



universität
wien

Masterarbeit / Master's Thesis

Titel der Masterarbeit / Title of Master's Thesis:

Trust in Democracy in the Light of Microtargeting

An explorative study on the effects of modern voter-targeting technologies on young adults' trust in democratic processes with a focus on Slovakia's 2020 parliamentary election

Verfasst von / submitted by:

Alexandra Jakubekova, Bakk.phil.

Angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of:

Master of Arts (MA)

Wien, 2020 / Vienna, 2020

Studienkennzahl lt. Studienblatt /
Degree programme code as it appears
on the student record sheet:

UA 066 841

Studienrichtung lt. Studienblatt /
Degree programme as it appears on
the student record sheet:

Masterstudium Publizistik- und Kommunikationswissenschaft

Betreut von / Supervisor:

Univ.-Prof. Dr. Sophie Lecheler

I. Abstract	3
1.1 English	3
1.2 German	4
II. Introduction	6
2.1 How Much is Your Privacy Worth to You?	6
2.2 A Contemporary Take on Privacy	8
III. Theory	12
3.1 Microtargeting, a Multifaceted Dilemma	12
3.2 The Effectiveness of Political Advertising	13
3.3 Microtargeting in Europe	16
3.4 Further Side-effects of Microtargeting	18
3.5 The Privacy Issue	20
3.6 The Consumer Perspective	25
3.7 Young People, Privacy and Democracy	27
3.8 The Specifics of Eastern Europe and Slovakia	28
IV. Research Questions	31
V. Method	32
5.1 Qualitative Approach	32
5.2 Focus Groups	33
5.3 Sampling	34
5.4 Qualitative Content Analysis	34
5.5 Focus Groups Protocol	36
VI. Results	39
6.1 Initial Case Summaries	39
6.2 Main Categories & Subcategories	40
6.3 Inductively Established Categories	41
6.4 MAXQDA Analysis	42
6.5 Analysis	43
VII. Conclusion	67
VIII. Discussion	71
8.1 Limitations	75
8.2 Suggestions for Future Research	77
IX. Bibliography	79
X. Appendix	84

I. Abstract

1.1 English

This master thesis set out to explore the effects that data-based political marketing techniques have on the understanding and interactions with democracy among young people from a specific geopolitical context, Slovakia, in the specific condition of an approaching national election. The thesis established a theoretical framework that suggested that microtargeting, while a controversial strategy, does not have researchers or experts agree on its effects or even on its nature. While political advertising in general often misses the mark of proven effectiveness, microtargeting has gained notoriety as a result of several high-profile news items related to Facebook data leaks and data mining companies being involved in prominent elections emerged. As such, even the widespread use and awareness of it can have detrimental effects on political culture, trust in political candidates and institutions; and further, on the perceived autonomy and privacy of individuals who feel surveyed as a result. Under such conditions, the freedom to make informed decisions can be seen as compromised, which can have detrimental effects on democracy.

To explore the topic, a qualitative method was chosen due to a lack of existing research in the specified geopolitical area. Focus groups and a subsequent qualitative analysis according to Kuckratz (2018), performed with the help of the MAXQDA software, were ran to illuminate the rather novel topic in a specific geopolitical context. Slovakia, as an Eastern European country, experiences a higher mistrust towards liberal democracy and displays a higher degree of dissatisfaction with the current system, which made the research interest all the more relevant.

The results suggest that while from a political point of view, participants do not view microtargeting favorably, they do not seem to feel too uncomfortable about its existence. Factors such as level of informedness, age and area of expertise appear to play a role. Participants were often aware of all the discussed phenomena (both microtargeting- and privacy-related) and their nuances to a detailed degree, even practicing data safety consciously. In terms of implications, they were disturbed at how right-wing, populist political forces can exploit microtargeting. The political bias was evident. They did not believe themselves to be vulnerable to microtargeting techniques. Existing findings about cynicism towards democracy and disillusionment by the political situation were supported.

The limitations of research include not enough focus groups, and possibly a lack of diversity in political opinion; while the suggestions for future research are clear — now more than ever, it is

vital to explore the implications that modern technology and data collection has on our trust towards, and the understanding of, democracy.

1.2 German

Diese Masterarbeit hat sich darangesetzt, zu erforschen, wie sich die Effekte von auf Daten basierten politischen Marketing Technologien auf das Verstehen von, und Interaktionen mit Demokratie unter jungen Erwachsenen in einem spezifischen geopolitischen Kontext (nämlich Slowakei), unter der Bedingung einer bevorstehende Wahl, ausspielen. Als theoretischer Rahmen hat die Arbeit etabliert, dass obgleich Microtargeting eine kontroverse Strategie darstellt, was die Effekte und Natur von Microtargeting betrifft, einen sich Forscher und Experte nicht. Während politisches Marketing generell in seiner Effektivität nicht immer unbestritten ist, ist Microtargeting dadurch berüchtigt geworden, dass es in verschiedenen öffentlichen Kontroversen, die mit Datenlecken und in Wahlen eingemischten Data Mining Firmen, in Verbindung gestellt wurde. Von daher ist offensichtlich geworden, dass auch das bloße Bewusstsein über die verbreitete Einwendung von Microtargeting schädlichen Folgen für das politische Kultur, politische Kandidaten und Institutionen, sowie auf die wahrgenommene Autonomie und Privatheit von Individuen, die sich unter diesen Bedingungen beobachtet fühlen können, haben kann. Unter solchen Bedingungen könnte die Freiheit zur einen informierten Entscheidung als bedroht interpretiert werden, was sich negativ auf Demokratie ausspielen könnte.

Um das Thema zu untersuchen wurde eine qualitative Methode eingesetzt, teilweise wegen einem mangelndem Forschungskorpus in dem geopolitischen Raum. Fokusgruppen und eine folgende qualitative Inhaltsanalyse nach Kuckratz (2018), durchgeführt mit der Hilfe vom MAXQDA Software, wurde ausgeführt um das relativ neue Thema in einem spezifischen geopolitischen Kontext aufzuklären. Slowakei, als ein Osteuropäisches Land, wird mit einem höheren Misstrauen gegen liberaler Demokratie und einem höheren Anteil von Unzufriedenheit mit dem aktuellen politischen System auseinandergesetzt, was die Forschung noch relevanter gemacht hat.

Die Ergebnisse zeigen, dass sich die Teilnehmer aus einem politischen Sicht mit Mikrotargeting nicht bequem fühlen, andererseits stört sie die bloße Existenz von Microtargeting nicht sehr. Faktoren wie Informiertheit, Alter und Studien- und Arbeitsschwerpunkt der Teilnehmer spielten auch eine Rolle. Teilnehmern waren die meisten besprochene Phänomene (was Microtargeting und Privatheit betrifft) und ihre Nuancen bewusst, oft sogar auf einem höheren Niveau, in dem sie Schutzmaßnahmen im Bezug auf ihre Daten aktiv praktiziert haben. Was Implikationen betrifft,

waren die Teilnehmer dadurch beunruhigt, wie rechtsextreme und populistische politische Bewegungen Microtargeting ausnutzen können. Ihre politische Einseitigkeit ist dadurch offensichtlich worden. Selbst haben sie sich nicht als durch Microtargeting gefährdet geschätzt. Die bevorstehende Befunde über Zynismus und Disillusionment im Bezug auf die politische Situation in ihrem Land wurden bestätigt.

Die Limitationen der Forschung sind unter anderen zu wenige Fokusgruppen und möglicherweise auch ein Mangel von politischer Vielfalt. Die Implikationen für weitere Recherche sind klar — jetzt wird es wie nie früher notwendig, die Implikationen von modernen Technologien und Datensammlung auf unseres Vertrauen und Verständnis von Demokratie zu untersuchen.

II. Introduction

2.1 How Much is Your Privacy Worth to You?

A simple question gaining an increasing momentum in the light of the socio-political events of the previous years. In a time when we are increasingly cognisant of the price of using social media; in a time when legal directives like the GDPR attempt to curb the effects of data erosion and data misuse; and in a time of increased political tension over what constitutes freedom of speech and freedom of expression, the question of what one is willing to do or, conversely, *not* do in order to protect their own electronic data and as such also their extended physical integrity, becomes increasingly pressing and relevant. But what is at stake when we speak of our privacy being threatened through the erosion and misuse of our own data? The issue is relatively new and seldom common knowledge; so what implications do the current operations with data have on our everyday lives, on the way we interact with the world around us, and, ultimately, on the way we look at the things that define our world—such as personal freedoms, liberties and democracy itself?

