

Political Microtargeting in Liberal Democracies

THREATS AND RECOMMENDATIONS FOR THE USE OF
ARTIFICIAL INTELLIGENCE IN POLITICAL CAMPAIGNING

LOTTE VAN ELTEREN

Supervisor: Giulio Mecacci
Second reader: Hanna Schraffenberger
S4487478

Table of contents

Abstract	3
Introduction.....	3
Chapter 1: Political Microtargeting and AI	5
History	5
Changes with AI	6
Types of PMT	7
Persuasive microtargeting.....	7
Predictive microtargeting.....	7
Process.....	7
Voter files	7
Voter modelling.....	8
Voter contact.....	8
Chapter 2: Values and threats.....	9
How are some societal values threatened?	9
Liberty.....	9
Equality.....	10
Data security.....	11
Privacy	11
Deliberation.....	13
Character building	13
Transparency	14
Political participation.....	14
Chapter 3: Conceptual tools.....	15
Translating Values to Design Requirements.....	15
Protecting values with policies.....	16
Current policies	16
<i>Europe</i>	16
<i>North America</i>	17
Creating policies	18
Chapter 4: Recommendations.....	19
Liberty.....	19
Design requirement.....	19
Equality.....	20
Policy recommendations.....	20
Data security.....	21

Design requirement.....	21
Privacy	22
Policy recommendation	23
Deliberation.....	23
Policy recommendations	23
Design requirements	24
Character building	24
Design requirement.....	24
Transparency.....	25
Policy recommendation	25
Design requirement.....	25
Political participation.....	26
Design requirement.....	26
Conclusion	28
Limitations	28
Future research	29
Manipulation	29
Misinformation and fake news.....	29
AI for good.....	29
Acknowledgements	29
Bibliography.....	29

Abstract

Political Microtargeting (PMT) is the use of data-driven voter research in personalized political campaigning. It is used to find voters most susceptible to political advertisements, and to tailor the advertising to a voter's specific interests. Previous research has shown that PMT can influence democratic processes. To decide on the validity of this practice, we look at what is valued within a certain type of democracy, and then decide whether or not these values are endangered by the use of PMT. In this thesis we define PMT, and show to what extent AI changed scale and efficacy of it. We then claim that the liberal democratic values of liberty, equality, privacy, data security, development of character, deliberation, transparency and political participation are threatened by its use. Lastly, we provide technical design solutions for designers of microtargeting algorithms that support these values, as well as policy recommendations to regulate the use of these techniques to protect the liberal democratic values.

Introduction

Artificially intelligent technology has an immense impact on democratic states. The development of surveillance technologies raises new questions about the privacy of citizens, automatization of jobs causes global unemployment, and the development of automated weapons changes views on just warfare. Because of this, the European Economic and Societal Committee (EESC) commissioned a report in 2017, highlighting the biggest societal concerns of AI. Among other topics, the report mentions concerns about voter manipulation through AI. This is what is known as Political Microtargeting (PMT). PMT is the use of data-driven voter research in personalized political campaigning. It is used to find voters most susceptible to political advertisements, and to tailor the advertising to a voter's specific interests. This makes advertisement more effective, as it can help to adapt the message and its format to a person's needs, and address issues important to an individual.

In order to do this, large amounts of voter data are needed. Acquiring, storing and analyzing this much data was previously impossible, but with the popularity of social media in the last two decades the doors are open for politicians to use voter information to their advantage. Political parties are becoming increasingly more interested in the effects of technique, especially since the election of president Donald Trump of the United States in 2016 (Cambridge Analytica, 2016). Political consulting firm Cambridge Analytica collected data from Facebook users, and analysed this data to predict voter's behaviour. These predictions have been said to be quintessential in Trump's victory, which indicates the colossal power that AI can have on democratic elections (González, 2017). The question then arises to what extent these practices are legitimate within democracies. Research on the effects of PMT is still largely missing, and the little information that is currently available shows seemingly contradicting results. Some studies focused on how PMT can be used as an aid in democracies, for example by getting voters more engaged in debates and getting more citizens to vote during elections (Holt et al., 2013; Zarouali et al., 2020). However, other studies show that PMT can be harmful to democracies, for example that PMT can induce divisiveness and discrimination, and even threaten the fairness of elections (Barocas, 2012; Groen-Reijman, 2018). It is therefore unclear whether or not PMT should be permissible. To decide on the validity of this practice, we need to look at what is valued within a certain type of democracy, and then decide whether or not these values are endangered by the use of PMT.

In this thesis we define Political Microtargeting, and show to what extent AI changed scale and efficacy of it. We then claim that the liberal democratic values of liberty, equality, privacy, data security, development of character, deliberation, transparency and political participation are threatened by its use. Lastly, we provide technical design solutions for designers of microtargeting algorithms that support these values, as well as policy recommendations to regulate the use of these techniques to protect the liberal democratic values.

We have chosen liberal democracy over other democratic theories because it is the most dominant form of democracies, especially in Europe. Furthermore, it has the most real-world examples to use. If PMT forms a serious threat to the values of a liberal democracy it is paramount that our options are assessed before damages are caused. This project does not aim to give a step-by-step solution for policymakers and creators of AI technology on how to solve the situation. Rather, it aims to give an overview of the dangers, possibilities and stakeholders involved, and outlines the direction of possible regulation, should the risk of PMT be larger than its gains. This can be used by policymakers to further explore solutions in the form of policies and regulations. Furthermore, it explores design perspectives for creators of PMT that feature a value-driven approach.

In order to accomplish this goal we first give an explanation of the concept of political microtargeting, how it is done, and what role AI plays in it. Then, we explore which values of liberal democratic states are threatened by the use of PMT. After this, we explore solutions from two different perspectives: how to design PMT-algorithms in such a way that they can be used within a liberal democracy, and how to protect democracies from maliciously designed PMT algorithms through policy. For the first part we will use the principles of Value Sensitive Design (VSD) (Friedman et al., 2002). This will result in technical solutions that endorse values. The second part will provide directions for policy-makers, outlining the risks and possibilities.

Chapter 1: Political Microtargeting and AI

The term 'Political Microtargeting' was first used during the American presidential election of 2004. Reports show that online microtargeting was used by campaign lobbyists. One of these companies defined the term in a white paper as: "the creation of customized winning messages, proof points and offers, accurately predicting their impact, and delivering them directly to individuals" (Tom Agan Penn & Associates White Paper, 2007). The core of this practice is the use of data analytics, used to craft and tailor the most impactful message to an individual or small group of voters. The message can be conveyed through all sorts of media such as tv ads, newspapers or billboards, but the most popular means at the moment is through social media. Although this thesis mainly focuses on online political microtargeting, it is false to assume that such practices did not exist before the digital era. In this chapter we show what changed in the practice of PMT, and why this change gives reason to investigate the topic in its current and future state.

History

Political microtargeting is often regarded as a new practice that emerged with the widespread use of social media. However, targeting a political campaign to individuals or small groups of voters has been done long before the use of the internet. For example, president of the United States Grover Cleveland kept extensive records of voter demographics for campaign purposes in 1892 (Nielsen, 2012). Political campaigning, which involves getting a message to a voter as well as getting a person to vote for a particular politician or regulation, is an integral part of the proper functioning of democratic states. Proper campaigning engages more voters into the political discourse, and ensures that voters vote for what closest resembles their political values. This contributes to a democratic government's legitimacy (Schultz, 2014). Furthermore, limited resources are also nothing new; politicians have always had a limited budget to campaigning, so getting a message to the most likely to be persuaded voters has been important long before the invention of the internet and social media (Ryabtsev, 2020). The main differences with the past are the channels through which a voter receives a message, the efficacy, and the scale in which it is executed.

Political campaigns employ a wide variety of media in order to get their message out to the public. Although the majority of campaigning budgets has shifted to online messages, most of the traditional media are still in use (Dommett, 2019). Examples of these offline campaigning media are flyers, billboards, newspapers and tv and radio advertisements. To get their message to the voter, politicians have needed to compress and summarize their message into something small enough to fit onto these limitedly-spaced media, so finding the optimal message is crucial. Finding the optimal message means finding the phrase or image that persuades the largest number of voters. However, where some message is optimal for one group of voters, it can be suboptimal for another group, for example because they have different interests. Politicians therefore started using voter management databases to keep track of demographic data such as age, gender, address and religion of their voters (C. Bennett, 2014). With these databases, flyers and billboard campaigns could be customized for specific areas in order to have a larger impact. Furthermore, combining voter demographic with radio and tv viewership data meant that specific ads were chosen to be broadcasted during different programs. Additionally, religious groups could have a large impact on elections, so politicians often sought endorsement from churches or other religious institutes in the region they wanted to target (van Wyk, 2005). Another important focal point was, and still is, the appearance of a politician. Attention is paid to the way a politician acts outside of their political duties, such as to the way they dress, or their marital status. Appearing to the public in particular regions means wearing a different outfit, speaking in a different manner or about different topics, in order to appeal in the most optimal way to the community (Scammell, 2016).

In conclusion, political microtargeting is not a completely new phenomenon, nor did it emerge solely from the use of social media. Political advertising has long been the topic of research, especially since the professionalization of political campaigning in the 1980's (Cook & Gronke, 2005). Rather, it should be seen as a practice that has evolved over a long period of time, with a sudden surge in development during the popularization of the internet and social media.

Changes with AI

The voter management databases of the 1980's changed to more integrated voter management platforms. This was mainly due to technological advancements in data storage. As it became increasingly cheaper to digitally store large amounts of data about voters, more information was stored and used for microtargeting purposes. Data capturing became less structured as data mining techniques advanced. This meant that, where data before was often labelled and only gathered if it was deemed immediately relevant, new techniques could find patterns in data that were not directly visible by human analysis. This practice started around the time data brokerage firms started offering their services to campaign managers.

Then, along with this larger capacity for data storage, social media platforms started becoming increasingly more popular. With personal profiles information could be gathered per individual, whereas before most information was gathered on groups of individuals with similar demographics. The availability and analysis of personal information made it possible to target users of social media platforms on specific factors of interest, and tailor political advertisements even more precisely (Kosinski et al., 2014). This meant that campaign messages could become not only more personalized towards individuals, but also cheaper, as mass messaging was no longer necessary. This increased the scale and the efficiency of political microtargeting massively.

The global popularization of the internet and social media has fundamentally changed the way in which political campaigning is done. For example: politicians are less reliant on regular media and journalists to relay their message. They can directly communicate their message to voters through their own channels, which can help messages be truer to source. This idea has been picked up by politicians all over the world, resulting in virtually all politicians having an active social media presence. Furthermore, the internet and social media have become the primary source of information for many citizens in democratic states. A survey in 2017 found that 67% of Americans receive news from social media (Shearer & Gottfried, 2017). With an estimated 2.912 billion active Facebook users (*Meta - Meta Reports Fourth Quarter and Full Year 2021 Results, 2021*), and 436 million Twitter users as of April 2022 (*Twitter Statistics and Trends, 2022*), social media has revolutionized the way in which citizens receive political messages (Eric Jardine, 2019). This change is not only in favor of politicians. The direct contact through social media with politicians allows voters to communicate their issues with politicians, and to feel as if the politicians in their state are more relatable. For example, the electoral success of President Barack Obama in the United States in 2012 can be largely credited to his social media presence (Hannan, 2018). This increase in popularity among politicians can also be seen in campaigning budgets, which are directing progressively more money into online campaigning, especially on social media websites.

