technologies such as PMT are worsened in contexts with low digital skills and media literacy. International efforts to facilitate regulation of persuasive and other technologies and to create alternatives should include diverse perspectives, especially from these contexts.[12] Development actors could support partner countries in the Global South to develop and reinforce regional alliances to increase their power and political influence, which would also help respective governments in liaising directly with tech companies and platforms. Development actors could also enable knowledge exchange and learning between sectoral stakeholders such as governments, academia, and those working on technology issues across countries.[12]

[xxx] For examples of diverse news stories, you may find the following sources helpful: Global Voices,[19] Project Syndicate,[20] and The Syllabus.[21]

References

1. Malik, N. (2022). How Facebook took over the internet in Africa – and changed everything. The Guardian. https://www.theguardian.com/technology/2022/jan/20/facebook-second-life-the-unstoppable-rise-of-the-tech-company-in-africa
2. Global Witness. (2022). Facebook approves ads calling for ethnic violence in the lead up to a tense Kenyan election. https://www.globalwitness.org/en/press-releases/facebook-approves-ads-calling-ethnic-violence-lead-tense-kenyan-election/
3. Global Witness. (2022). Facebook unable to detect hate speech weeks away from tight Kenyan election. https://www.globalwitness.org/en/campaigns/digital-threats/hate-speech-kenyan-election/#:~:text=Despite%20the%20risk%20of%20violence,the%20country%3A%20Swahili%20and%20English.
4. Global Witness. (2022). Facebook approves adverts containing hate speech inciting violence and genocide against the Rohingya. https://www.globalwitness.org/en/campaigns/digital-threats/rohingya-facebook-hate-speech/
5. Leerssen, P. (2021). Platform research access in Article 31 of the Digital Services Act: Sword without a shield? Verfassungsblog. https://doi.org/10.17176/20210907-214355-0
6. Meyer-Resende, M., & Straub, M. (2022). The Rule of Law versus the Rule of the Algorithm. Verfassungsblog. https://doi.org/10.17176/20220328-131300-0
7. Kayser-Bril, N. (2021). AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook. AlgorithmWatch. https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/
8. GIP Digital Watch Observatory. (2021). Regulating digital platforms from and for the Global South. GIP Digital Watch Observatory. https://dig.watch/event/igf2021/regulating-digital-platforms-from-and-for-the-global-south
9. Takhshid, Z. (2022). Regulating Social Media in the Global South. Vanderbilt Journal of Entertainment and Technology Law, 24(1). https://scholarship.law.vanderbilt.edu/jetlaw/vol24/iss1/1
10. UNCTAD. (2019, September 4). Global efforts needed to spread digital economy benefits, UN report says. https://unctad.org/press-material/global-efforts-needed-spread-digital-economy-benefits-un-report-says
11. Corpus Ong, J., Tapsell, R., & Curato, N. (2019). Tracking Digital Disinformation in the 2019 Philippine Midterm Election. New Mandala. https://www.newmandala.org/wp-content/uploads/2019/08/Digital-Disinformation-2019-Midterms.pdf
12. Kumpf, B., & Hanson, A. (2021). Reshaping social media: From persuasive technology to collective intelligence. In: Development Co-operation Report 2021: Shaping a Just Digital Transformation. OECD. https://doi.org/10.1787/ce08832f-en
13. Kröger, J. (2022). A Note on the Independence of Internet Research. In: Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors (pp. 234–235). Doctoral dissertation. Technische Universität Berlin. https://www.researchgate.net/publication/367636082_A_Note_on_the_Independence_of_Internet_Research
14. Clarke, L., Williams, O., & Swindells, K. (2021). How Google quietly funds Europe's leading tech policy institutes. New Statesman. https://www.newstatesman.com/science-tech/big-tech/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes
15. Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. Social Science Research Network (SSRN Scholarly Paper 3409279). https://doi.org/10.2139/ssrn.3409279
16. Oliver, L. (2021). The fight for facts in the Global South: How four projects are building a new model. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/news/fight-facts-global-south-how-four-projects-are-building-new-model
17. Tactical Tech. (2023). Identifying and Responding to Misinformation. The Digital Enquirer Kit. https://digitalenquirer.org/en/identifying-and-responding-to-misinformation/
18. Ciampaglia, G. L., & Menczer, F. (2021). Biases Make People Vulnerable to Misinformation Spread by Social Media. Scientific American. https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/
19. Global Voices. (2023). Citizen media stories from around the world. https://globalvoices.org
20. Project Syndicate. (2023). Project Syndicate—The World's Opinion Page. https://www.project-syndicate.org/
21. The Syllabus. (2023). Welcome to The Syllabus. https://the-syllabus.com/