The first time the term ‘microtargeting’ gained a world-wide notoriety, seeping into the everyday lingo, was around the time of the 2016 US presidential election, a time when the information about how this technique was used to campaign a political candidate emerged. But what is microtargeting, precisely? Microtargeting, though not an entirely new phenomenon, is a way of delivering personalized messages due to precise definition and mapping of the potential recipients and delivering them directly to the individual. Whilst in the past, microtargeting worked in more simple ways, such as through delivering messages specific to a ZIP-code (one message per household), and was not always precise; today, it exists as a means to target individuals based on their psycho-geographic segmenting, and is more precise than ever, owing largely to the widespread and quotidian use of social media by billions of people worldwide. The method was popularized in the US where it was used to lobby during electoral campaigns with the help of data mining companies, or companies who otherwise have access to large quantities of user data. (Barbu-Banes, 2013)

The way social media are designed and encouraged to be used incentivizes users to reveal their personality, mannerisms and opinions, which are then collected in the form of data, stored and used repetitively to target content at the users, or to expose them to content they might be interested in. This content will have been personalized and tailored to suit their needs based on the data they themselves provided through their use, based partly on their geographical location and in part on

their personal features, such as age, gender, preferences, habits, friends, etc., to the point where even a specific individual can be targeted if the criteria are set right, under the so-called method of nanotargeting, as defined by Bradshaw and tested via the Facebook Add platform. (Barbu-Banes, 2013) Combine that with cookies collected on the websites one visits while their social media tabs are also open, and a surprisingly accurate picture of what one ticks to and how to push the right buttons to make them tick so, emerged. Thus far, all of what has just been described is legal. Some data-gaining initiatives, however, go further and use concealed means of gathering data, such as personality quizzes and tests that collect user data as well as the information of one's friends, passing these on to third parties who are interested in such data. (Amer & Noujaim, 2019) That is approximately what happened in the 2016 US presidential election as well as the 2016 British referendum, thus triggering the very debate on data, data privacy and the information we, as users, share obliviously. (Torra, 2017)

While it is obvious to see how such access to and use of data benefits marketers (they no longer need to study the market in such detail to collect data; rather, it is collected for them), it is also apparent that the exceptionally precise use of one's personal data and what is in most instances subliminal targeting based on that data might make individuals uncomfortable. After all, when many users signed up to Facebook in the late 2000s or early 2010s, agreeing to the contemporary terms and conditions of use, very few of those users could have predicted the social network becoming any more than a means of sharing personal content and staying in touch with one's families, friends and acquaintances. And yet, the conception of what social media are and do has evolved so much since, that the mindset with which one entered them in 2007 no longer applies by any means. The changes, however, occurred gradually and without much public debate or widespread concern. That is, until the manner of collecting user data and their purpose of use (in other words, the business model of said social media) has become mainstream popular knowledge. It is here that the newly ubiquitous concerns about our data and the related matters of protecting one's private sphere start to emerge. (Amer & Noujaim, 2019)

At this point, however, one also faces a factual dilemma as well as an ethical concern. Whether knowingly or not, users consent to the use of their data by agreeing to terms and conditions repeatedly and on numerous occasions, such as by accepting new versions of applications, which leaves the issue of reading the said terms and conditions irrelevant—one is obliged and expected to do so at least by law. The ethical dilemma, however, is a far graver and pressing one. At what point does microtargeting cease to be a viable marketing tool and begin to infringe on our freedom to make informed decisions, due to the fact that it selectively exposes us to only a particular type of

information or a specific framing of an issue in a circular process defined by our pre-defined data-driven preferences? (Barbu-Banes, 2013) Are we obliged to develop our informedness ourselves by searching for alternative sources of information, thus avoiding the negative effects of the erroneous news-find-me-perception (Zuniga, 2017), and is this even a realistic expectation to lay on the shoulders of people who are oversaturated with information as it is? Furthermore, the question of what products can be marketed to us via microtargeting is also of grave importance. Are consumer goods acceptable, but are political candidates not? And why?

2.2 A Contemporary Take on Privacy

‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’

Art. 12 of the **Universal Declaration of Human Rights**¹,
10 December 1948, UN General Assembly

The right to privacy is one of the most fundamental human rights, while privacy itself is closely related to one’s honor and reputation, as the art. 12 of the Universal Declaration of Human Rights suggests. The yearning to have a private sphere distinct from the public persona is one of the most natural human urges, and the law recognizes and protects this sphere. The only instances at which any intrusion is allowed into one’s privacy within a democratic society, include national security, public security, economic wellbeing of the country, for the prevention of disorder and crime, for the protection of health and morals, or for the protection of freedoms and rights of others. (European Convention on Human Rights, 1995) State members of the Council of Europe are obliged to comply with this clause, while nearly all member states transpose this principle into their own legislations or constitutions. Companies and legal entities are not exempt from the following of such laws and must set their policies in a way that respect the right to privacy of both their their data and the data of their clients. However, privacy breaches still occur, to the extent that the ongoing debate discusses to what extent they should be tolerated—instead of whether they should occur or not. While the body of data collected on known users grows thanks to the ubiquity of the internet, so does the complexity of protective measures against data leaks and data breaches. (Torra, 2017)

The Universal Declaration of Human Rights was drafted and signed in 1948, at a time when the existence of barely any of today’s prevalent technological tools could have been predicted. As such,

¹ (Universal Declaration of Human Rights, 1948)

the understanding of privacy has also changed substantially, and to this day, several interpretations of its meaning exist. Shoeman (1992) suggests that privacy can mean **a)** a claim, entitlement, or right of an individual to determine what information about himself or herself may be communicated to others; **b)** the measure of control an individual has over information about himself, intimacies of personal identity, or who has sensory access to him; **c)** a state or condition of limited access to a person—a person has privacy to the extent that others have limited access to information about him.

All three understandings are put to question in instances of dubious operations concerning private data that microtargeting might lead to—and especially the interpretation **c)**. The limited access to one's data is compromised inasmuch as we are not aware what data ends up where, and for what purposes it is used.

Another scholar (Benn, 1971) explains the relation between privacy and autonomy — when one knows that they are being watched, their autonomy to act as they please is directly compromised. One acts differently when knowing they are being observed and when certain that they are not. The collection of data, as well as the record of online activities, are nearly omnipresent, and while this knowledge has not been mainstream for years, it is so now, making the sensation of being watched and analyzed an ever-present one. If one adheres to the definition of privacy proposed by Benn (1971), one could argue that through the internet, social media and collection of data, our privacy is being intruded constantly, and are fundamental rights are thus not being respected in their essence. As such, the internet, social media, and data collection are incompatible with this understanding of privacy.

The modern era has given rise to new privacy concepts and phenomena that make meditations about whether privacy as we used to define it still exists more than legitimate—whether on a legal, ethical or philosophical level. Previously, the right to privacy used to mostly protect the integrity of our domestic lives, and us from being documented (i.e. photographed or recorded) in public without our consent. (Torra, 2017) But with the rise of the internet, the borders and divisions of the public and private have shifted enormously. A vast portion of the data we willingly or unwillingly share about ourselves might originate in our domestic lives and private homes, while no external force extracts these—we put them out ourselves. There are legal directives, such as the GDPR (General Data Protection Regulation) in Europe, which attempt to address privacy concerns in a contemporarily appropriate matter. Under the aforementioned directive, one has the following rights: **a)** right to rectification, **b)** right to erasure (or 'to be forgotten'), **c)** right to restriction of processing, **d)** notification obligation regarding rectification or erasure of personal data or restriction of processing,

e) right to data portability. (*General Data Protection Regulation*, 2018) The popular opinions on GDPR are multifold, but the fact of the matter is that only a few events have allowed data protection to momentarily become such a popular subject of public debate as they did during the period leading up to the directive taking effect.