The techniques with which information is gathered and turned into useful data for campaigning is still rapidly evolving. The main takeaway from this brief history is the massive change in scale and efficiency that AI has brought, and with it the interest of politicians. The smaller scale and effect of offline microtargeting did not pose a large threat, so regulating its use was not necessary. We argue however, that now PMT is used on a larger scale, investigating regulation is called for.

Types of PMT

Modern, online PMT has not attracted the attention of many researchers yet. Investigation from a technical perspective in particular is meager. So far, two types of political microtargeting can be discerned: persuasive and predictive microtargeting. This distinction is important for our further analysis, because the technical and institutional solutions we will provide can be type-specific.

Persuasive microtargeting

Persuasive microtargeting aims to make a message as attractive as possible. This can be done by tailoring a message to the interests and concerns of the targeted voter. For example, if a political party is aware of a particular interest of a voter, like strategies against climate change, they may choose to feature this issue prominently in the message to that particular voter. Studies have shown that tailoring a message to a person's personality traits significantly increases the persuasiveness of that message (Noar et al., 2007). Tailoring a message can be done in many ways. The typography, language, images, medium and possibly more factors can be modified to create a more persuasive message (Billard, 2016; Constantinou, 2022; Doherty & Anderson, 2004; Mannetti et al., 2010).

Predictive microtargeting

In predictive microtargeting, a political party tries to predict which group of voters is most likely to respond and act upon their message. Campaigns have limited resources, so it is important to know who to target. For example: a socialist party can choose to focus their campaign resources on the working class instead of on more affluent voters. This technique is however unreliable, because not every working class voter is socialist, and some affluent voters are. Predictive microtargeting therefore focuses on smaller groups or individuals with similar personality traits and interests, instead of larger demographic factors. This becomes especially important when a party has a very diverse base of voters. A political party will try to predict the response of a group of voters, in order to find out who to send which message.

Process

Although the algorithms with which to perform political microtargeting may differ, the overall process usually has three steps. At the base is always the creation of a so-called voter file. From this file a voter model can be constructed. Then, with this model, a message is sent to this particular voter, for example through a personal social media advertisement.

Voter files

To create a voter profile, political parties can access information on individual voters through voter registration databases. In many democratic countries these databases are maintained by local or state governments. The databases contain information about a voter, such as their birthdate, phone number, and address. Some governments register even more information about their voters, such as their race, occupation and need for special assistance at polls (Barocas, 2012). This results in a voter file, constructed by a political party, for each voter in their area or state. The voter files can be enriched by merging them with information from other databases, for example their own information on which people are a member of their party. Most information however is sourced from social media: social media platforms like Facebook and Twitter sell information about their users to political parties. This information, combined with the voter file, results in an enhanced voter file. These enhanced voter files often include more than 900 individual data points per voter, containing highly specific information. However, as storing and mining data becomes cheaper and easier over time, this number is likely to increase (Barocas, 2012).

Voter modelling

The enhanced voter files provide the raw information that is needed to create voter models. These models are digital representations of a particular individual or group of voters. They are made by analyzing the immense amount of data points in the voter files with data mining techniques. These techniques can show correlation between different voter files or data points that exceed traditional demographic categories. The groups may for example contain people that seemingly have not much in common, but may very well respond to a certain message in a similar way.

To predict whether or not multiple voters will have the same response to a message, an important indicator is their personality. It is likely that people with similar personality traits will have a similar response to a message (Hirsh et al., 2012). Moreover, it is also likely that voters will respond positively to a message by a politician with a similar personality trait (Amsalem et al., 2018; Caprara et al., 2003). The more closely the personality of a politician matches that of a voter, the more positive the perception of that politician will be. This is called the *congruency model of political preference* (Caprara & Zimbardo, 2004). It is therefore of interest to a politician to know which personality traits to show off to a particular group of voters.

Voter contact

The voter model is then used to create a political advertisement. The model provides intel on how someone will likely respond to a message. The closer a person resembles the model, the more accurate the prediction will be. This way, a customized political advertisement is created. After the message has been tailored to perfection, it needs to be sent to the voter. Most often microtargeted campaigns use individual contact, such as direct mail, phone calls and social media advertising (Barocas, 2012). Microtargeting to groups of lower granularity is done with tv-advertisements, billboards and canvassing. Although advertising on this lower granularity may seem to be the least straining on resources, anecdotal evidence suggest that campaigning on a high granularity is cost-effective because of the higher chances of a message persuading a voter (Scola, 2012).

Chapter 2: Values and threats

The field of democratic theory is very broad. To say a country is 'a democracy' does not often tell us much about the governmental structure, or even the voting system of that country. Compare for example the constitutional monarchy of the Netherlands with the 'people's democratic dictatorship' of China. Both countries claim to be democratic, but the way in which these countries interpret the theory is very different. Democracy, which is the most generic definition a method of collective decision making, can be thus be a confusing topic (Christiano & Bajaj, 2022). Even limiting the topic in this thesis to liberal democratic theory leaves a lot of room for discussion on what exactly such a democracy looks like. Because of this, we use the Stanford Encyclopedia of Philosophy as a main source of information, supplementing it with more detailed information from other authors. The entry for 'Democracy', by Christiano & Bajaj gives an overview of democratic theory, and some of the values of liberal democracies.

Generally speaking, liberal democracies are characterized by a liberal ideology, meaning that individual rights, freedom and equality before the law are quintessential to citizen's welfare (Courtland et al., 2022). Liberal democratic states mostly use a representative or indirect form of political participation, in which citizens elect a representative that holds the power of decision making. Most liberal democracies have a constitution, and universal suffrage, meaning that all adult citizens have the right to vote. It is however difficult to define a finite list of normative characteristics of liberal democracies, because even within liberal democratic theory there is disagreement about what exactly a liberal democracy should look like. Sub-divisions, such as protective liberal democratic theory and developmental liberal democratic theory focus on different aspects or values, which means that even two liberal democracies can have very different ideologies (Joshi, 2013). For example: a protective liberal democracy values the utilitarian ethical approach of Jeremy Bentham and James Mill, arguing that we should strive to create the greatest net amount of happiness for the greatest amount of people (Macpherson, 1977). If less control over political decisions means that citizens have fewer worries and make fewer bad decisions, then that must be the way forward. Deliberative liberalists however value the utilitarian approach of John Stuart Mill, and argue that not all happiness is equal. Some forms of happiness are of higher value, namely those that employ 'higher faculties', like the happiness derived from intellectual pursuit. Political participation is considered one of these higher faculties, because gives citizens the opportunity to develop their characters (Brink, 2022). They therefore believe that the more informed, involved and deliberative a citizen is within democratic decision-making, the better. This also connects to theories of virtue ethics: the virtues that are emphasized are those of a democratic citizen (Zuckert, 2014).

This shows that finding the universal values of liberal democracies may prove impossible. We therefore chose to approach the problem of finding these values by including values that are common, but not necessary, in order to tackle a wide range of issues. For each of these values we claim that they are threatened by persuasive and/or predictive PMT. Even though, due to lack of research, many effects of PMT are still unknown, we can already find threatening results in the information that is available at this point in time. The values of a liberal democracy we claim to be threatened by political microtargeting are: liberty, equality, privacy, development of character, deliberation, transparency and political participation.

How are some societal values threatened?

Liberty

The concept of liberty can mean many different things. In this thesis, we follow Pettit's definition of freedom as synonymous to liberty. Pettit says that freedom is the opposite of domination (Pettit,

1997). An unfree person is subject to the will of another, and liberal democracies should therefore have no arbitrary power over any citizen (Courtland et al., 2022). Any attempt of politicians to influence the decisions of a citizen without the consent of said citizen, can be seen as a form of domination, and therefore a threat to the value of liberty.

Persuasive microtargeting, which explicitly aim to make a political message as persuasive as possible, are used to influence the political deliberations of a voter. It is important to note that the intent of using this technique is not to correctly inform a voter about certain issues, but to influence the decision they will make about these issues. One could claim that the voter is in theory still free to make their own decisions, regardless of this influence. However, we have reason to assume that freedom of decision is effectively reduced or even taken away when someone is subject to intensive persuasive microtargeting. Experiments by Zarouali et al. (2020) have shown the effectiveness of PMT with personality profiling. They state that: “electoral candidates and political parties might adopt this technique as a persuasive tool during electoral campaigns by tapping into citizens’ psychological dispositions with emotionally-charged political content, and subsequently, impact how these people intend to vote” (Zarouali et al., 2020, p. 20). We can therefore say that the use of political microtargeting, if successful in its aim to influence decisions of voters, threatens the value of liberty. One could also argue that PMT is not different from other methods of campaigning, such as with flyers or posters. We however argue that there is a difference in the effect it has on a voter. PMT is much more effective in persuading a voter than traditional campaign methods. The personalized strategy can be so effective that voters no longer choose to do what is in line with their own values. This does not mean that they are persuaded by rational arguments and deliberation, but rather that the algorithm has been successful in finding exactly what was needed to persuade that person in particular. Is it fair to ask a person to remain rational when they are presented with a message exactly tailored to their interests, emotions and fears? Traditional campaign methods have the same goal as PMT, namely to persuade a voter, but the effectiveness of the method blurs the lines between persuasion and manipulation of behavior.

Equality

The value of equality immediately raises the question: “equality of what?”. One could, in the context of liberal democracies, mean ‘equality of opportunity’, which on itself can mean many different things (Gosepath, 2021). It can also mean ‘equality before the law’, which could mean that everyone should be equally protected under the law, or that everyone should be subject to the same law. In this thesis we tackle three different interpretations of equality, and claim that they are all threatened by the use of PMT.

First, one can value equality in political representation, meaning that different groups of people are proportionally represented in the elected government. Predictive microtargeting, as described in chapter 1, is used to find the target group of voters most susceptible to their message. This could mean that certain groups of voters are ignored during the campaign times, causing them to be less informed about the issues at hand than other voters, and less motivated to cast their vote. Furthermore, this technique can also be used to keep certain groups of voters from voting all together, leaving them underrepresented in the elected government (Borgesius et al., 2018). Additionally, the algorithms used in PMT can be unfairly biased for or against certain individuals. Some PMT algorithms structurally and unfairly neglect the targeting of certain groups of people, for example when this group is highly unlikely to vote. To be classified as an ‘unlikely voter’ means that your personal information shares a significant amount of characteristics with a model ‘unlikely voter’. This model is often created with data from previous elections, and can be highly biased. For example,

if during a previous election an important soccer match was played in Nijmegen, soccer-enthusiasts in Nijmegen may have been less inclined to vote that day. If voter-attendance data in Nijmegen has been used to train the PMT algorithm of the upcoming, the 'unlikely voter'-model may be highly sensitive to people from Nijmegen, regardless of their current inclinations of voting. Biases can be more severe or unpredictable when they are intersecting, which happens when a voter profile contains multiple data points against which an algorithmic bias exists. For example, if this 'unlikely voter' model is also sensitive to wheelchair-users, the likelihood of wheelchair-users in Nijmegen being classified as unlikely voters could be unjustly high.

Second, PMT may pose a threat to equality in the sense that not everyone has equal means to make use of its benefits. PMT can be expensive, which could mean that political parties with more means will be able to use PMT more effectively, and on a larger scale. Because PMT is very effective, this could mean that some political messages will be more prevalent to voters than others.

Lastly, PMT can pose a threat to equality because citizens have varying time and resources to spend on deliberating their political decisions. Christiano (2022) states that some people have the means to be immune to persuasive microtargeting techniques, for example by spending more time researching political parties, or by making use of algorithmic communications. The type of equality that is threatened is that of political informedness. Predictive microtargeting can be used to find out which persons are most susceptible to a message. This can lead possibly to the decision to target and inform some groups of voters more than others. Furthermore, PMT can cause political informedness to be divided even more unequally, because only people with enough resources are able to surpass its persuasive power.