8 Outlook

As we look ahead to the near-term future, the landscape of PMT is set to undergo significant developments and advancements. While technological innovations may offer benefits in terms of campaign efficiency and voter engagement, they may also increase the risks associated with PMT and should be monitored and addressed in a timely manner.

Key developments will likely be observed in the following areas:

- **Data collection and analysis technologies:** The proliferation of modern sensor-based technologies, such as Internet of Things (IoT) devices, wearables, voice assistants, and smart homes, offers an unprecedented level of insight into people's private lives.[1,2] New possibilities through modern data analytics, eye-tracking data,[3] voice recordings,[4] and data from seemingly innocuous smartphone motion sensors,[5] for instance, may reveal people's biometric identity, gender and age, mental and physical health, personality traits, emotions, interests, habits, and socioeconomic status. Once gathered by data brokers, online platforms or political campaigns, such insights could be integrated into microtargeting strategies and thus lead to more personalized and invasive political campaigns. Advances in facial recognition and emotional analysis could enable campaigns to gauge voters' reactions to specific messages and adjust their strategies accordingly in real-time.[6] Other technological frontiers, such as "mind-reading" technology[7] or genomics,[8] may lead to even deeper insights into people's characteristics and attributes in the near- to mid-term future. The better individuals are known in terms of the abundance of data available about them, the more accurately they can be targeted through PMT. The refinement of psychological profiling techniques could allow campaigns to tailor messages to exploit specific fears, beliefs, or biases more efficiently. Advances in computational processing power (e.g., the possible advent of quantum computing) could exponentially increase data processing capabilities, enabling even more efficient and sophisticated microtargeting efforts.

- **Content delivery channels:** Over the last two decades, the emergence of interactive content delivery channels such as social media or technological devices like smartphones have transformed the way we interact with information and engage in political discourse. These developments have given political campaigns new possibilities to target specific audiences with personalized content (e.g., through online ads, WhatsApp messages or campaign apps[9]). Now, we are witnessing the dawn of a new age of content delivery with the rise of voice assistants, Virtual Reality (VR), and Augmented Reality (AR). New immersive technologies may offer unprecedented opportunities for PMT, allowing campaigns to create realistic and even more interactive experiences that can deeply resonate with voters. Similarly, while still in the early stages, neural interface technologies hold the potential to further revolutionize how we interact with digital systems. These technologies could enable direct communication between the human brain and computers, potentially opening up new avenues for direct influence on perceptions and opinions.

- **Methods for content generation and manipulation:** New AI-powered technologies for the automated generation of media such as texts, images, and videos have the potential to profoundly shape PMT. The ability to create tailored and persuasive content with minimal effort may increase its effectiveness. Furthermore, AI-based content generation increases the risk of disinformation by enabling the rapid creation and dissemination of highly convincing and misleading information, such as deepfakes,[xxxi] which could also be used in deceptive PMT campaigns. Malicious actors could use deepfakes to misrepresent candidates, fabricate events, and create convincing but false narratives to sway public opinion and erode trust in legitimate information sources.