The emergence of new privacy-related concepts further shapes our understanding of what privacy means in the age of the internet. Some especially relevant concepts include data traceability or the possibility to identify a person based on cluster data. Both should. Concern any internet user who might not wish to be associated with the internet use that they seemingly performed ‘in private’. What internet users and legal regulations of data privacy should strive for is data anonymity and unlinkability. Anonymity means that a subject (person) is not identifiable within a set of subjects (people)—such as within a cluster of data that characterize the preferences of a particular psycho-geographical subset. (Torra, 2017) As mentioned previously, however, targeting techniques like nanotargeting do allow this, if targeted very specifically, for which, however, there is seldom enough reason or resources. (Barbu-Banes, 2013) Unlinkability describes a state at which several IOI (items of interest) about a target (person) cannot be traced to one another within a system, which could make the identification of an individual easier. Unlinkability implies anonymity, but anonymity can exist where unlinkability does not. (Torra, 2017) The selling of data to third parties without sufficient anonymization compromises both anonymity and unlinkability, and together with it, also the user’s experience or privacy. Within the Cambridge Analytica affair, both anonymity and unlinkability were compromised when Facebook provided the company with unauthorized access to PII (personally identifiable information) on 87 million of its users. (Isaak & Hanna, 2018)

When the debate on data security (brought to public attention by the Senate hearings of Facebook founder and CEO Mark Zuckerberg) was taking place throughout the world, many were prompted to think for the first time about the price they pay for the use of social media, which previously only existed for supposed leisure. (Alter, 2020) As Zuckerberg sat before the Senate, questioned about Facebook’s involvement in the suspected selling of data on American users to Russian subjects aiming to influence the 2016 US presidential elections, a seemingly ignorant question landed on the table from by Senator Orrin Hatch: ‘How do you sustain a business model in which users don’t pay for your service?’ The seemingly baffled Zuckerberg replied: ‘Senator, we run ads.’ (Alter, 2020) Many viewers saw this moment as representative of the disconnect that exists between the older and younger generation when it comes to modern technology and contemporary means of communication. But perhaps the remark was not quite as ignorant as it was revelatory of the character in which a company that does not ask for any monetary compensation for its use, manages

to build a multi-billion fortune and a monopoly in the world of social media, bringing the famous saying to mind—*if you're not paying, you're the product*. As such, Mark Zuckerberg was forced to admit in front of a nation-wide (and world-wide) audience that Facebook's business model relies on the selling of data, under perfected precision formed by the use of user data, triggering the subsequent discussions (both mediated and private) on what implications this has for our lives. (Alter, 2020)

Coincidentally, it was also the trigger that, combined with the 2020 parliamentary election in Slovakia looming above on the horizon, triggered my interest in the topic in the first place.

What does the awareness of being watched—whether by actual human eyes or by an automated program that sorts through heaps of information based on a pre-defined algorithm—and of potentially being influenced in areas as highly sensitive as our democratic self-determination do to us? Especially to young people like me, who have grown up on social media and have never had the luxury of an older adult warning us to be careful, lest we end up targeted in ways we would not wish to be? Does the potential of meddling with sacrosanct democratic processes, such as national elections, shift the way we look at elections and democracy? If so, how? If not, why not?

These are the questions that have conceived the topic for this master thesis, and ones this master thesis will attempt to explore in depth.

III. Theory

3.1 Microtargeting, a Multifaceted Dilemma

While the discussion about whether microtargeting is ethical, safe and compatible with our understanding of democracy usually steals the limelight, far less attention is being paid to the normative heart of the matter—the effectiveness of microtargeting. There should be no doubt about the fact that social media has a huge mobilizing potential. Pivotal political moments have been triggered and sustained by the prolific exploitation of social media, such as the so-called Arab Spring that twitter helped spread and keep alive (Alhindi, Talha & Sulong, 2012), or the 2018 Slovak anti-government that followed the murder of a journalist, organized spontaneously via Facebook events. (Matuščáková, 2018) Social media can inspire its users to broaden their political knowledge, to discuss politics with their friend and families, to inspire political events, and even to vote. (Borgesius et al., 2019) Whether or not the same effects can be achieved with intentional and directed political messages spread through the social media channel is uncertain—at least according to academic research.

Voter mobilization typically happens in two steps. First, a campaign identifies the targets most suitable for mobilization efforts (voter targeting). This is generally based on two factors—the likelihood of support and the likelihood of turnout. Second, the campaign comes up with persuasive measures and tactics that might motivate this particular portion of the population to come out and vote, in order to make sure that the campaign's mobilization is effective. Based on how likely a potential voter is to support and to turn out, they are then targeted with various messages. (Rusch et al., 2013) This method could be referred to as positive persuasion, i.e. trying to motivate a voter to vote for someone. But it is not the sole type of pervasive political communication. There are also campaigns that aim to de-mobilize a voter, or to dissuade them from voting for an opponent, or from voting at all, assuming that they are unlikely to support the desired candidate. This can be referred to as negative persuasion—persuading a voter to *not* vote for someone. (Isaak & Hanna, 2018) There is also a third special category: the undecided voters, the so-called swing states, those who regularly switch between parties and thus carry no firm allegiances, or the protest voters. These do not typically respond to classical political messaging, but can be of immense value if properly targeted. They can decide the fate of elections, tip the scales of political power, and are increasingly becoming the mobilization target of fringe and anti-establishment political movements and figures. (Barocas, 2012) But in order to predict any of these behaviors, a campaign needs rich voter data and

data models that authentically foresee results; a type of proxy model of target variables that can resemble the outcomes to a highly genuine degree. These proxies can either be previous election data or reliable data polls about voting intention. (Rusch et al., 2013)

Alternatively, they can be millions of data points that allow a campaign to target their potential supporters and non-supporters in real time, collected through the omnipresent social media. Facebook, Whatsapp, Twitter and other globally popular social media have become so dramatically popular at collecting and subsequently reselling data because they are people-oriented and because they monopolize our online communication. Nearly everyone uses at least one of these, and so, to do what is par for the course in today's world, one is active on them, or else risks not being able to communicate with their family, friends, acquaintances, or university colleagues as effectively. Using social media platforms becomes convenient. (Klingspor, 2016) And for political marketers, or any marketers at all, this becomes convenient as well.

3.2 The Effectiveness of Political Advertising

When it comes to political advertising in general, Motta & Fowler (2016) demonstrate, while focusing on the US context, that its effects generally tend to be small, short-term, and conditioned by the viewer's unpredictable own characteristics and the context in which they view the ad. According to the same source, there are only two instances in which political advertising seems to take an effect: firstly, when candidates take unpopular positions and invest heavily into identifying persuadable voters, and secondly, when campaigners contact voters long before the election and measure the persuasive effects immediately (but these effects nevertheless decrease overtime and might not reflect the electoral choices of said targets). In a meta-analysis of 40 field experiments and a subsequent nine original experiments, Kalla & Broockman (2018) showed that the effects of campaign contact, persuasive personal contact and advertising on candidate's choices are close to zero. They explained their findings by claiming that most people's political stances are usually made along partisan lines well before an election cycle and campaigns cannot do much to change them. By far, the most enthusiastic conclusion about campaigning states that 'there is evidence in literature that campaigning does indeed have a measurable effect on persuasion or mobilization of the electorate.' (Rusch et al., 2013)

And yet, every election cycle, no matter how big or small, in countries all across the globe, politicians and their campaigns pour thousands, millions, and even billions into their persuasive public self-presentation, and are constantly on the lookout for a novel, accurate (often statistical)

method that could provide them with more encouraging results than oversaturated channels that carry little research-based evidence of effectiveness. (Rusch et al., 2013) The current novel method involves the prolific use of social media for precise targeting of voters based on their characteristics. A political scientist, Colin Bennet, lists four trends justifying such rise of political microtargeting (specific to the USA). They are ‘the move from voter management databases to integrated voter management platforms; the shift from mass-messaging to micro-targeting employing personal data from commercial data brokerage firms; the analysis of social media and the social graph; and the decentralization of data to local campaigns through mobile applications.’ (Borgesius et al., 2019) All suggest a simple fact, specifically, that political advertising is only following a more general trend set by the use of social media, intelligent devices and the collection and subsequent analysis of user data for advertising purposes. Advertisers are able to pick-point their precise target group instead of dispersing their message across a whole communication channel while hoping for the best, and they simultaneously make the target audience ever-approachable.