Data security

Data security is the protection of digital data, often stored in a database, from unauthorized or unwanted actions (Summers, 2004). Microtargeting involves collecting vast amounts of personal data. The act of collecting data and storing this data all together in one place makes it more vulnerable to data breaches by hackers, because the incentive to hack a database becomes larger the more data is stored. The negative effects of a data breach can be very large. The data stored for PMT is highly sensitive, as it often contains information about political biases, ethnicity, and opinions on controversial topics. Furthermore, the scale of such data breaches can be very large, as owners of the data often store information about many different voters. In a 2017 data breach scandal in the united states, the US Republican party had data stored of nearly 200 million citizens.

Privacy

Privacy, as defined by Parent (1983), means to have control over information about oneself. This can be with respect to the government, but also with respect to citizens or companies. It is perhaps difficult to understand privacy as a value of liberal democracies, and is often even argued to be harmful when it stands in the way of safety measures. For example, the Dutch Intelligence and Security Services Act (Wiv) of 2018 caused a lot of discussion about this dichotomy (Amnesty International, 2022; Rijksoverheid, 2017). This law allows security services to collect and analyze information of all individuals, including innocent persons, in order to prevent criminality and terrorism. This means that, even when both privacy and security are valued, it seems that sometimes one must be chosen at the cost of the other. Furthermore, liberal democracies also value transparency, characterized by the visibility or accessibility of information. Thus, we need to further specify why privacy is of value to liberal democratic states.

Privacy is often valued from the perspective of the individual. For example, Parent mentions privacy as a facilitator of individuality and personal freedom (Parent, 1983). Others, like Gavison (1980),

value privacy because it leads to autonomy, selfhood and improved interpersonal relations. The benefits of keeping information private seems to be primarily for the person whose information is private. According to Priscilla Regan however, privacy should not only be valued from the perspective of the individual, but more importantly, seen as of value to the democratic political system (Regan, 1995). Regan argues that, when privacy is valued from the perspective of the collective, the dichotomy between privacy and security or transparency is avoided. Privacy is something we should value as a community, rather than on the individual level, because it is integral to the functioning of a liberal democracy. It fosters and encourages the moral autonomy of citizens, self-development and individual integrity, all of which are necessary for the democratic system to work properly (DeCew, 2018; Hoven, 1999; Solove, 2008). Furthermore, privacy rights guard a state against governmental oppression and totalitarian regimes (Moore, 2003). Individuals need privacy, and all of its individual benefits, to perform their democratic duties that benefit the collective. For example, if a person is not autonomous when voting, their vote may not be a result of their own beliefs, which distorts the democratic election outcome. Seeing privacy not only as a benefit to the individual, in contrast to values like security which are often valued on the collective level, could help to relieve some of the tension in these debates. We can however conclude that, in practice, liberal democratic states will nevertheless sometimes have to make decisions that place one value above the other.

Part of the procedure of PMT involves the making of a voter profile. In order to do this, information about citizens is not only sourced from external collectors such as social media, but a large part of it is generated during the process itself. The information is a prediction about a person's characteristics or interest, so may not necessarily be correct. However, as machine learning techniques are becoming more advanced, the chances of the predicted information to be correct are rising. Protecting privacy by choosing not to share information via social media does therefore no longer mean that this information is not, to a certain degree, available to the users of PMT (Crawford & Schultz, 2014). Whereas a citizen may have control over some types of information they share, and even a sense of protection by means of laws such as the GDPR, the actual control they have over their data is debatable (Council of the European Union, 2016a). If an algorithm is very accurate in predicting information about a citizen based on the limited information that is shared, the citizen loses control over their data. Moreover, they may even have the false presumption that their data is safe, because they feel as if they have control over what to share and what to keep private. This therefore threatens the privacy of citizens. If the algorithms used in this process however fail to make accurate predictions, voters may still be negatively affected. They may, through predictive PMT, be placed in a voter category that does not receive targeted messages, and therefore miss out information of importance to them.

Furthermore, the expectation that someone is collecting information about a person can influence the behavior of that person. If people suspect that their behavior is monitored they may choose not to visit certain sources of information (Richards, 2014; Borgesius et al., 2018). This is also known as the Hawthorne effect: the feeling of being observed or merely participating in an experiment can affect individuals' behavior (Schwartz et al., 2013). Citizens that are aware that there are companies or political parties that track their information with the purpose of influencing their political opinion, may therefore be cautious or uncomfortable when visiting sources of information about controversial topics. People may also be afraid of the repercussions of visiting certain sources of information, which is known as the 'chilling effect' (Büchi et al., 2022). For example, a person may be hesitant to look up information about LGBTQ+ events if they suspect a political party that supports the prosecution of queer persons to gain power in the next elections. One could argue that this influence on a voter's behavior and sense of privacy threatens their liberty.

Deliberation

The value of deliberation is most prominent in the deliberative liberal democratic theory. This type of liberal democracy values that citizens rationally deliberate their decision, are aware of their options, know what the effects of their decisions are and choose the option they believe is the most in line with their own beliefs. Furthermore, they are aware of the arguments that support their decision (Habermas, 1994). This in turn will result in a government representative of its citizens, because the voters are less likely to vote for the 'wrong' candidate. To deliberate a decision therefore involves correct information, and an appropriate amount of time and resources spent on figuring out which option is best. A successful deliberation will result in a choice representative of one's beliefs, desires, and intentions.

Persuasive microtargeting is problematic in this regard because it can prevent deliberation from resulting in a choice most in line with a voter's beliefs. If a decision is to be made from rational arguments, the personality traits and interests of the voter should not be of interest for the message that is sent. Persuasion PMT is effective partly because it relies on non-rational persuasion, such as creating a public persona for a politician that is similar to that of the voter. If this persona becomes part of the reasoning behind a decision, even, or perhaps especially when the voter is unaware of this, the value of deliberation is threatened.

Predictive microtargeting threatens deliberation from a different perspective. Election campaigns are crucial to help voters be aware of certain issues and the solutions that different parties propose. The risk of PMT is that the likelihood of a person to act upon a certain message decides whether or not this person receives a message. Predictive microtargeting focuses on getting the message to the most likely to be persuaded group of voters. When certain voters are excluded because they are not expected to be persuaded, they are likely to miss out on information distributed through campaigning. This will in turn limit their deliberative process.

Character building

Philosophers like Mill and Rousseau believe that living in a democracy has a positive effect on the character of a person (Christiano, 2022). For example, democratic citizens often stand up for themselves, and being active in political decision-making cultivates active, moral, and productive character traits. This effect that living in a democracy has on citizens is, among other reasons, due to the promotion of active deliberation and participation in politics. A state in which character building is optimally promoted should provide the voter with all necessary information to deliberate a decision, and the means to deliberate and be active in the decision-making process. Furthermore, the further development of character can be promoted by stimulating the engagement with a wide range of topics and discussions, which can enrich a person's knowledge and develop critical thinking skills. If these factors are thwarted by PMT, then this may have an effect on the character of the citizens.

Persuasive microtargeting often uses character traits and interests derived from social media data to create a voter model. If a targeted message is created on the basis of these modelled personality traits, this may stand in the way of the development of other interests and traits. For example, a voter model that includes a lack of interest in a particular topic, may result in not presenting this topic to the respective voter at all. After all, it is costly and it likely has little effect. This means however, that this voter may never learn about new issues and possible interests, because they are never presented to them. Furthermore, it can even deeper ingrain certain beliefs, leading to

polarization. A similar effect has been studied in relation to personalized searches on website algorithms leading to 'filter bubbles' (Bozdag & van den Hoven, 2015). When people are not presented with a balanced information diet, but only see information that targets their established interests, then they may end up in a state of intellectual isolation. This means they are separated from different viewpoints and counterarguments to their own beliefs. It is possible that the personally curated messages of PMT algorithms have a similar effect on a person's political views, which may lead to political polarization. If people are not able or willing to engage with the topics outside of their own political bubble, the development of their character is inhibited.

Transparency

In order for a voter to make the decision most in line with their ideals, deliberation needs to take place, based on the correct information. Incorrect, or incomplete information, will lead to a vote that does not represent the voter. Therefore, political parties need to be transparent when presenting information.

The use of persuasive PMT begs the question of how transparent a party is when campaigning. If PMT is used to find the message that is most persuasive to the voter, it could mean that this message is not actually reflective of a political party's ideology. The political party may then choose to misrepresent themselves. This can obviously be seen as a malicious practice, but even when the information in the message is correct, a party can misrepresent itself. A campaign message always only shows part of a party's ideology, because the space and resources are limited. Choosing not to advertise certain parts of their political plans is therefore inevitable. However, when a party highlights certain issues, and hides others, it could present itself misleadingly as a one-issue party. The 'one' issue they choose to present can differ for each targeted voter, tailored to that person's interests. This may lead to a biased perception of that party. When a political party uses PMT to achieve this goal, and hides their views on certain topics in order to be more persuasive, this threatens the transparency of the campaign (Borgesius et al., 2018).

Political participation

Democracies require political participation of citizens to function. What form this participation takes will differ for each democratic theory. Most liberal democracies however, require citizens to vote for a representative, and the success of an election is measured by the degree to which it reflects the opinion of its voters. When few people vote for their preferred politician or party, the result may be that the elected representatives do not reflect the ideology of the citizens. It is therefore of great value to the success of a democratic government that as many citizens as possible cast their vote.

PMT can be used to suppress voter turnout (Borgesius et al., 2018; Green & Issenberg, 2016). As seen in the previous chapter, persuasive PMT is used to predict the likelihood of a certain person to vote during elections. If a person is likely to vote for an opposing candidate, targeted messages can be sent to discourage this person from voting. The targeted people may for example see a message about another candidate that reflects negatively on them, causing a loss of motivation to vote for that politician. Furthermore, predictive PMT can be used to target certain groups, leaving other groups of voters without information about certain issues and proposed solutions, which may cause them to have less motivation to cast their vote.

Chapter 3: Conceptual tools

After seeing how PMT can threaten values of liberal democracies, we ask if there is a way to use PMT for social good. We aim to find design perspectives and policy changes for PMT that do not threaten, but protect and promote the values of liberal democracy. In this chapter we describe the conceptual tools that help us to create these recommendations.

To find design requirements we use some of the principles and methods of Value Sensitive Design. Designing value-conscious technology is often done with this design methodology, that provides a principled approach to embedding human values into technology (Friedman et al., 2013). The VSD method originally consists of three parts: the conceptual, empirical and technical investigations. These steps are elaborate, and require an iterative approach. In practice, the methods of VSD are adapted to fit a certain project, and should be viewed more as a guideline than a detailed project plan. For this thesis we focus on a specific part of the VSD methodology: the translation of values into more concrete design requirements. This allows us to put the findings from chapters 1 and 2 to use, and requires a theoretical reflection based on philosophical and political theory. Some of the provided design recommendations are meant to be used for PMT methods deployed at this moment. They are practical, and more likely to be picked up by current creators of PMT. Others are more idealistic in nature, and show what PMT could look like in the future, as an instrument to aid democratic processes. They may not necessarily benefit the creators of the technology, such as the individual political parties. Rather, they show how the techniques that are currently used for personal gain can be used to benefit the people.