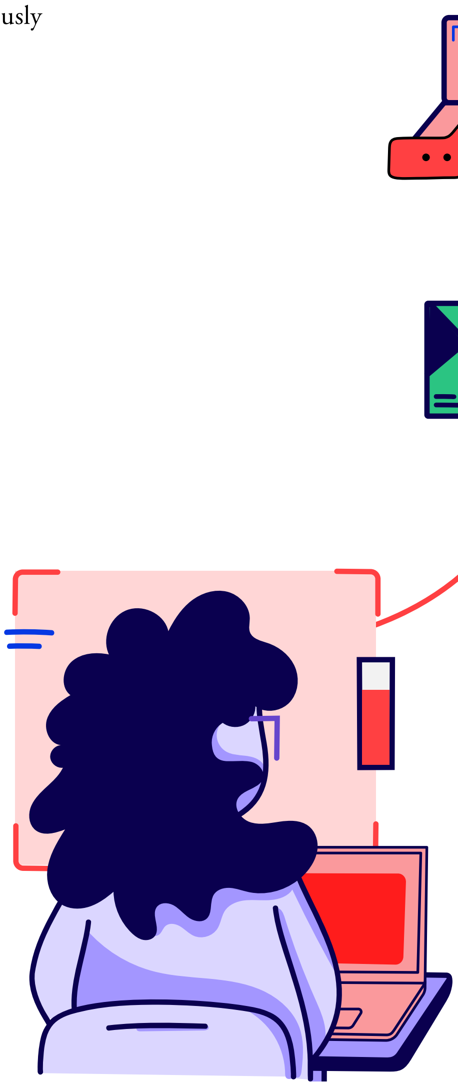
As new technologies continue to evolve, striking a balance between harnessing their benefits and preserving the integrity of democratic processes will remain a pressing challenge for policymakers, technology companies, and society. The ethical concerns surrounding user consent, data privacy, and potential manipulation

[xxxi] A deepfake is a media content, such as an image, video, or audio recording, that undergoes algorithmic editing to substitute the person in the original with someone else (e.g., with the face or voice of a public figure), in a way that appears real.

are substantial and require careful consideration. To ensure the responsible and ethical use of AI in political campaigning and to prevent the misuse of modern technologies for deceptive purposes, stringent regulation and transparency measures will be required. To address these challenges, a combination of various potential approaches is essential due to the complexity of the issue, in order to achieve a functional and effective solution.

Some approaches for regulating the use of AI in content generation and reducing the manipulative potential of deepfakes would be to: (1) mandate clear disclosure when content is generated by AI, (2) implement digital watermarking for media files to help verify the authenticity of content and track its sources, (3) launch public awareness campaigns to educate individuals about deepfakes and AI-generated content, (4) support the development of open-source tools for deepfake detection, (5) incentivize responsible AI usage through ethical guidelines and standards, (6) establish independent auditing and certification processes for AI systems used in content generation, and (7) outline penalties for those who create or distribute maliciously manipulated content for harmful purposes.

To ensure the responsible and ethical use of AI in political campaigning and to prevent the misuse of modern technologies for deceptive purposes, stringent regulation and transparency measures will be required.