In spite of the aforementioned established findings on the effectiveness of political marketing, when data mining and political consulting companies like Cambridge Analytica and Aggregate IQ appeared to have been involved in microtargeting campaigns during crucial national elections and referendums, providing the data for creating personalized algorithms in a divide-and-conquer strategy, their decisive contribution to the success of the campaigns seemed to be implicit. (Faizullabhoy & Korolova, 2018) On the other hand, if the effectiveness of the said technique was insignificant or negligible, political parties across the ideological spectrums would not be investing millions of euros, dollars and pounds to develop their own voter databases. Indeed, there is some evidence suggesting that the contribution of companies like Cambridge Analytica in political elections has been far from insignificant. Isaak & Hanna (2018) suggest that their use of very specific individualized and high-impact messaging on undecided voters may have tipped the scales of the 2016 US presidential election in several swing states by as little as 100.000 voters, thereby serving at least a useful, if not critical, contribution. The authors nevertheless agree that this might not have been the only reason for the outcome of the election.

There are in fact two arguments to be made on behalf of the effectiveness of microtargeting as opposed to classical advertising. Firstly, it can reach its intended audience precisely because of how firmly based in user data it is, and secondly, it allows campaigners to reach people who might be lost in the noise of classical media, such as TV or radio, or in an offline environment. The fact that this method is relatively cheap (if one is using intermediaries who already have data on their users available, such as Facebook, as opposed to creating their own database, which is not as cheap

(Dobber et al., 2018)) when compared to using classical media is surely also a big motivator, especially for small parties and fringe groups. (Borgesius et al., 2019)

Despite the encouraging this must provide to marketers and campaign managers, when examined in experimental conditions, the meaningful effects of microtargeting that would justify the amount of money invested into it are not firmly established. The contemporary academic consensus on its effects (as well as its ethical nature) are not unified. On the contrary.

Some opinions make the case for its positive effects. For instance, in their research, Bodó et al. (2017) argue that better profiling and better targeting is simply a way to provide social media users with more relevant information, which could potentially be in the users' interest. Borgesius et al. et al. (2019) argue that microtargeting could make the political campaign arena more diversified, broadening the marketplace of political ideas and as well as the knowledge of voters, exposing them to the information that is most relevant to their voting decisions. After all, humans have a limited attention span. This way, the paper reasons, that attention could be put to issues close to a voter's heart. Kreiss (2017) even argues that micro-targeting is a tactic that can strengthen democratic participation, as it is typically used to activate users who already have a known preference for a certain party/candidate. The same paper also goes against the notion that MTC (microtargeting campaigns) manipulate the public and sway it in ways that would have otherwise not been possible, by claiming that MTC only have a short-term effect of activating and mobilizing known supporters to participate in public affairs and politics. Similarly to political advertising in general.

Other studies examine the effectiveness of MCT in more detail, and add even more complexity to the argument, but unfortunately, no resolution. A study by Madsen & Pilditch (2018) suggests that MCT that use the psychological profiles of voters can be more successful at convincing people to vote for a *disliked* candidate than typical advertising is at convincing a person to vote for a liked candidate. (Negative persuasion campaigns.) A negatively attuned MCT can thus garner more potential than a celebratory one. Another US-based online experiment showed that well-targeted messaging can also increase a person's positive feelings towards a candidate, however, it does not significantly affect the likelihood of the person voting for them. (Krotzek, 2019) This is in fact a common problem with testing the effectiveness of voter marketing strategies. While it is relatively easy to measure attitudes post-exposure, it is difficult to predict to what extent these could play a role (or could have played a role, in retrospect) in actual voting behavior. When looking at how behaviorally-targeted advertising affects the implied audience in terms of more than just their attitudes, Summers, Smith & Reczek (2016) found out that it actually works as an implied social

label, which can even lead to some people adjusting their self-perception to fit that label. Whether or not the label holds, and can have any long-term effects on the person, depends on how well this label is connected to a person's prior behavior—in other words, if it is well-targeted based on available data.

3.3 Microtargeting in Europe

Most research on microtargeting reasonably focuses on the USA, where the method first gained notoriety and appears to be used most prolifically at the moment. While the North American countries set the trend on microtargeting, European counterparts were quick to adopt it within their legal means. (Dobber et al., 2018) The European continent has its specifics, however. For one, regulations on data collection are far stricter than in the USA. French and Dutch political campaigns have nevertheless already been known to hire microtargeting campaign strategists and digital strategy firms previously active and successful in the USA, while the method itself is known to have been used in several key elections, such as the 2015 UK general election campaign and the 2016 British EU membership referendum campaign, both of which were triggers for three major British political parties (Tories, Labour and Liberal Democrats) to invest in voter databases. (Borgesius et al., 2019) As the trend slowly establishes itself in the European political climate, the body of academic works examining it thickens.

A Germany-focused experimental study by Papakyriakopoulos et al. (2017) looks at the implications of microtargeting, and as a result, claims that the technique can have the positive effects of breaking through 'bubbles' and 'echo chambers' on social media that users often find themselves in, and to target them with novel information, which nevertheless aligns with their general political attitudes. Especially relevant to this phenomenon, they believe, are the undecided voters—but even these do not seem to be persuadable to vote or think in a manner that opposes their already existing views. As Kalla & Broockman (2018) explain and as is cited above, most people's political stances are usually made along partisan lines (such as Democrat vs. Republican, Tory vs. Labour, SPD vs. CDU), and as such, campaigns cannot do much to change that. The only problematic issue, as Papakyriakopoulos et al. (2017) expresses based on their study, is that some users use social media like Facebook far too little, leaving few information about themselves available, which could lead to inaccurate targeting. As it appears, inaccurate targeting is something that gets the political subject of interest in trouble rather than in a strategically favorable position. A study from 2013 showed that voters rarely preferred targeted messaging to general messaging, and if they were 'mis-targeted', they would 'penalize' the candidate enough to erase any positive effects

of targeting. (Hersh & Schaffner, 2013) This finding suggests that when voters feel negatively about the phenomenon of microtargeting, they may carry this impression over onto the candidate. Hence, although a well-targeted message might be successful, an ambiguous messaging, or worse, mistargeted messaging, might prove risky or even backfire.

In another European study focused on the Netherlands, Dobber et al. (2018) examined the attitudes of Dutch people towards political behavioral targeting (further referred to as PBT). Their findings suggest that PBT might have a chilling effect on voters—when voters feel monitored, they refrain from certain behaviors, such as researching certain controversial topics, are more careful online and self-censor if they know advertisers collect their data. In an extreme case, the experience of losing a sense of privacy, intellectual privacy and autonomy can have a detrimental effect on the exercise of democratic rights—i.e. if a citizen cannot reflect and experiment with different ideas as a result of a perceived loss of privacy, they are less likely to use their democratic rights freely, since this requires a degree of self-constitution, independence and rationality, especially when it comes to efficacious voters, i.e. those who believe themselves to be an active citizen capable of making their own political decisions. Thus, by extension, this phenomenon could contribute to the spiral of silence, a theory developed by Noelle-Neumann (1974), in which one gradually refrains from expressing deviating opinions, instilling an atmosphere that lacks dissent and is perpetuated by self-censorship. Since autonomy is a necessary prerequisite for privacy, it can, by extension, be considered a prerequisite for democracy. This finding is also supported by a legal precedent. In one of its rulings, the German Federal Constitutional Court ruled that ‘if someone is not reasonably certain of how his personal information is used and shared, he can be inhibited in its freedom, to plan and decide in a self-determined way.’ (Klingspor, 2016) Therefore, if one does not know what information is being collected and held on them, their behavior might turn as inconspicuous as they see possible—raising the possibility of infringing fundamental rights related to privacy even without direct awareness of this taking place. (Klingspor, 2016)

In their own study about the demographics that predict attitudes to PBT, Dobber et al. (2018) found out that age is the only significant predictor of attitudes, in that there is a linear relationship between age and privacy concerns, up until the age of 65, when the trend stop and then reverses. The youngest voters are least concerned by PBT. Another finding is that women hold more negative attitudes toward PBT than men, while those with pre-existing knowledge about PBT (33% of participants admitted to having any) have more favorable attitudes about the phenomenon as well. Efficacy and education level have not been established as having any significant effect. Hence, they conclude that privacy concerns are not a matter of a certain portion of society, rather, they are a

widespread phenomenon, although a gap between digital natives and digital immigrants could be observed. The study also confirmed the negative effects a sensed loss of privacy (mediated through PBT) could have on a citizen's deliberative autonomy, suggesting that political parties should amend these consequences by becoming more transparent about their influencing techniques, because the alternative is very disingenuous.