We can further mitigate the risk of PMT by creating sound policies. The goal for these policies is to provide protection from malicious use of PMT, and complement the design recommendations. This is a difficult task, since there is still a lot we do not know about the practice and effects of PMT. Definitive policy recommendations can therefore not be given, but we can start indicating the direction that policies may take in the future, given the risks we are aware of now. The most important point of action at this time however, is to do more research on PMT. We outline some policies that already exist, and argue why they fail to protect the values of liberal democracies. After this, we know where to add additional policies, or which policies need to be amended.

Translating Values to Design Requirements

The previous chapter resulted in a list of values: liberty, equality, data security, privacy, development of character, deliberation, transparency and political participation. To turn these values into design requirements, we create a value hierarchy for each value, as depicted in Figure 1 (van de Poel, 2013).

A value hierarchy shows how the concepts of the abstract level, the values, relate to more specific concepts: norms. These norms are prescriptions for, and restrictions on actions, and are a specification of a value. This specification involves a value judgement because a transition is made from the evaluative to the descriptive domain, and can often be done in multiple ways. Therefore, van de Poel (2013) describes two criteria to assess the adequacy or tenability of a specification. The first is that a norm should be an appropriate response to a value, meaning that the norm should do the value justice. To this end, we can use the findings from chapter 2, as they provide an argument for some of the chosen norms. Second, the set of norms should be sufficient to properly respond or engage with the value. The resulting norms and design requirements are meant to be context-

specific, meaning that they do not need to solve larger democratic problems by themselves, but should be regarded only in the context of designing PMT-technologies.

These norms are then further specified in the most concrete layer of the hierarchy: the design requirements. A design requirement describes how the technology needs to be designed to meet the norms. These requirements also need critical reflection, because they can often be given in multiple ways. Part of this reflection is to assess the ‘for the sake of’ relation they have to the norms. The norms give the reason and justification for the design requirements, which needs to be made transparent and debatable.

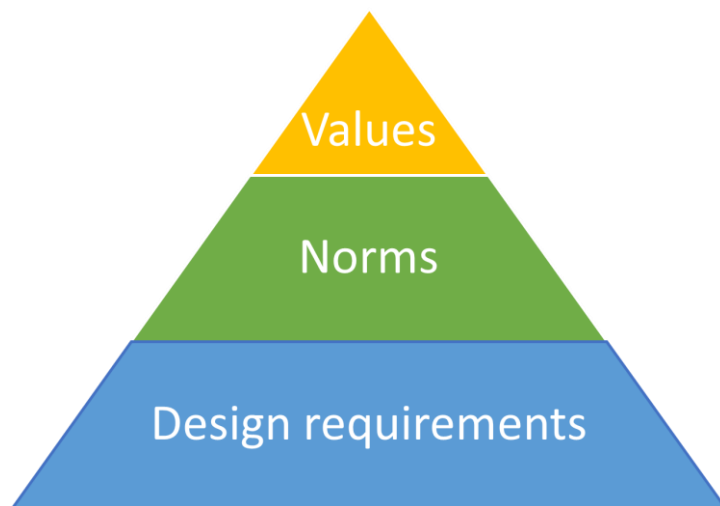


Figure 1: Value Hierarchy

Protecting values with policies

Current policies

The theory of liberal democracies used in this thesis is not a definitive set of qualifications, but rather an ideal that applies to some real states more than others. It is therefore not possible to make a proper distinction between countries that are, or are not, liberal democracies. For the purpose of this thesis, given that we wish to explore real policies of real states, we will focus on policies in Europe and North America. The ‘western democracies’ on these continents are considered ‘free democracies’ by the Centre of Systemic Peace (Marshall & Elzinga-Marshall, 2017). Although they list several other countries such as Mongolia and Chile as free democracies, we will leave these out of consideration for simplicity.

Europe

In the EU, many of the threats listed in the previous chapters, such as manipulation and privacy breaches, are supposedly tackled by Data protection laws, such as the GDPR. PMT makes use of personal data, and the purpose of the GDPR is to ensure that personal data is used fairly and transparently. Compared to the data protection policies of the United States for example, the GDPR is much stricter. Since personal data, and the freedom to use it for PMT, is more strictly protected than in the US, we could argue that countries that enforce the GDPR mitigate the risks of microtargeting (Borgesius et al., 2018). However, this does not mean that they are sufficient measures to protect citizens against the threats of PMT. The interpretation and enforcement of the GDPR varies per state, which means that the efficacy of the regulations can be questionable. In

addition to this, we argue that the GDPR leaves a policy gap for political microtargeting that needs to be addressed.

First, the GDPR is only a measure to protect personal data, not a measure against malicious use of PMT. Although these policies may indirectly help to protect liberal democratic values, they do not specifically protect against, for example, manipulation. This means that the GDPR alone is not a sufficient measure against these threats. There are several countries that provided additional policies concerning the use of personal data for political purposes. For example, the Italian Data Protection Authority created policies for the processing of personal data by political parties. It prohibits the use of personal data for the purposes of political communication, if this data was collected for other purposes (*Provvedimento in Materia Di Trattamento Di Dati Presso i Partiti Politici e Di Esonero Dall'informativa per Fini Di Propaganda Elettorale*, 2014). However, these additional regulations are only used nationwide, and aim to further protect personal data, rather than the wider range of problems caused by PMT.

Second, the GDPR provides transparency measures, which can aid in exposing the source of information, and in turn raising awareness to the citizens whose data is used. However, this neglects the accountability of the other stakeholders involved. There is a multiplicity of actors involved, among which the political party, the creator of the algorithm, and the providers of the voter data, which makes it difficult to allocate appropriate responsibility. It is often hard to tell who is in control of the personal data when a political party has outsourced their data analytics to an independent company (*EDPS Opinion on Online Manipulation and Personal Data*, 2018). Currently, the European Data Protection Board has published guidelines for the allocation of a Controller and Processor in these situations, which are crudely speaking the deciding and the executing party respectively (*Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*, 2020). In many cases however, we can argue that both parties are in control, especially when the independent company is free to decide how to collect and process the voter data.¹ This means that it is often unclear which party can be held accountable.

Lastly, the GDPR relies heavily on the concept of consent, which must be provided by the data subject before their data can be collected and used. It specifies that consent must be freely given, specific, informed and unambiguous (Council of the European Union, 2016b). It is however debatable whether the current specifications to ensure consent is given are sufficient. Especially the criterion that consent must be 'informed' is difficult to satisfy. It is after all in the PMT-user's best interest to acquire consent, so designing consent forms that provoke an undeliberated reaction of consent, rather than an informed one, seems to be the norm (Waldman et al., 2020). These nudges in consent forms, known as 'Dark Patterns', can prevent persons from giving meaningful consent by overstepping the deliberative process that is needed.

North America

While the GDPR provides some protection for countries in the European Union and the United Kingdom, the situation in the United States and Canada is much more dire. Even though the political environment of the United States, the two-party system, is an excellent breeding ground for malicious PMT, the regulations are less strict than in Europe. At the moment, there is no principle law for data protection in Canada or the US. There are several laws enforced by different levels of

¹ Similar arguments have been made on the topic of Health Information (Mobile Health: Reconciling Technological Innovation with Data Protection, 2015).

governance, none of which seem to provide sufficient protection against PMT (C. J. Bennett, 2016). New Data protection laws have been proposed in both countries, but since these are considered to be less strict than the GDPR, we may assume they do not provide the protection that is needed (Hartzog & Richards, 2020). To create new policies, we will therefore use the stricter European policies as a baseline, and explore which policies can and need to be added to these.

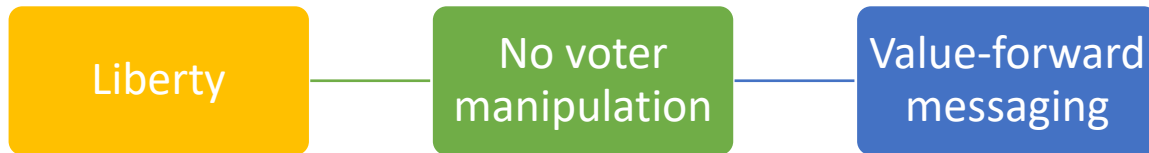
Creating policies

Additional policies are needed to protect liberal democratic values. The difficulty in creating policies lies in finding a compromise between different values, for example between privacy and safety. In this case, the value of freedom of expression is conflicting with the values we wish to protect. The right to freedom of expression protects the right to political advertising, including the use of microtargeting techniques. It is however not uncommon for countries to limit these rights in special circumstances, such as during political campaign times. This means that it is possible to create new policies for PMT, although the options are limited (Dobber et al., 2019).

Chapter 4: Recommendations

In this chapter we show a value hierarchy for each threatened value described in chapter 2. The values are represented in yellow boxes, followed by the corresponding norms in green. The blue boxes show the design requirements and policy recommendations that follow from the norms.

Liberty



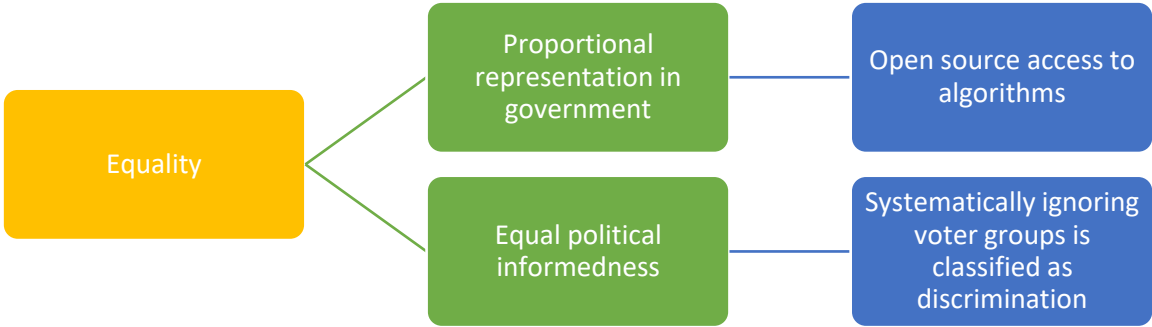
We argued before that the value of liberty is threatened by the use of PMT because in certain cases it leads to voter manipulation. To protect the value of liberty voters must therefore not be manipulated.

Finding design requirements for PMT's that guarantee that voters cannot be manipulated is a complex task. The reason for this is that there have not been many empirical studies that show how to design technology in such a way, nor on how to measure manipulation. Some empirical work has been done in the field of interaction design patterns, mainly applied to cookie consent statements (Graßl et al., 2021; van Elteren, 2020). These studies show the manipulative effects of different interaction designs, and promising effects of virtuous design patterns that help users to be more deliberative in their interactions with technology. It is however debatable to what extent these findings tell us something about the design of PMT, since there is no interaction on the side of the voter with the technology itself. We will therefore argue from a more theoretical perspective.

Design requirement

Persuasive PMT's are used to nudge voters into making a certain decision. Problems only arise when nudging turns into manipulation. Defining the difference between these concepts is however a difficult task, as there is no consensus among political theorists on the definition of manipulation (Wilkinson, 2013). Most definitions however share the common belief that manipulation is an infringement on autonomy which causes people to make a choice that is not in line with their own values and interests. In order to prevent manipulation, voters need to be aware of the values a particular political decision promotes. Therefore, we propose the design requirement of value-forward messaging: when advertising a political message, the underlying values that support that message must be made explicit. Theories of moral psychology such as by Haidt and Lakoff suggest that moral domains inform political decision making (Haidt, 2012; Lakoff, 1996). This is supported by empirical studies on moral language in political campaigns. Specifically, increasing the use of explicitly mentioned values such as fairness, loyalty or authority increases support for a political standpoint. Moreover, voters respond more positively to a message that contains words closely related to the values they hold themselves. For example: a voter that values authority will respond more positively to a message using words such as 'law', 'respect', and 'obey'. This could make them more likely to vote for a party that has values in line with their own (Hanel, 2017).