References

1. Cheng, P., & Roedig, U. (2022). Personal Voice Assistant Security and Privacy—A Survey. Proceedings of the IEEE, 110(4), 476–507. https://ieeexplore.ieee.org/document/9733178
2. Kröger, J. (2019). Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In L. Strous & V. G. Cerf (Eds.), Internet of Things. Information Processing in an Increasingly Connected World (pp. 147–159). Springer. https://doi.org/10.1007/978-3-030-15651-0_13
3. Kröger, J. L., Lutz, O. H.-M., & Müller, F. (2019). What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In S. Fricker, M. Friedewald, S. Krenn, E. Lievens, & M. Önen (Eds.), Privacy and Identity Management. Data for Better Living: AI and Privacy (pp. 226–241). Springer. https://doi.org/10.1007/978-3-030-42504-3_15
4. Kröger, J. L., Lutz, O. H.-M., & Raschke, P. (2020). Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference. In M. Friedewald, M. Önen, E. Lievens, & S. Krenn (Eds.), Privacy and Identity Management. Data for Better Living: AI and Privacy (pp. 242–258). Springer. https://doi.org/10.1007/978-3-030-42504-3_16
5. Kröger, J. L., Raschke, P., & Bhuiyan, T. R. (2019). Privacy Implications of Accelerometer Data: A Review of Possible Inferences. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP), 81–87. https://doi.org/10.1145/3309074.3309076
6. Alyze. (n.d.). Campaigning in the Digital Age: How Facial Recognition is Revolutionizing Political Strategy. https://alyze.us/blog/campaigning-in-the-digital-age-how-facial-recognition-is-revolutionizing-political-strategy/
7. Devlin, H., & correspondent, H. D. S. (2023). AI makes non-invasive mind-reading possible by turning thoughts into text. The Guardian. https://www.theguardian.com/technology/2023/may/01/ai-makes-non-invasive-mind-reading-possible-by-turning-thoughts-into-text
8. Juda, E. (2017). Genome Analytics: The Battle Between Science and Privacy. Maryville University Online. https://online.maryville.edu/blog/genome-analytics-the-battle-between-science-and-privacy/
9. Tactical Tech. (2019). Campaign Apps: Tap to Participate. https://ourdataourselves.tacticaltech.org/posts/campaign-apps/
10. O'Carroll, L., & Milmo, D. (2023). Musk ditches X's election integrity team ahead of key votes around world. The Guardian. https://www.theguardian.com/technology/2023/sep/28/elon-musk-ditches-x-twitter-election-integrity-team-key-votes-disinformation
11. O'Carroll, L. (2023). EU warns Elon Musk after Twitter found to have highest rate of disinformation. The Guardian. https://www.theguardian.com/technology/2023/sep/26/eu-warns-elon-musk-that-twitter-x-must-comply-with-fake-news-laws
12. Lomas, N. (2023). EU fires urgent warning at Elon Musk's X over illegal content and disinformation following Hamas attacks. TechCrunch. https://techcrunch.com/2023/10/10/eu-dsa-warning-elon-musk-x/
13. The Commission sends request for information to X under DSA. (n.d.). European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953
14. European Commission confirms requests for information on harmful content. (2023, October 26). Reuters. https://www.reuters.com/technology/eus-breton-confirms-investigations-into-three-tech-platforms-including-x-2023-10-26/

9 Conclusion

PMT may offer certain benefits and carries multiple significant risks, making it a complex and contentious issue in the realm of modern political campaigning. While much of the existing research and public discourse on PMT is focused on the Global North, this report has put a focus on the Global South, examining context-specific factors and example cases from Africa, South & Southeast Asia, and South America. The findings suggest that the societal and political risks associated with PMT are at least as serious in the Global South as they are in the Global North—if not more.

The potential for spreading disinformation, reinforcing echo chambers, and manipulating public opinion calls for careful consideration and proactive measures to prevent harm to individuals and groups, and to safeguard democratic processes. As fundamental rights and values such as free speech and the integrity of free and fair elections are at stake, public debate and appropriate regulatory action are urgently needed. The complexity and seriousness of PMT warrants government action beyond transparency obligations and consumer awareness campaigns. Industries' capacity or interest to self-regulate around PMT should not be relied upon, as recent experiences with the digital advertising industry failing to ensure ethical data practices have shown.

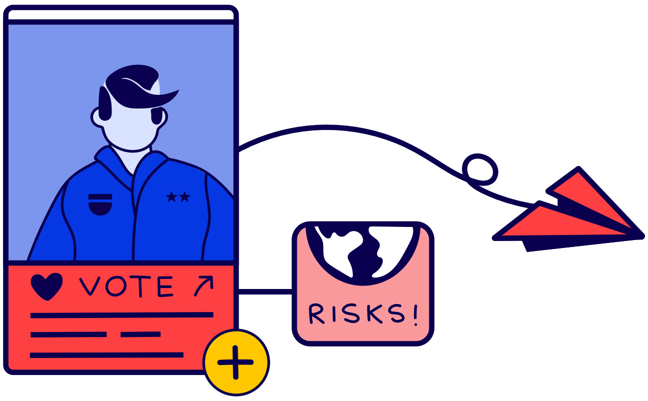
To support informed and timely policymaking, this report has provided an overview of options for regulating PMT, along with their respective advantages, limitations and challenges. It is important to understand that most of the available policy options only address a fraction of the risks associated with PMT. While a legal restriction or complete ban of PMT might be most effective in removing risks, such measures can pose a significant threat to freedom of expression, if not carefully designed. In regulating PMT, policymakers therefore need to strike a delicate balance to protect fundamental rights and public interest. Thus, a carefully constructed policy mix is required, addressing different facets of complex phenomena such as disinformation and hate speech.