3.4 Further Side-effects of Microtargeting

While microtargeting might not have an established direct effect on the electability of political candidates, it may have an effect on other matters. The previous paragraphs outlined how such an effect could play out on one's feeling of autonomy, but research has identified more. For instance, some academics express concerns about voters being targeted unfairly (i.e. without their awareness) and that this might be seen as manipulation, the consequences of which raise concerns about the self-determination and the public deliberation of citizens in democratic societies. (Borgesius et al., 2019) If they do not base their decisions on accurate information, are they making a free and informed decision?

The general guidelines and legal regulations on advertising demand that advertising be easily recognizable as such, and yet, one of the core attributes of micro-targeting is the users not necessarily being aware of whether or why they are being targeted with specific content and what data was used to determine their suitability for the content—or even that they are being targeted in the first place. (Dobber et al., 2018) This raises the possibility of them erroneously believing that they are being exposed to objective, albeit random, information (Love, 2011), or, in other words, not being aware that they may be one of the few people in the world seeing the content targeted at them. Neither do they receive any warning that the messages they receive and are shown come from political campaigns, instead of news. (Isaak & Hanna, 2018) Such worries were first raised during the 2008 US presidential election cycle (Levy, 2008), since this election is considered to be the first US election to have used voter profiles for precise microtargeting (although it is Donald Trump's 2016 campaign that has received the most negative feedback for it, instead of Barack Obama's). Running up to the 2012 election, the Obama campaign introduced an 'Are You In?' application that provided access to the users' Facebook pages, hobby information, network membership and region of residence. (Laslo, 2011) But even years before that, in 2004, the Former Chief Counselor for Privacy of the Clinton Administration, Peter Swire, warned about the rise of microtargeting, drawing a future in which 'the candidate knows everything about the voter, but the media and the

public know nothing about what the candidate really believes. It is, in effect, a nearly perfect perversion of the political process.’ (Barocas, 2012)

A further concern is the effect microtargeting might have on the political culture. For instance, Barocas (2012) points out that due to how precisely a voter can be targeted, the data-driven approach allows political candidates to avoid a public discussion on divisive or polarizing issues, instead allowing the targeting of such messages directly at people who will be open to hearing about them. While Borgesius et al. (2019) argue about the positive sides of this, the exclusivity of viewed content might lead to an increased news-find-me perception effect (de Zuniga, 2017), in which one, under the erroneous conviction that they can rely on news finding them via social media, ceases to look for them proactively and instead relies on data-based algorithms. Overtime, this passive approach to novel information leads to a lower level of knowledge. A second negative consequence is that while exclusive exposure to relevant issues might help politicians avoid a public controversy, the microtargeting method may also contribute to single-issues politics. In other words, to exploiting a controversial subject that the public might react to well (i.e. abortions, discrimination, wealth distribution), but that seldom encompass the complex reality of everyday governance and politics, instead simplifying politics to a counterproductive degree that favors populism over expert knowledge and contribute to partisanship between political camps. (Borgesius et al., 2019) The prominence of microtargeting also tips the scales of power towards the data-mining companies that run microtargeting—a relatively new player in the political arena with an unprecedented influence. (Borgesius et al., 2019)

Yet another negative consequence of a widespread use of microtargeting might be, ironically, voter disenfranchisement. As candidates appeal to undecided voters, swing states, or those who often switch between parties, the ‘faithful’ voters might feel left out, and avoid their democratic duties altogether. Lastly, a perceived loss of privacy that results from using voter’s data may result in them avoiding voting activities completely. In America, the use of voter registration data (in no way as precise as data mined through virtual use) motivated some voters to not register to vote at all, or to refrain from other political activities. (Barocas, 2012) While voter registration is not an issue for most European countries, the negative attitudes that people hold towards microtargeting according to a survey (Borgesius et al. et al., 2019), which could spill over onto the candidates, as established by Hersh & Schaffner (2013), could well be an issue—especially since micro-targeting campaigns are not only deployed to work towards a political candidate in an election. A study has shown evidence for notoriously discussed Russia-linked malicious advertising that spread fake news and

hoaxes on polarizing topics to vulnerable subpopulations through MCT in order to divide said foreign populations. (Ribeiro et al., 2019)

Table 1 Promises and threats of microtargeting for citizens, parties and public opinion

	Promises	Threats
Citizens	More relevant political advertising Reaching social groups that are difficult to contact	Invading privacy Manipulating voters Excluding voter groups
Political parties	Cheap (some types of microtargeting) Efficient Effective	Expensive (some types of microtargeting) More power for commercial intermediaries
Public opinion	Campaign diversification More knowledge among voters about individually relevant issues	Lack of transparency regarding politicians' priorities Fragmentation of the market place of ideas

Table source: Borgesius et al., 2019

3.5 The Privacy Issue

But what about the method is so novel to justify such concerns? After all, collecting voter data is a technique that outdates modern technology and has only been allowed to become more precise with the evolution of technology. So if not the means in itself, it is perhaps the method in which data are recycled and targeted back at users, that makes many uncomfortable. Or, as Swire is cited by Barocas (2012), the unequal relationship in which one side knows too much (candidate) and the other (voter) too little. In the past, data might have been collected from many miscellaneous sources (i.e. supermarkets, magazine subscriptions, charitable contributions, online book vendors, drug stores, automobile dealerships and issue surveys, to cite a few examples), and the behavior of said subjects could have been predicted to a surprising accuracy, including one of 87% (Murray & Scime, 2010), but it returned to the same people in the form of easily discernible advertisements on TV, radio, newspapers, in the streets or in the mail. Hence, the in-depth insights provided by data mining are likely not the real issue, rather, it is the ambiguity of microtargeted social media content and social media advertising that is so starkly different. It seems the loss of agency, the potential of lacking self-determination and the sensation of being under intense and incessant scrutiny in activities that were first thought to be private, is a recurring pattern.

Some of the first modern interpretations of privacy in democratic societies (coined together by US judges Samuel Warren and Louis Brandeis in the 19th century) defined the term ‘privacy’ as the right to be left alone, usually from an oppressive state power. Later, in the 20th century, when audio

and video recordings became commonplace, the term was refined as the temporary withdrawal of an individual from society by Alan Westin in the 1960s. One of the reasons for this withdrawal was a need for limited and protected communication, while the exercise of personal autonomy also began to gain importance. About a decade later, Irwin Altman developed Westin's thesis to define privacy as a process of controlling access to the self or to a group and negotiating between the benefits of openness and security of privacy. Consumer privacy, perhaps the most timely take on the matter yet, describes a specific subset of privacy that recognizes the unique position of a person with valuable information to offer in exchange for the goods they pay for. It is defined as the consumer's ability to control when, how and to what extent their personal information is to be transmitted to others. (Youn, 2009) However, in the last decades, surveillance technology and documentation methods used for various purposes have made the full implementation of all interpretations rather difficult in practice. (Ward, 2017) We are never truly left alone, never not observed, and, as it turns out, not always able to comprehend the ways in which we are being monitored. Very often, however, this is due to our own actions rather than those of an oppressive authority. So, the definition of privacy needed an upgrade, and perhaps even a division.