Equality



We argued before that PMT threatens the value of equality in two ways: it can cause an unproportionate representation in the elected government, and unequal political informedness among voters. Therefore, in order to protect the value of equality, we turn these threats into the norms of our value hierarchy.

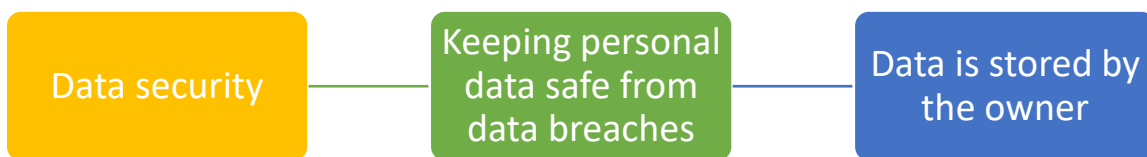
Policy recommendations

In order to achieve proportional representation in governments, all representatives need equal access to the floor, and equal power to influence voters (Huddy et al., 2013). If some politicians routinely speak more than others, participation is not equal (Sanders, 1997). An inequality in resources such as PMT technologies mean that some speakers will be more effective than others, which is a particular concern for socially disadvantaged groups (Mansbridge, 1983). Therefore, all political representatives should have equal access to PMT techniques. This means that the algorithms created and used to this end should have an open-source software license. This software license allows anyone to access and use the code, and even edit or improve it, as long as the new version remains open sourced (Perens, 1999). Not only will this provide some transparency on the mechanisms used, it will also ensure that anyone can access the technology without additional means. One could argue that access to source code is not enough, but that an equality in expertise is required to use the code correctly. We argue however that this is not a design requirement for the technology itself, but rather a consideration for the policies for its use. Furthermore, one could argue that this requirement is not sufficient to achieve proportional representation. There may be other reasons why people cast a vote that is not in line with their own beliefs and values, like strategic voting or misinformation (Myatt, 2007). Moreover, some people have reason not to vote at all, which causes their governmental underrepresentation. These problems however, result from deeper, more complex issues in democratic states, and do not stem directly from the use of PMT. It is important to note however, that although open-source software licensing is in theory a way to make software more accessible, in practice it is currently rather exclusive. This has mainly to do with the community surrounding its use, which is notoriously hostile to women (Nafus, 2011). This issue needs to be addressed first, in order for this to be a viable solution.

Achieving equal political informedness is a difficult task, and certainly not one that can be accomplished with PMT alone. Moreover, lack of access to information is not the only reason for inequality. For example, some people have more time to invest in gathering information than others. At the very least however, we argue that deliberately ignoring groups of voters as an integral part of a campaign strategy further promotes this inequality. Using predictive PMT to find out which groups of people are more susceptible to a message than others is not problematic in itself. However, it can become problematic if this results in certain groups of voters being systematically excluded from receiving critical information. This exclusion harmful, especially for those individuals that these algorithms are biased against. The consequences for individuals that suffer from the effects of

algorithmic bias can be tremendous. If voter turnout plummets for certain groups of people as a result of this algorithmic bias, their wants and needs will be underrepresented in the elected government. Especially in the case of PMT, where bias can have a direct effect on democratic decision making, policies that promote inclusivity, and prevent bias and unfair treatment are needed. As a starting point for the creation of these policies, we need to reason from the margins: find out which individuals are most likely suffer from biases, and create policies that are rigorous enough to prevent harmful consequences for these people (Crenshaw, 2013). We argue that systematically excluding groups of people, whether intentional or through algorithmic bias, is a form of discrimination. Most liberal democracies have a constitutional law against discrimination, such as the Dutch Artikel 1 (Algemene Wet Gelijke Behandeling, 2020). These laws specify that persons have the right to be treated equally, regardless of a number of characteristics such as ethnicity, sexuality or gender. The Dutch law even further specifies particular terrains in which discrimination is punishable, like access to collective resources, commercial services, education and political opinion. In the case of the systematic exclusion of certain voter groups, persons are being discriminated on the basis of personal characteristics. These characteristics are even made explicit, because they are represented in voter models. It is therefore fitting that being excluded by political microtargeting should be classified and treated as a form of discrimination.

Data security



In chapter 2 we discussed that the databases used to store voter data are often the target of data breaches. This brings us the norm that personal data must be kept safe from data breaches, and the design requirement that adequate security must be provided. It is hard to specify what adequate security measures are, because this is dependent on the type of storage that is used. Data breaches happen in different ways, including hacking or technical errors. However, in many instances, a human is responsible, for example by abuse of network privileges, or loss or theft of storage devices (Ayyagari, 2014). Adequate security must be provided in context of the type of storage, and for all possibilities of data breaches.

Design requirement

The fundamental problem with databases is that they act as a locker. A select group of people has a key, and the security of all information is dependent on them. This means that the data is safe, until one of the key holders loses their key, whether intentional or not. To provide more security one can add extra locks, but the problem remains: keys can be bought or lost. An alternative is to stay away from databases, and leave personal information to be stored by its owner. This approach requires a radical change in the way we process data at the moment, but has multiple advantages. The first of which is that data breaches can only reach one person at a time. Second, each person holds the key to their own information, and can decide for themselves where, when and to whom the data is shared. This method has been used in IRMA: an application that functions as a digital passport (Privacy by Design Foundation, 2022). Users can share personal information for verification by only sharing what is relevant in that particular case. For example: when buying alcohol in the

supermarket, it is only relevant to share that you are of legal drinking age. Date of birth, and much less an ID-card with even more information, are not needed, but often still requested by supermarkets. The IRMA app can be used in this case to verify the needed information (see Figure 2). Personal information is stored on personal devices, and sharing is done by the users themselves.

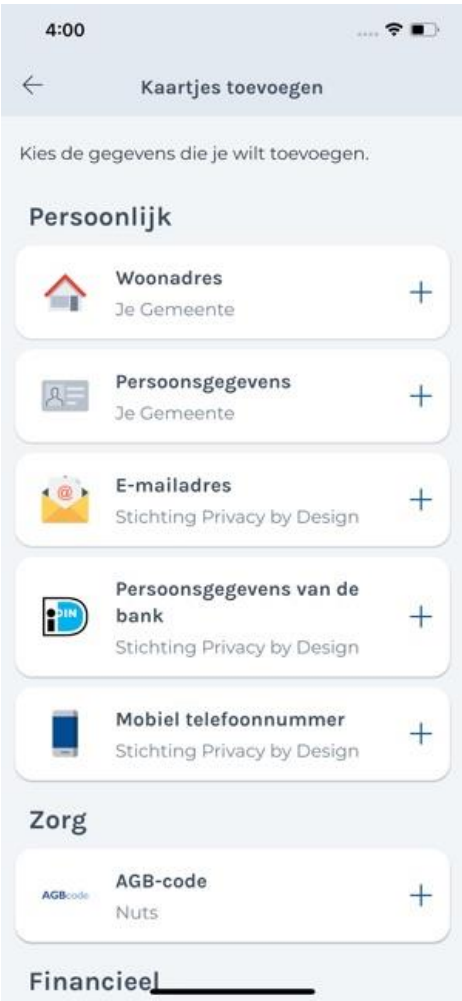
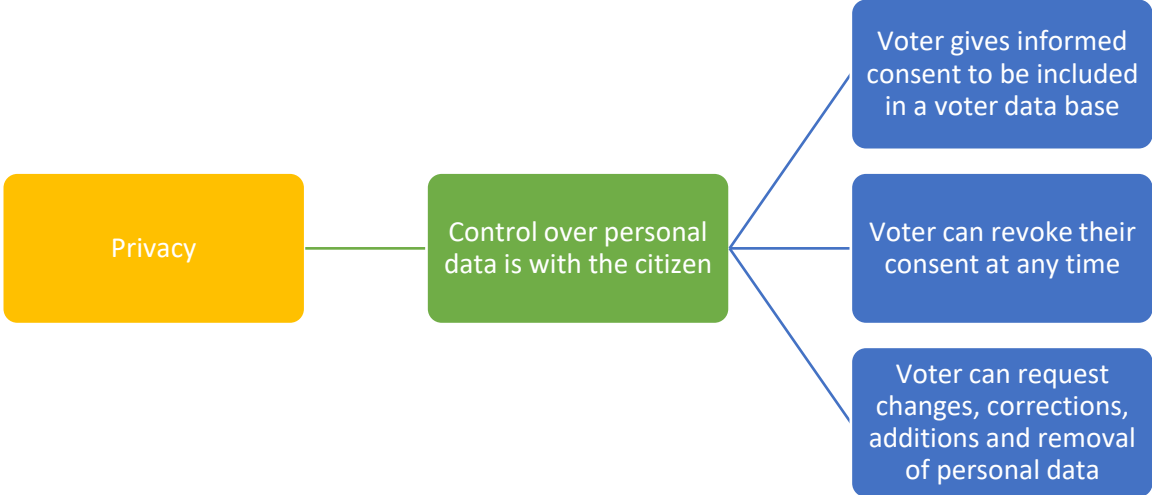


Figure 2: IRMA app (IRMA Authenticatie in de App Store, 2022)

Privacy

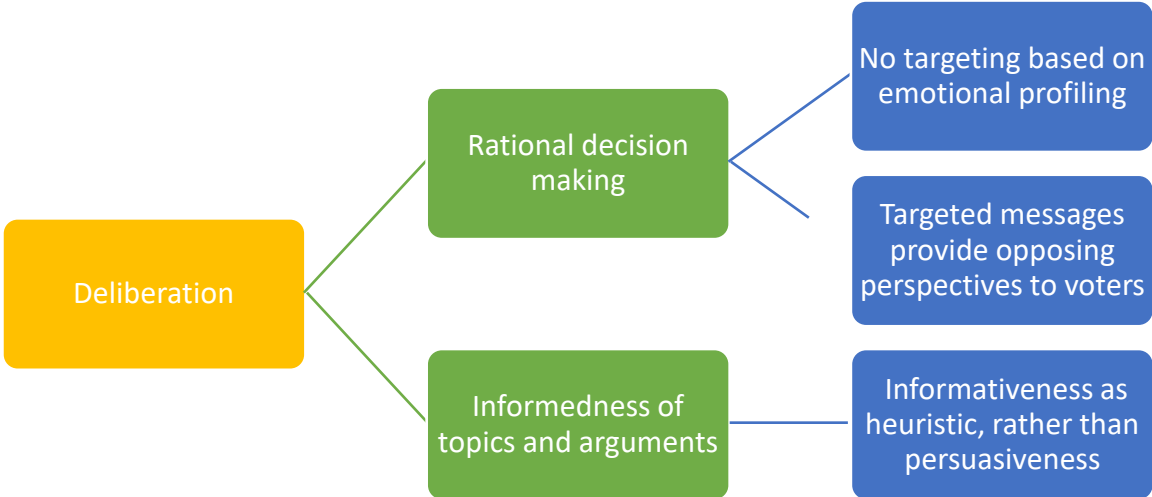


In chapter 2 we defined ‘privacy’ as having control over information about oneself. In the context of PMT, this gives us the norm: control over personal data is with the citizen. This leaves us to argue how much control over this data is needed to assure that the control is meaningful.