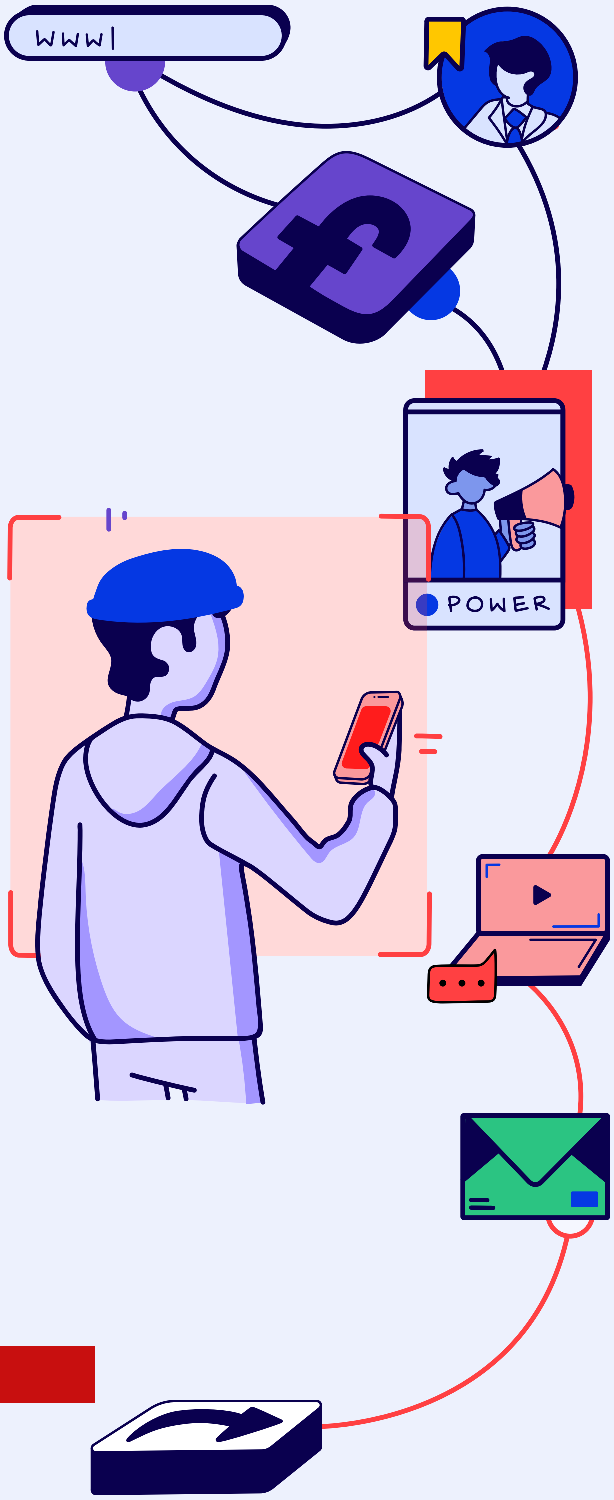
To offer some orientation, this report has provided a set of concrete and actionable recommendations—not only for governments and political actors but also for users and experts in development cooperation.

The global PMT industry is a complex ecosystem, comprising numerous powerful companies. Recognizing the unique challenges and limited resources that low- and middle-income countries face, they are advised to collaborate with other states in devising PMT regulation and strategies to manage its harmful impacts. To ensure sustainability, the development of regulatory responses to PMT should involve diverse stakeholders, especially from the realms of academia and civil society.

In sight of the substantial and urgent risks that PMT introduces and owing to the time horizons required in developing proper regulatory solutions, preliminary protective measures (such as strong transparency obligations or temporary restrictions in the use of PMT) should be adopted while a regulatory response is being developed.

Finally, this report also addressed possible advances in persuasive technologies that may significantly impact the benefits and risks associated with PMT in the near-term future. Given their potential to be abused for disinformation and online manipulation campaigns, these advances need to be monitored and addressed in a timely manner.





Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 32 + 36
53113 Bonn, Deutschland / Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Deutschland / Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

Supported by:

Federal Ministry
for Economic Cooperation
and Development