Currently, there is not a single established definition of privacy available, but most scholars agree that it is a multidimensional construct, and so are privacy concerns. (Mahmoodi et al., 2018) Some scholars distinguish between several dimensions of privacy. *Informational* privacy means that one's data will not be made public until he/she wishes so. *Decisional* privacy means that one has the right to be protected in their decision-making from unsolicited external influences. And lastly, *local* privacy means being protected from the entrance of an unwanted intruder into our physical private spaces. Only those who fully respect another individual's privacy fully respect them as an autonomous person, one that is capable to make their own decisions, exist independently, and pursue their own version of fulfilment. A private sphere can be intruded in several ways—physically, virtually, directly, indirectly, and so on. One of the indirect type of intrusions is owning secret knowledge about people, since it gives the owner a degree of power over the people in questions. The owner can be a blackmailer, but also an institution—government or otherwise private. (Mahmoodi et al., 2018) And owning secret knowledge about others, as determined by the ruling of the German Constitutional Court cited above, inhibits their freedom, can lead to changes in their free behavior, and, in essence, infringes on central fundamental rights. (Klingspor, 2016)

When Cambridge Analytica collected data on millions of Americans from social media networks such as Facebook, and purchased them from data other brokers (i.e. Acxiom, Nelson), they essentially interrupted the US voting process, having violated the citizens' autonomy and limiting

their abilities to make rational voting decisions on their own, in a sense (Ward, 2017). This argument is made on a philosophical rather than legal basis, but complex societal events are rarely judged solely from a factual legal perspective, and law itself is largely built on philosophical and moral imperatives and fundamentals that hard-fact logic often fails to fully entail—which is why the philosophical perspective should also be considered. Philosophically, the distinction between private and public is necessary for a functional democratic society. An individual needs the private sphere for their self-determination and to be able to take part on democratic processes publicly. This fundamental idea is built on the essentialism of personal autonomy and was coined together in Habermas' Public Sphere Theory, though later challenged by feminist scholars who questioned the duality of private vs. public. But it still remains that media, of any kind, remain crucial not only in maintaining the public sphere (Calhoun, 2011), but can also act to intrude it, as was the case in the Cambridge Analytica scandal.

Specifically, the actions of a company like Cambridge Analytica (subliminal targeting of voters by biased information presented as neutral news) trespassed not only against the decision-making autonomy that serves as a prerequisite to personal liberty and the democratic processes that require this liberty, but they also violate Kant's categorical imperative, which also constitutes our philosophical understanding of democracy. If one is not able to autonomously make their own conclusions about what is ethical and what is not, due to basing their conclusions on biased information presented to them under pre-defined conditions, their autonomy is not being exercised fully. It is from autonomy that one can think rationally, and it is from thinking rationally that positive freedoms emerge. It is not only about being able to do what one wishes to, but also on basing one's decisions on their own reason that allows them to arrive on ethical decisions. (Ward, 2017) If this process is tampered with, such as by an intervention by a company that presented selective information that distort our worldview, not only is our informational privacy compromised, but so is our decisional privacy. (Klingspor, 2016)

The further problem with data collection, of course, is not only its tampering of our autonomy, but also a more practical fact—that they reveal a lot about us, a factor that, as discussed above, can also hinder our autonomy. But from a more privacy-oriented perspective, it also poses a long-term threat to our sense of security. For reasons both strategic and practical, data collected on us is being stored and physically separated from us in centralized facilities that are often abroad, while the insurance of anonymization falls short when evidence emerges time and time again of the real possibility of linking users to their confidential collected user information (Klingspor, 2016), including information as sensitive as sexual orientation, which could be inferred from a person's like history.

(Mahmoodi, 2018) According to an analysis by Isaak & Hanna (2018), in 2013 a group of researchers from Cambridge's Psychometrics Centre found out that Facebook user data can be used to reliably predict an OCEAN psychological profile (openness, conscientiousness, extraversion, agreeableness, neuroticism) by drawing a correlation between personality tests of Facebook users and the data collected on them via their Facebook activity and other online indicators. This suggested that data metrics alone could suffice to predict an accurate personality model and to target people according to it. The company Cambridge Analytica came to the conclusion that they could use this data, together with additional data from other social media platforms, browsers, online purchases, voting results, etc., in order to put together the 5000+ data points they had on more than 230 million Facebook users. Combined with the OCEAN analysis, the company was able to microtarget users with personalized information in the so-called 'project Alamo' used in Donald Trump's 2016 presidential election. (Isaak & Hanna, 2018)

If one expected to be exempt from such tactics by opting out of using social media like Facebook altogether, reality offered little solace. One did not need a Facebook account in order to have their data collected—affiliated websites with a Facebook button all collect user data for the company, including search engine behavior, or one's shopping history. (Isaak & Hanna, 2018) Hence, the question of providing consent to having data collected seems to become increasingly secondary. Whether or not we agree with the cookie policies on sites we visit, we may not realize whom these websites are providing our data to, and under what conditions, or which of the information we have chosen to disclose on the internet is being used to target us. (While the GDPR sets to curb this effect, it is only in force in the EU, and only since 2018.) Out of the plethora of terms of conditions forms that we have ticked off and agreed with throughout the past decades, we do not know which is responsible for the particular advertisement we are seeing, or who is paying for it to appear on our feed in the first place. At the current rate, a user would have to spend hours to opt out of all interest and preference that Facebook has on us, not even mentioning the terms and conditions of third-party websites. (Faizullahoy & Korolova, 2018; Denham, 2018) Besides, according to a study performed by Fox & Royne (2018), even a condition as plain as having terms and conditions that are too complicated for the average consumer to understand might be seen by them as breaching a social contract (being presented important information about one's safety in a comprehensible manner) and thus decreasing the consumers' trust. This might not only be an issue for the social media itself, but also for the entities that use it to advertise their products and services. Although the information in terms of conditions of use are meant to be for the consumer, they are too often meant merely to circumvent privacy litigations—not to be understood by the average consumer. (Fox & Royne, 2018)

What makes many scholars as well as common citizens so concerned is that by allowing political micro-targeting to be run on social media user data (as we would with any other micro-targeting), we are essentially treating our democratic voice (i.e. voter participation) as simply another commodity available on the free market to the highest, most skilled and data-equipped bidder. (Gizzi, 2018) But since we are already treating our personal data as a commodity, perhaps it should not come as surprising that the same fate awaits all that our data is related to—including our privacy and fundamental rights. (Fox & Royne, 2018) As discussed in the Introduction, the personal sphere is something necessary for democratic liberation and self-determination, often protected by the constitution or democratic countries and cited in the Universal Charter of Human Rights, which is precisely why voter micro-targeting seems so disturbing an implication for democracy—even those who do not think of microtargeting in philosophical terms. (Rubinstein, 2014) Though their storage of data, their anonymization and aggregation is regulated (and more so in the EU than elsewhere in the Western world), authorities are short to respond to every new product with new legislation in a timely manner—contributing to a reactive rather than preventative system of establishing preventative measures against data breach offences. (Klingspor, 2016)

The suggested remedies for the perceived (and legitimate) loss of privacy are multiple. They encompass both legislative and corporate changes, some of which have already been at least theoretically imposed by the European GDPR directive. These suggestions are divided into three categories: public transparency, disclosure for users and control. ‘Public transparency’ covers issues such as the the public being able to learn about the types of data collected by any website and electronic means, how it is used and how it is shared with third parties, both directly and indirectly. It also suggests that the information available to users must be sufficient for users to identify and every website or application must disclose content they place on a user’s device and what its use is. ‘Disclosure for users’ includes suggestions such as the user being able to access complete disclosure of the data collected on them by a website or a third party, both directly and indirectly. The third category, ‘control’, suggests the following—a user opting out of being tracked and blocking disclosures to third-party cookies and services, such as clouds. Furthermore, consent to use one’s data must not extend to the data of their friends (as was the case with Cambridge Analytica personality quizzes) and users must also be able to delete the data stored on clouds, or alternatively to identify, uninstall or terminate any such content on their devices, while the disputes about user data must be pursuable under conditions that are not restricted by licenses or arbitration processes. Minors should be exempt from releasing their private information. In case data breaches do occur, users must be informed about them, as well as about the source of their privacy violations, while

advertising based on one's data must always be clearly identified as such, and lead to the ordering party or company collecting the data in such cases. (Isaak & Hanna, 2018)

Currently, GDPR is European Union's best hope for data protection. European data privacy law also requires transparency about personal data processing as well as about most forms of online targeted marketing. Organizations using personal data are obliged to be transparent about their use of said data, and are also obliged to disclose information about the purpose of personal data processing. (Borgesius et al., 2019) At least in Europe, therefore, and at least in legal theory, political parties and their hired intermediaries that collect personal data for their microtargeting operations are obliged to disclose on their public websites what data they use and for what purposes. The EU e-Privacy Directive further imposes transparency and requires consent for cookie tracking, which is also often employed in collecting politically interesting data on citizens. As such, companies are also obliged to inform users of their websites that their data is being used for political targeting as they roam the free web. (Borgesius et al. et al., 2019) While the fact that these disclaimers appear on websites and need to be consented with does not alone mean that their visitors will also read them and absorb their full meaning and implicants, it is at least a start that gives them the opportunity to do so—and to simultaneously make microtargeting less transparent of a method.