Policy recommendation

The self-management of privacy starts with consent (Solove, 2012). Privacy policies such as the European GDPR lean heavily on this principle (Utz et al., 2019). Consent can only be given by someone if they are fully aware of what they are consenting to. The GDPR states that consent must be “freely given, specific, informed and unambiguous” (Council of the European Union, 2016b). In the context of PMT’s, this means that for a voter’s data to be included to a data base, the voter needs to be thoroughly informed about the consequences of their consent. Furthermore, they need to be aware of, and able to revoke their consent at any time. We can promote control even further by adding requirements to allow voters to access, change, and remove their personal data if they wish (Lazaro & Métyayer, 2015). The downside of this is that, even when people have the option to make these changes, many people rarely make use of it. Regulations like this may therefore not be very effective. Design solutions, such as proposed in the previous section, may be more effective in promoting privacy.

Deliberation



Proper deliberation requires a voter to be informed of the topics to deliberate on, and is valued when it results in a rational decision. Information alone, however, is not sufficient, because a voter needs enough time and resources to spend on this deliberation. This factor is dependent on the personal situation of the voter, and cannot be solely provided by a PMT algorithm. The two norms that we consider in this analysis are therefore ‘rational decision making’ and ‘informedness of topics and arguments’.

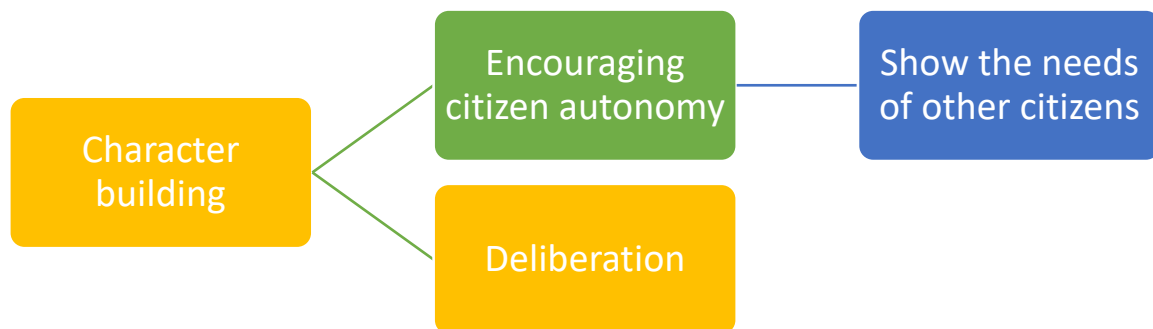
Policy recommendations

In chapter 2 we argue that the rationality of a decision is threatened when PMT’s use emotional profiling to support a particular political view. These tailored messages do not persuade a voter based on rational arguments or facts, but are made to incite an emotional reaction. To protect rationality, this method should not be used. Policies are needed to specify the types of information that can and cannot be used for political microtargeting. At the moment, no such specifications are made.

Design requirements

Currently deployed PMT algorithms are designed to find the message that is most likely to persuade a voter. This means that a message is not judged on how well it informs a voter on a particular view, but rather on its persuasive power. We can however use the techniques of PMT to tailor a political advertisement to be as informative as possible to a particular voter. For example, if we know a voter values action against climate change, a message focusing on persuasiveness could show a picture of a new gas-free neighborhood. The targeted voter will likely be aware of the consequences of using fossil fuels, and may be persuaded because they believe gas-free neighborhoods are an effective message against climate change. The voter did not learn any new information, and may not even deliberate their choice. A message that uses informativeness as a heuristic, rather than persuasiveness, could inform a voter on other values or measures against climate change that they had likely not considered before. Moreover, the aforementioned picture of a gas-free new neighborhood could be used to inform a voter about other topics they may value, like affordable housing. These messages will broaden the viewpoint of the voter, rather than reaffirm the beliefs they already had. Furthermore, it is helpful to show opposing perspectives (Suiter et al., 2020). This increases empathy for other viewpoints, and increases policy knowledge. As a design perspective, we can implement this by judging a message on how different it is from the current beliefs and interests of a person.

Character building

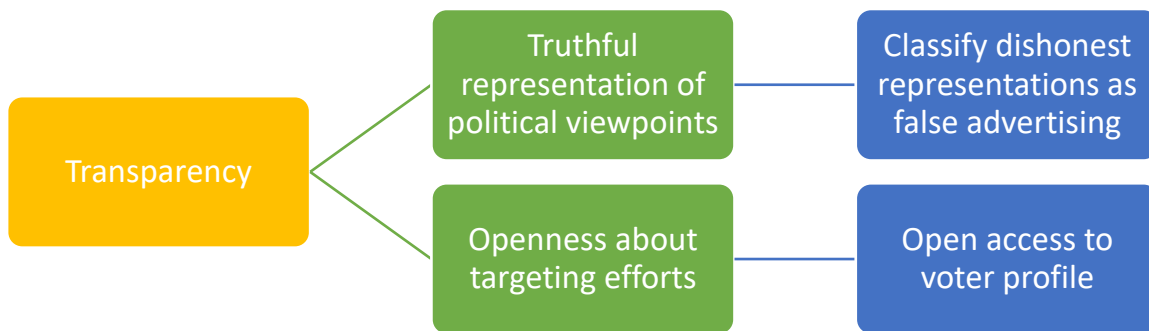


Democracy is endorsed by some political theorists for its beneficial effects on the citizens within democratic states. Since collective decision-making requires their input, democracy makes people behave more autonomously and deliberative (Christiano & Bajaj, 2022). The value of character building can be supported by norms that support, encourage and facilitate these character traits. Deliberation as a value of itself is already discussed in the previous section.

Design requirement

As mentioned in the section on liberty, autonomy is something that should be protected against manipulation. In this instance however, we wish to not only protect autonomy, but also to further promote it. To encourage citizen autonomy, we must first define what autonomy means in the context of character improvements through democratic citizenship. Rousseau, one of the philosophers that created and support this theory, believes autonomy requires listening to other voices and needs (Cohen, 1986). He believes that autonomy can only be achieved when citizens see their democratic status as a social membership, rather than a right to be defended as an individual (Neuhouser, 2011). We can encourage this ideal by using voter profiles to tailor messages to show the needs of other citizens, especially those that the targeted voter is likely not aware of.

Transparency



In chapter 2 we argued that transparency is threatened when tailored messages do not give a truthful representation of political viewpoints. Furthermore, people may not be aware that they are being targeted, and what the consequences of this are for them. These threats are turned into the norms of this value hierarchy.

Policy recommendation

There is very little known about the consequences of receiving targeted political messages. In order to get a clearer picture of these consequences, for example on the psychological effect on targeted individuals or the democratic effects of voter manipulation, more research needs to be done. Without this information, the given consent is not properly informed and can therefore be considered of dubious meaning. One could argue that providing a complete list of consequences is not possible in any case, because some circumstances may be unforeseen. However, the little information we already have is alarming, and gives motivation for a more thorough investigation before possible negative effects become significant. We believe a conservative approach in policy-making is needed, limiting the right to use PMT, until further research is done.

To protect the value of transparency against untruthful representations, we can take inspiration from advertising and marketing laws. Most countries have strict laws to prevent false advertising such as unclear, misleading or incomplete information. We argue that political parties that do not truthfully represent themselves in advertisements are falsely advertising, and should be treated accordingly.

Design requirement

Aside from protecting transparency, we can use PMT to further promote the value of transparency. Political campaigning can be made more transparent by being open about the targeting efforts used to persuade voters. Simply giving voters access to the algorithm behind this process is not enough, as this does not give any context to the decisions that are made. It does not provide them with an intelligible explanation. Furthermore, not all voters are trained in reading code, or have resources to spend on this investigation. A reasonable compromise is to provide them with access to their own voter profile. This voter profile already consists of modelled character traits and interests, and can easily be made explainable to a voter. An example of how this could work is Google's targeted advertising profile. A Google user is able to access the information that Google has collected and inferred, in order to look into the reasoning behind the targeted advertisements they see (see Figure 2). The list is written in natural language, and privacy settings concerning the information in the list are provided on the same page.

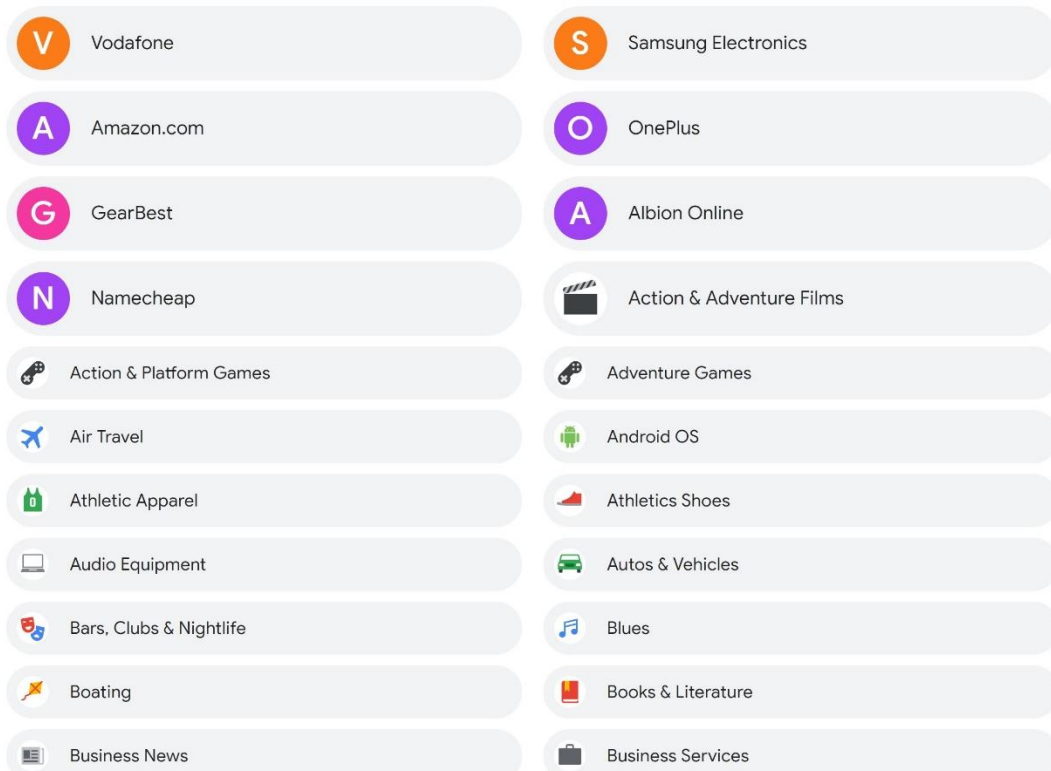
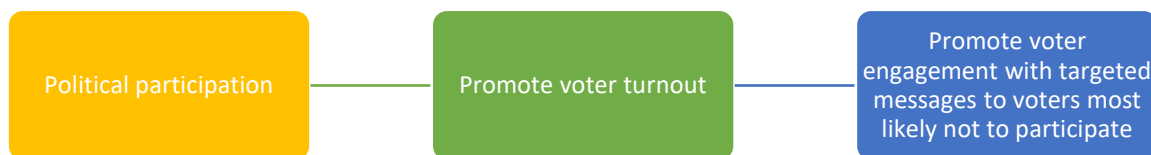


Figure 3: An example of a Google advertising profile (Gordon, 2022)

Political participation



The value of political participation is mainly threatened by PMT because it can be used to suppress voter turnout. Therefore, the norm connected to political participation is to promote voter turnout. The proposed solutions however do not give a complete solution to the problem of political non-participation. The socio-structural characteristics of a person, for example their educational background, income and social position are the most important factors that determine to what extent someone is politically involved (Verba & Nie, 1987). The reasons for political non-participation can roughly be placed in three categories: (i) citizens do not want to participate, (ii) citizens can not participate, and (iii) nobody asked them to participate (Verba et al., 1996). The first and last reason are tackled in the following design solution. The second one however, is part of a broader problem that PMT alone cannot solve. They may for example not be able to vote because of a lack of time, or inaccessibility of polling places.

Design requirement

To further promote voter turnout, voter engagement with politics should be increased. The techniques of PMT can be used for this. Predictive microtargeting can show which people are likely not to engage with political topics, while persuasive microtargeting can uncover the topics that may

interest them. Targeted messages should be send to those likely not to vote, and contain information that may enthuse those persons.

Conclusion

In this thesis we defined Political Microtargeting as the use of data-driven voter research in personalized political campaigning. We then showed that the popularity of using AI has changed the scale and efficacy of it tremendously. This can be seen in the increase of campaign budgets for targeted ads, the increase of political advertising through social media, and the results of studies that prove the effectiveness of targeted ads on changing voter behavior.

These changes gave ground for an assessment of the threats PMT forms for the values of liberal democracies. We argued that the liberal democratic values of liberty, equality, privacy, data security, development of character, deliberation, transparency and political participation are threatened by its use.

We then proposed design solutions to protect these values, by using the method of Value Sensitive Design. This resulted in a list of practical design solutions that can be used in the construction of PMT algorithms. We also recommended a change in policies to support and protect the values that are currently threatened.

Limitations

Although this thesis has provided an overview of threats and solutions, it remains an incomplete project. The main issue, as shown in many parts of the thesis, is that not enough research has been done to provide us with a definite picture. This means that the list of risks and solutions must be updated when more information is available. In the next section we list some of the directions this future research may take.

Though these limitations are empirical, there are also limitations of a theoretical nature. The main concern here is that the solutions are provided to improve democracies from the voter's point of view. PMT's however, are used by political parties, who may not be interested in changing their campaign strategies to benefit the voter. The proposed design solutions may not be in the best interest of the party that makes use of the algorithm, which means that without regulation, they may never be used in practice. They may however be used in a politically neutral tool, created on behalf of the state, to facilitate the spread of political information or boost voter turnout.

Another limitation is found in the policy recommendations. Policy makers are limited by freedom of expression, which is in many states a constitutional right. In many cases, this may mean that proposed policies that are rigid enough to remove a threat may be impossible to install, while compromising policies may not be enough to resolve issues. It is therefore useful to create a reliable measure of manipulation through advertisement. If a practice can be proven to be manipulative, it may be treated as an exclusion to the right of freedom of expression.

This thesis is built around a set of values belonging to liberal democracies. Values however, are not set in stone, and can change over time. In this sense, this thesis is a work of its time, and needs to be revised when values change.

Lastly, the provided solutions neglect to touch on problems caused by deeper, more complex issues in democratic states. Some of the threats of PMT are caused by societal issues such as systemic inequality. Treating them with the solutions provided in this thesis may be impossible when the root of the problem is never addressed. This issue also has a flip-side: though PMT may alleviate some of the issues caused by more complex issues, it must not be seen as a proper solution to them.

Future research

The goal of this thesis is to assess the threats of PMT to liberal democracies, and to provide solutions in the form of policy recommendations and design solutions. Although some of these threats and solutions have been stated in chapters 2 and 4, it is likely that the list is incomplete. This is due to lack of research on the effects of PMT on democracies. Therefore, we will outline some of the directions future research should take, in order to get a more complete picture of the risks of using PMT.

Manipulation

One of the biggest threats we mentioned in this thesis is the risk of voter manipulation. Previous research has suggested that PMT may not leave a targeted voter with the freedom to make their own decision (Zarouali et al., 2020). This research however is exploratory, and is limited in generalizability. It would be interesting to see future research find out how strong the effect of PMT can be: how strong of an ideological change can it cause for targeted voters? Furthermore, can we predict which type of voter is most likely to be persuaded with a targeted add, and why? After this, a risk assessment must be done, in order to decide to what extent the effects of PMT are manipulative.

Misinformation and fake news

In this thesis we explored how targeted advertisements can threaten democracies. These targeted ads however, are presumed to contain truthful information. Political campaigns over the last decade however have shown an alarming trend: fake news (Lazer et al., 2018). The spreading of misinformation is not new, but using it as part of a campaign strategy started during President Trumps 2016 election campaign in the United States, and the UK Brexit referendum (Pennycook & Rand, 2021). Fake news is most commonly spread through social media, which makes it an excellent vehicle to spread targeted messages. Future research should assess the effects and risks of fake news in targeted messages. For example, does it make a message more persuasive? And what effect does the credibility of the message have on the behavior of a voter?

AI for good

In chapter 4 we described design and policy recommendations that mitigate some of the risks of PMT, or even promote values. Perhaps there is a way to use what is known about PMT to the advantage of liberal democratic states. For example, PMT can be used to boost voter turnout, or spread information more effectively. Future research should focus on further possibilities that PMT has to be used as a tool to improve democracies. An application of this knowledge could be a system that is used as a personal democracy teacher: an AI system that personally recommends societal topics and solutions that promote political engagement.

Acknowledgements

I would like to express my deepest appreciation to my supervisor, Giulio Mecacci. Your feedback, support and expertise have inspired me to pursue a career in academia. I am also grateful to Hanna Schraffenberger, for once again putting her time and expertise into my education. I would also like to thank Jorrit, Jochem and Rosa, for their feedback, moral support and friendship.

Bibliography

Algemene wet gelijke behandeling, Pub. L. No. BWBR0006502, Binnenlandse Zaken en Koninkrijksrelaties (2020). <https://wetten.overheid.nl/BWBR0006502/2020-01-01/0/informatie>

- Amnesty International. (2022). *Sleepwet vormt een bedreiging voor de mensenrechten*.
<https://www.amnesty.nl/mensenrechten-in-nederland/veiligheid-en-mensenrechten/sleepwet>
- Amsalem, E., Zoizner, A., Sheaffer, T., Walgrave, S., & Loewen, P. J. (2018). The Effect of Politicians' Personality on Their Media Visibility: <https://doi.org/10.1177/0093650218758084>, 47(7), 1079–1102. <https://doi.org/10.1177/0093650218758084>
- Ayyagari, R. (2014). An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights. <http://dx.doi.org/10.1080/15536548.2012.10845654>, 8(2), 33–56.
<https://doi.org/10.1080/15536548.2012.10845654>
- Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. *International Conference on Information and Knowledge Management, Proceedings*, 31–36. <https://doi.org/10.1145/2389661.2389671>
- Bennett, C. (2014). Voter Surveillance, Micro-Targeting and Democratic Politics: Knowing How People Vote Before They Do. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.2605183>
- Bennett, C. J. (2016). Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law*, 6(4), 261–275. <https://doi.org/10.1093/IDPL/IPW021>
- Billard, T. J. (2016). Fonts of Potential: Areas for Typographic Research in Political Communication. *International Journal of Communication*, 10(0), 23.
<https://ijoc.org/index.php/ijoc/article/view/6019>
- Borgesius, F. J. Z., Möller, J., Kruikemeier, S., 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/METRICS/>
- Bozdag, E., & van den Hoven, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, 17(4), 249–265. <https://doi.org/10.1007/S10676-015-9380-Y/FIGURES/8>
- Brink, D. (2022). Mill's Moral and Political Philosophy. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/entries/mill-moral-political/>
- Büchi, M., Festic, N., & Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda: <https://doi.org/10.1177/20539517211065368>, 9(1).
<https://doi.org/10.1177/20539517211065368>
- Cambridge Analytica. (2016, November 9). *Cambridge Analytica Congratulates President-elect Donald Trump and Vice President-elect Mike Pence*. PR Newswire. <https://www.prnewswire.com/news-releases/cambridge-analytica-congratulates-president-elect-donald-trump-and-vice-president-elect-mike-pence-300359987.html>
- Caprara, G. V., Barbaranelli, C., Consiglio, C., Picconi, L., & Zimbardo, P. G. (2003). Personalities of Politicians and Voters: Unique and Synergistic Relationships. *Journal of Personality and Social Psychology*, 84(4), 849–856. <https://doi.org/10.1037/0022-3514.84.4.849>
- Caprara, G. V., & Zimbardo, P. G. (2004). Personalizing politics: A congruency model of political preference. *American Psychologist*, 59(7), 581–594. <https://doi.org/10.1037/0003-066X.59.7.581>

- Christiano, T. (2022). Algorithms, Manipulation, and Democracy. *Canadian Journal of Philosophy*, 52(1), 109–124. <https://doi.org/10.1017/CAN.2021.29>
- Christiano, T., & Bajaj, S. (2022). Democracy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2022). Metaphysics Research Lab, Stanford University. <https://plato.stanford.edu/archives/spr2022/entries/democracy/>
- Cohen, J. (1986). Reflections on Rousseau: Autonomy and Democracy. *Philosophy & Public Affairs*, 15(3), 275–297. <https://www.jstor.org/stable/pdf/2265213.pdf>
- Constantinou, E. (2022). Messaging the Bases: Tailoring Political Ads to Audiences. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.4002875>
- Cook, T. E., & Gronke, P. (2005). The skeptical American: Revisiting the meanings of trust in government and confidence in institutions. *Journal of Politics*, 67(3), 784–803. <https://doi.org/10.1111/J.1468-2508.2005.00339.X>
- Council of the European Union. (2016a). *General Data Protection Regulation (GDPR) – Official Legal Text*. <https://gdpr-info.eu/>
- Council of the European Union. (2016b, August 30). *Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/art-4-gdpr/>
- Courtland, S. D., Gaus, G., & Schmidtz, D. (2022). Liberalism. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/entries/liberalism/>
- Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, 55(1). <https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>
- Crenshaw, K. W. (2013). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *The Public Nature of Private Violence: Women and the Discovery of Abuse*, 93–118. <https://doi.org/10.2307/1229039>
- DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/archives/spr2018/entries/privacy/>
- Dobber, T., Fathaigh, R., & Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1440>
- Doherty, B. J., & Anderson, M. C. (2004). Message Tailoring in Spanish. In D. A. Schultz (Ed.), *Lights, Camera, Campaign!: Media, Politics, and Political Advertising* (1st ed., Vol. 11, p. 121). Peter Lang.
- Dommett, K. (2019). The Rise of Online Political Advertising: <https://doi.org/10.1177/2041905819891366>, 10(4), 12–15. <https://doi.org/10.1177/2041905819891366>
- EDPS Opinion on online manipulation and personal data*. (2018). https://edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf
- Eric Jardine. (2019). *Beware Fake News*. Centre for International Governance Innovation. <https://www.cigionline.org/articles/beware-fake-news/>