Klingspor (2016), however, suggests a broader change than that of policy, namely that of a fundamental change in style of legal approach. While currently, breaches in privacy are dealt in a constitutional state (devoid of preemptive action, and investigating and punishing offences only once they objectively occur), to a preventative state. A preventative state would mean a certain degree of restriction of the freedom of action, compensated for by an intense discussion on all possible breaches of privacy (i.e. before the establishment of a video surveillance) in order to avoid smearing the fine line between security and upholding fundamental rights. The end goal would be to prevent as many offences as possible before they happen while also respecting the privacy of individuals, an end that can only be achieved through a thorough public debate. The author suggests this is at least possible in Germany, where the current trend of legal rulings suggests a tendency towards the preventative approach. What effects this would have on the decisional autonomy and perceived privacy of citizens is yet to be determined.

3.6 The Consumer Perspective

Although a majority of them report feeling concerned about their privacy online and on social media, even those who are especially sensitive to the idea of such threats still continue to use them

and share large amounts of their private information through them. (Mahmoodi et al., 2018) Interestingly, users tend to be more concerned about the access to their data and their unauthorized secondary use (i.e. by third parties) than by the data collection itself. (Esrock & Ferre, 1999) One of the possible explanations for the cognitive dissonance resulting from using social media while also being concerned about one's data, also referred to as the privacy paradox (Norberg et al., 2007), is the privacy calculus model. (Mahmoodi et al., 2018) According to the privacy calculus model, the extent to which we choose to engage in disclosures on social media networks and related activities depends on us subjectively 'evaluating the resulting risks and benefits' (the benefits being, f.e., social gratifications). (Trepte et al., 2017) If the benefits outweigh the risks of disclosure, a user goes ahead with the disclosure. Other factors that also play a role is a lack of knowledge about privacy functionalities (which the social media in question do not go out of their way to illuminate) and a perceived lack of viable alternatives. This constitutes an asymmetric relationship between users and providers, putting the users in an unfavorable position with little bargaining power to protect their privacy. (Mahmoodi et al., 2018)

To address the concerns users have about their privacy in a comprehensible manner, Malhotra et al. (2004) developed a model called the Internet Users' Information Privacy Concerns (IUIPC), which consist of the three dimensions: collection, control and awareness; and argues that users have the right to control all three, how their data is collected, stored and shared. Using previous research on the topic, Mahmoodi et al. (2018) concluded that users would be willing to pay for enhanced privacy services based on a tradeoff of the following cognitive mechanisms: perception of usefulness, risk and trust towards companies and services. Different levels of privacy concerns could require different modes of premium accounts catering to the said concerns. (Krasnova et al., 2009) More research is required on the topic to identify the specifics of such tradeoffs and how much users would be theoretically willing to pay for them, which could also serve to determine which aspects of privacy they value the most.

But whatever means and measures are drafted in theory, social media will likely do their best to counter them. Social media devote countless energy, financial resources and brain power to make their products appealing and even addictive. Facebook, despite the numerous privacy-related scandals it is currently entangled in, still harbors a user base of more than 1 billion per month. Furthermore, Facebook CEO Mark Zuckerberg, under scrutiny of the US Congress, stated that Facebook would not take a hard line approach towards political advertising. In contrast, Twitter, a platform populated and favored by political communication, decided to ban political advertising altogether. (Kovach, 2019). But even with such events, which make global headlines and dominate

public discussions for weeks, it is questionable whether they can at all significantly and negatively affect the attitudes of billions of Facebook users.

3.7 Young People, Privacy and Democracy

Although the research into young people and privacy with regards to social media is not extensive, they do represent a particularly interesting age group whose interactions with social media are worth noting. After all, young people (adolescents, teenagers, young adults) were some of the early adopters of social media such as MySpace, Facebook, Instagram, ICQ, etc., particularly because they are digital natives and the internet comes to them as natural as TV does to their parent's generations and the radio does to the generation of their grandparents. However, at the same time, they are also a particular age group in that they may not realize the practical implications of their actions precisely because of how young they are. Youn (2009) examined the privacy concerns of adolescents over a decade ago, and while the state of affairs is likely to have evolved since, the perspective they presents is nevertheless valuable. Contrary to the perspective of a clueless teenager addicted to smart technological tools, his research showed that pupils as early as in their 7th or 8th grade were able to understand the negative consequences of Internet use, including online privacy invasion, reporting being cautious about the information they disclose about themselves online. Youn's (2009) study also found that the more benefits adolescents perceived in disclosing their information, the less they were concerned about their privacy (in line with the privacy calculus model), while, in contrast to that, the perceived vulnerability caused by information disclosure was positively related to increased privacy concerns. The perceived risks were increased when self-efficacy was not related to privacy concerns, similarly to the study performed by Dobber et al. (2018) on adults.

How we evaluate the risks and benefits mentioned in the privacy calculus model also depends on cultural factors—people from more individualist nations find it less important to generate social gratification on social media, but and also less of a need to safeguard their privacy. (Trepte et al., 2017) Slovakia, which will be the focus country of this research, ranks in the middle on the individualist-collective scale ("Slovakia - Hofstede Insights", 2020), which makes any implications about its citizens' privacy calculus according to this model difficult. Slovakia also ranks in the middle of the uncertainty avoidance scale, which is positively correlated to higher concerns about privacy. A study performed in the Netherlands (Dobber et al. 2018) confirmed the inconclusiveness of demographics, but highlights a long-term reciprocal relationship and a negative downward spiral dynamic between attitude towards political behavioral targeting and privacy concerns.

Thus far, 41% of millennials (i.e. already adults) reported that they use Facebook less as a result of the platform's privacy scandals (but as far as they still have the account and visit third-party websites, their data is being collected). A spillover of their reluctance to use the platform as much to age groups is also questionable. (Herhold, 2019) Perhaps it is only a part of a wider trend in which young people (Millennials, Gen Z) are leaving Facebook for Instagram, TikTok or Youtube regardless of micro-targeting, because they view Facebook as the platform of their parents' generations. (Even so, micro-targeting campaigns generally prefer older people as their targets, but whether this is because of their social media use patterns is unclear. (Endres & Kelly, 2017)) According to Klingspor (2016) privacy is especially relevant to young people. In general, a functional private sphere allows us to evolve mentally, but for young people, who are only yet to find themselves spiritually and define themselves intellectually, a private sphere is crucial. It allows them to learn to think for themselves and to act self-confidently, while the less a teenager (or young person) has trust in their own privacy, the less confident in themselves they will be and the more they might conform instead; the less they will find it easy to rebel against their group peer norms. Trepte et al. (2012) further states that privacy allows us the benefit of autonomy to break social norms and to experiment with new ideas and ways of thinking.

3.8 The Specifics of Eastern Europe and Slovakia

Eastern European youth (as well as the general population) is somewhat specific due to the particular political climate that they inherited and grew up in. Democracy had only been established in Eastern Europe (including Slovakia) after the 1989 'Velvet Revolution', thus dating only slightly over 30 years back into the past. This plays out in a multitude of ways related to democracy and, more importantly, the perception of democracy. A recent report conducted by GLOBSEC (2020), which categorizes Slovakia under 'consolidated democracies' in the CEE region, found out that only 49% of Slovaks support a liberal democracy with regular elections and a multi-party system, while 38% would prefer a strong leader who can bypass parliament or elections. In fact, liberal democracy has witnessed a decline in popularity within the central and Eastern European region, and a partial decline to populism and authoritarianism. While this is especially prominent in countries like Poland (PiS) and Hungary (Fidesz), Slovakia is not exempt from the trend either. (Krastev & Holmes, 2019) Disappointed by their 30-year quest to become more like the countries of the former Western bloc, embittered Eastern Europeans whose collective memory seems to turn foggy with regards to their authoritarian communist past, flock en masse to strong leaders who promise to unburden them from democratic processes and instead offer clear and simple solutions to complex issues. European liberalism, multiculturalism and progressivism are often framed as the

main enemies of national sovereignty and ethnic heritage among these young democracies. (Krastev & Holmes, 2019) In Slovakia, a particular perceived threat to national sovereignty comes from the USA - 53% of the population views it so. (GLOBSEC, 2020)