- Friedman, B., Kahn, P. H., & Borning, A. (2002). *Value Sensitive Design: Theory and Methods*.
www.ischool.washington.edu/vsd
- Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 471.
<https://doi.org/10.2307/795891>
- González, R. J. (2017). Hacking the citizenry?: Personality profiling, 'big data' and the election of Donald Trump. *Anthropology Today*, 33(3), 9–12. <https://doi.org/10.1111/1467-8322.12348>
- Gordon, S. A. (2022, May 27). *How to control and limit Google's ad tracking*. Android Authority.
<https://www.androidauthority.com/how-to-limit-ad-targeting-google-876590/>
- Gosepath, S. (2021). Equality. In E. N. Zalta (Ed.), *Stanford Encyclopedia of Philosophy*.
<https://plato.stanford.edu/entries/equality/>
- Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, 3(1), 1–38.
<https://doi.org/10.33621/JDSR.V3I1.54>
- Green, J., & Issenberg, S. (2016, October 27). *Inside the Trump Bunker, With 12 Days to Go*. Bloomberg. <https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go>
- Groen-Reijman, E. (2018). *Deliberative political campaigns : Democracy, autonomy and persuasion*.
Guidelines 07/2020 on the concepts of controller and processor in the GDPR. (2020).
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
- Habermas, J. (1994). Three Normative Models of Democracy. *Constellations*, 1(1), 21–30.
<https://doi.org/10.1111/J.1467-8675.1994.TB00001.X>
- Haidt, Jonathan. (2012). *The righteous mind : why good people are divided by politics and religion*. Knopf Doubleday Publishing Group.
- Hanel, J. A. (2017). Moral Psychology And Political Campaigns [University of Mississippi]. In *Electronic Theses and Dissertations*. <https://egrove.olemiss.edu/etd/781>
- Hannan, J. (2018). Trolling ourselves to death? Social media and post-truth politics.
<https://doi.org/10.1177/0267323118760323>, 33(2), 214–226.
<https://doi.org/10.1177/0267323118760323>
- Hartzog, W., & Richards, N. (2020). Privacy's Constitutional Moment and the Limits of Data Protection. *Boston College Law Review*, 61(5).
<https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3>
- Hirsh, J. B., Kang, S. K., & Bodenhausen, G. v. (2012). Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits. *Psychological Science*, 23(6), 578–581.
<https://doi.org/10.1177/0956797611436349>
- Holt, K., Shehata, A., Strömbäck, J., & Ljungberg, E. (2013). Age and the effects of news media attention and social media use on political interest and participation: Do social media function as leveller?: <http://dx.doi.org/10.1177/0267323112465369>, 28(1), 19–34.
<https://doi.org/10.1177/0267323112465369>

- Hoven, J. van den. (1999). Privacy and the Varieties of Informational Wrongdoing. *Australian Journal of Professional and Applied Ethics*, 1(1), 30–43. <https://philpapers.org/rec/VANPAT-21>
- Huddy, L., Sears, D. O., & Levy, J. S. (2013). *The Oxford Handbook of Political Psychology* (2nd ed.). Oxford Handbooks. <https://global.oup.com/academic/product/the-oxford-handbook-of-political-psychology-9780199760107?cc=nl&lang=en&>
- IRMA authenticatie in de App Store*. (2022). Apple App Store. <https://apps.apple.com/nl/app/irma-authenticatie/id1294092994>
- Joshi, D. K. (2013). The protective and developmental varieties of liberal democracy: a difference in kind or degree? *Democratization*, 20(2), 187–214. <https://doi.org/10.1080/13510347.2011.634581>
- Kosinski, M., Bachrach, Y., Kohli, P., Stillwell, D., & Graepel, T. (2014). Manifestations of user personality in website choice and behaviour on online social networks. *Machine Learning*, 95(3), 357–380. <https://doi.org/10.1007/S10994-013-5415-Y>
- Lakoff, G. (1996). *Moral politics : how liberals and conservatives think*. Chicago press.
- Lazaro, C., & Métayer, D. le. (2015). Control over Personal Data: True Remedy or Fairy Tale? *SCRIPTed*, 12(1), 3–34. <https://doi.org/10.2966/SCRIP.120115.3>
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science (New York, N.Y.)*, 359(6380), 1094–1096. <https://doi.org/10.1126/SCIENCE.AAO2998>
- Macpherson, C. B. (1977). *The Life and Times of Liberal Democracy*. Oxford University Press.
- Mannetti, L., Giacomantonio, M., Tory Higgins, E., Pierro, A., & Kruglanski, A. W. (2010). Tailoring visual images to fit: Value creation in persuasive messages. *European Journal of Social Psychology*, 40(2), 206–215. <https://doi.org/10.1002/EJSP.726>
- Mansbridge, J. J. (1983). *Beyond adversary democracy*. University of Chicago Press. <https://press.uchicago.edu/ucp/books/book/chicago/B/bo3618381.html>
- Marshall, M. G., & Elzinga-Marshall, G. (2017). *Global report 2017: Conflict, governance and state fragility*. <http://www.systemicpeace.org/vlibrary/GlobalReport2017.pdf>
- Meta - Meta Reports Fourth Quarter and Full Year 2021 Results*. (2021). <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>
- Mobile Health: Reconciling technological innovation with data protection*. (2015). https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf
- Moore, A. D. (2003). Privacy: it's Meaning and Value. *American Philosophical Quarterly*, 40(3). <http://about.jstor.org/terms>
- Myatt, D. P. (2007). On the Theory of Strategic Voting . *Review of Economic Studies*, 74(1), 255–281.
- Nafus, D. (2011). 'Patches don't have gender': What is not open in open source software. <Http://Dx.Doi.Org/10.1177/1461444811422887>, 14(4), 669–683. <https://doi.org/10.1177/1461444811422887>

- Neuhouser, F. (2011). Jean-Jacques Rousseau and the Origins of Autonomy. *https://doi.org/10.1080/0020174X.2011.608880*, 54(5), 478–493.
<https://doi.org/10.1080/0020174X.2011.608880>
- Noar, S. M., Benac, C. N., & Harris, M. S. (2007). Does tailoring matter? Meta-analytic review of tailored print health behavior change interventions. *Psychological Bulletin*, 133(4), 673–693.
<https://doi.org/10.1037/0033-2909.133.4.673>
- Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy and Public Affairs*, 12(4), 269–288.
<https://philpapers.org/rec/PARPMA>
- Pennycook, G., & Rand, D. G. (2021). The Psychology of Fake News. *Trends in Cognitive Sciences*, 25(5), 388–402. <https://doi.org/10.1016/J.TICS.2021.02.007>
- Perens, B. (1999). Open Sources: Voices from the Open Source Revolution. 1-56592-582-3, 171–188.
<https://www.oreilly.com/openbook/opensources/book/perens.html>
- Pettit, P. (1997). *Republicanism: A Theory of Freedom and Government*. Oxford University Press.
<https://philpapers.org/rec/PETRAT>
- Privacy by Design Foundation. (2022). IRMA. <https://irma.app/>
- Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale.* (2014, March 6). Official Gazette of the Italian Data Protection Authority . <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267>
- Regan, P. M. (1995). *Legislating privacy : technology, social values, and public policy*. UNC Press.
<https://uncpress.org/book/9780807857496/legislating-privacy/>
- Richards, N. M. (2014). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*.
- Rijksoverheid. (2017). *Waarom is een nieuwe Wet op de inlichtingen- en veiligheidsdiensten nodig?* | *Rijksoverheid.nl*. <https://www.rijksoverheid.nl/onderwerpen/bevoegdheden-inlichtingendiensten-en-veiligheidsdiensten/vraag-en-antwoord/waarom-is-een-nieuwe-wiv-nodig>
- Ryabtsev, K. (2020). Political Micro-Targeting in Europe: A Panacea for the Citizens' Political Misinformation or the New Evil for Voting Rights. *Groningen Journal of International Law*, 8(1), 69–89. <https://doi.org/10.21827/GROJIL.8.1.69-89>
- Sanders, L. M. (1997). Against Deliberation. *Political Theory*, 25(3), 347–376.
<https://doi.org/10.1177/0090591797025003002>
- Scammell, M. (2016). Political Marketing: Lessons for Political Science: *Http://Dx.Doi.Org/10.1111/1467-9248.00228*, 47(4), 718–739. <https://doi.org/10.1111/1467-9248.00228>
- Schultz, D. (2014). Election law and democratic theory. *Election Law and Democratic Theory*, 1–286.
- Schwartz, D., Fischhoff, B., Krishnamurti, T., & Sowell, F. (2013). The Hawthorne effect and energy awareness. *Proceedings of the National Academy of Sciences of the United States of America*, 110(38), 15242–15246.
https://doi.org/10.1073/PNAS.1301687110/SUPPL_FILE/PNAS.201301687SI.PDF

- Scola, N. (2012, January 18). *Doing Digital for Romney: An Interview with Zac Moffatt*. The Atlantic. <https://www.theatlantic.com/politics/archive/2012/01/doing-digital-for-romney-an-interview-with-zac-moffatt/251495/>
- Shearer, E., & Gottfried, J. (2017). *News Use Across Social Media Platforms 2017*. <https://www.pewresearch.org/journalism/2017/09/07/news-use-across-social-media-platforms-2017/>
- Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press. <https://www.hup.harvard.edu/catalog.php?isbn=9780674035072>
- Solove, D. J. (2012). Privacy Self-Management and the Consent Dilemma. *University of Pennsylvania Law Review*, 135(3), 707. <https://doi.org/10.2307/3312079>
- Suiter, J., Muradova, L., Gastil, J., & Farrell, D. M. (2020). Scaling up Deliberation: Testing the Potential of Mini-Publics to Enhance the Deliberative Capacity of Citizens. *Swiss Political Science Review*, 26(3), 253–272. <https://doi.org/10.1111/SPSR.12405>
- Summers, G. (2004). Data and Databases. In H. Koehne (Ed.), *Databases with Access* (4th ed., pp. 4–5). Nelson Australia. <https://catalogue.nla.gov.au/Record/4610312>
- Tom Agan Penn, by A., & Associates White Paper, B. (2007). *Silent Marketing: Micro-targeting*.
- Twitter Statistics and Trends*. (2022, August 15). Kepios Analysis. <https://datareportal.com/essential-twitter-stats>
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field ACM Reference Format. *ACM SIGSAC Conference on Computer and Communications Security*, 973–990. <https://doi.org/10.1145/3319535.3354212>
- van de Poel, I. R. (2013). Translating values into design requirements. In D. P. Michelfelder, N. McCarthy, & D. E. Goldberg (Eds.), *Philosophy and engineering: reflections on practice, principles and process* (pp. 253–266). Springer.
- van Elteren, L. M. (2020). *Boosting with Friction: The Effects of Design Friction on Deliberation in the Context of Privacy Decisions* [Radboud University]. <https://theses-test.ubn.ru.nl/handle/123456789/12735>
- van Wyk, I. W. C. (2005). The political responsibility of the church: On the necessity and boundaries of the theory of the two kingdoms. *HTS Teologiese Studies / Theological Studies*, 61(3). <https://doi.org/10.4102/HTS.V61I3.457>
- Verba, S., Lehman Schlozman, K., & Brady, H. E. (1996). *Voice and Equality: Civic Voluntarism in American Politics*. Harvard University Press. <https://www.hup.harvard.edu/catalog.php?isbn=9780674942936>
- Verba, Sidney., & Nie, N. H. (1987). *Participation in America : political democracy and social equality*. University of Chicago Press. <https://press.uchicago.edu/ucp/books/book/chicago/P/bo3637096.html>
- Waldman, A. E., John, L., Tamir, D., & Slepian, M. (2020). Cognitive Biases, Dark Patterns, and the “Privacy Paradox” Cognitive Biases, Dark Patterns, and the “Privacy Paradox” Cognitive biases, dark patterns, and the “privacy paradox.” *Current Opinion in Psychology*, 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>

- Wilkinson, T. M. (2013). Nudging and Manipulation. *Political Studies*, 61(2), 341–355.
<https://doi.org/10.1111/J.1467-9248.2012.00974.X>
- Zarouali, B., Dobber, T., de Pauw, G., & de Vreese, C. (2020). Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media: <https://doi.org/10.1177/0093650220961965>.
<https://doi.org/10.1177/0093650220961965>
- Zuckert, C. H. (2014). Aristotelian Virtue Ethics and Modern Liberal Democracy. *The Review of Metaphysics*, 68(1), 61–91.
https://www.jstor.org/stable/24636542#metadata_info_tab_contents