Furthermore, according to the Pew Research Center ("Views of democratic satisfaction across Europe", 2019), only 52% of Slovaks are satisfied with the rule of democracy they witness in their country, and while these are not the worst results within the EU (in fact, satisfaction with democracy has risen in the CEE region over the last the years 1991-2019), neither is it a wholly optimistic insight. The same study states that the more educated a person is, the most satisfied with democracy they seem to be (+14). Still, Slovakia is among the more optimistic of the CEE region. Throughout the last 10 years, more people in Slovakia see the value in voting (+29), more believe that politicians are working in the favor of the general population (+17) and more people think that elected officials care about them (+14). ("Views of democratic satisfaction across Europe", 2019) When it comes to reliability of the news, 44% of the CEE population trust in media, in Slovakia this figure is 46%, while 79% of Slovaks believe that the media are free of influence. If they believe them to be influenced, it is by financial groups and oligarchs rather than the government (46% vs 23%). On the other hand, Slovakia is the most prone to believe in conspiracy theories of all observed countries. 60% of them believe world events are coordinated not by governments and political bodies, but by secret groups aiming to establish a totalitarian world order. (GLOBSEC, 2020) The belief in conspiracy theories and in the news offered by the so-called alternative media will be one of the focuses of this research, which makes this statistic particularly insightful.

In general, however, this data refers to the whole population and less so to young people. The National Democratic Institute ("As Democracy Wavers in Central Europe, Young People Consider Their Options", 2018) offers some insights on young people's perception of democracy. For instance, while young people (aged 16-29) living in the CEE region (specifically Hungary, Poland and Slovakia) consider democracy the ideal ruling system (70-80%), they are dissatisfied with the political situation in their respective countries. Only 38% of all Slovaks are content with how democracy functions in their country (GLOBSEC, 2020), but again, these are results non-specific to the youth. The most formative event related to democracy that Slovakia has witnessed in the last years (as seen by the report by GLOBSEC) is the murder of investigative journalist Jan Kuciak and his fiancée Martina Kusnirova, which sparked massive anti-government protests and led to uncovering corruption schemes among the ruling party, financial groups, judges, and civil servants. A cleansing process of these structures has begun, but the repercussions of these findings and the damage they have to people on a subconscious level are no doubt large.

Taken as a whole, young people are the future's electorate, the biggest living generation (at least in the US), and have spent a considerable portion of their lives online and on social media. Their lives are digilog—they no longer differentiate between the online and the offline world, but rather see them as complementary. ("How To Grow Your Business Through Online #Marketing", 2019) They likely cannot remember a world without micro targeting, social media advertising, and politicians fighting over their attention on the internet. How and why they vote, based on what information, and whether or not they engage in democratic processes is of grave importance to not just political marketers, but also researchers, politicians, and the society at large.

In Slovakia, according to a poll conducted among young people in Slovakia (18-30 years old), 18.9% of them would have voted for the far-right, borderline fascist in January 2020 (the representatives of the party LSNS have been accused of crimes such as praising the Slovak and German Nazi regimes, wearing fascist-era uniforms, denying the holocaust, using Nazi symbolism, and enticing hatred against minorities). Such electoral results would have secured the anti-EU party a majority in the parliament. (Gehrerová, 2020) Looking at the patterns of behavior of the young electorate therefore seems to be of vital importance.

But whatever insights this thesis will offer, whatever stances and approaches young people will display with regards to microtargeting and democracy, one thing is certain. Big Data cannot and will not be abolished or stopped. Today, data is more valuable than oil. ("The world's most valuable resource is no longer oil, but data", 2017) In a sense, talking about its use and practices is the only thing that can be done to facilitate public interest and trigger more transparent measures in data handling through public debate. This master thesis is one such attempt and simultaneously a direct reaction to such a public discussion.

IV. Research Questions

In the light of evidence and existing research provided, especially that on the effects of being surveyed on one's personal autonomy and decision-making processes in a democratic context, this master thesis will seek to further explore the effects of micro-targeting campaigns on the possible erosion of trust in democratic processes among the youngest electorate portion. It will do so in the context of Slovakia, which held its parliamentary election on 29 February 2020, thereby offering a unique opportunity to explore voters' attitudes prior to a national election that dominates the communication channels in the country, with the possibility of prompting an increased degree of attention to micro-targeting campaigns in the voters who participate in this research.

The main research question will therefore be: **How does the use of microtargeting affect the trust young people (ages 19-24) have towards democratic processes in their countries and beyond, specifically in the context of Slovakia?**

Some additional research questions the thesis will explore will be:

- To what extent does microtargeting contribute to an increased feeling of being surveilled among young people, and if applicable, how does this affect a young voter's self-determination and sense of autonomy in the context of exercising their democratic rights?
- How does the sense of an invasion of privacy affect young voters' actions regarding their safeguarding of their private sphere?

While this master thesis does explore the theme of privacy and microtargeting, the topic of privacy will not be explored explicitly throughout the focus group proceedings, as it will be far more interesting to see whether microtargeting implicitly leads or triggers young people to making the associations between microtargeting techniques and concerns about their private sphere. Generic questions about protecting their online presence will be posed.

V. Method

5.1 Qualitative Approach

Since the topic at hand (micro-targeting in this specific geographical context) is rather unexplored, it is best to go ahead with an explorative method—i.e. to use qualitative research. Qualitative research allows an in-depth approach to unknown phenomena, and while it does not aim to capture a representative sample of the whole population, it is instrumental in building a case on single instances that are studied extensively until they yield results that can be added to the general discussion, in this case, the general discussion on microtargeting and privacy in the context of exercising one's democratic rights (or all three separately). (Flick, 2016) The material gathered can then be used to represent a certain typology of cases (young voters/people from Slovakia) and quantitative research can be built on the knowledge of these cases, if applicable.

The explorative factor of a qualitative approach will serve two functions in this case. First, it will illuminate a topic in a geographical area where it has not received enough attention yet (the closest studies on microtargeting occurred in Germany (Papakyriakopoulos et al. 2017) and Eastern Europe (Faizullabhoj & Korolova, 2018)), and second, it will consider that the participants themselves might not know a lot about microtargeting and the privacy concerns related to it. (This assumption is based on existing research and the level of public discussion on the matter.) Hence, a qualitative approach will be better-suited for a general discussion about a topic that might be vague to the involved research participants, or one that they need help with (via triggers and cues) to discuss at length.

But since the data collected in qualitative means is so rich (and yet, not standardizable), it needs to be coded and analyzed in a reliable and valid manner. Qualitative research, however, does not aim to fulfil the quality concepts of reliability and validity in the way quantitative research does—it aims to be informative and serve as an inspirational stepping stone to be built on and next to. Hence, qualitative research aims to fulfil the quality criterium of *trustworthiness*, which is defined as an extent to which the data, their interpretation, and the method used for this interpretation ensure the quality of a study. (Elo et al., 2014) In qualitative research and more specifically content analyses, this can mean the establishing of a replicable and well-structured protocol of proceedings for those who wish to review the study, and/or providing a reasonable justification of coding categories, as

well as the concepts that stand behind them and how they have been arrived at. (Both will be done in this thesis.) All such steps are to be approached with a high degree of transparency to justify their choice in the given research context, as well as to make sure that the research in question lives up to the four components of trustworthiness, which are, as established by Guba & Lincoln (1994): **credibility** (those participating in research are described accurately), **dependability** (stability of data overtime and under different conditions), **confirmability** (objective evaluation of data), and **transferability** (extrapolation potential). These criteria should be reviewed and referenced throughout the research process.

5.2 Focus Groups

Focus group discussions have great potential for empirical research of unexplored topics, but with a defined research interest, or target group, in mind, as is the case in this particular context (young people from Slovakia). There are several reasons for this. First, focus groups reduce the hierarchical gap between researcher and subject, since the subjects make up the majority of people present, which is expected to make participants feel more confident and less under pressure to express their opinion and experience. Secondly, the exchange between ‘equals’ encourages positive group dynamics and creates an environment similar to everyday discourse—or as similar as regulated social science research can get. Observation of natural environments would be easier, but would not allow the moderation of the discussion in a productive manner. Thirdly, since the majority of the discussion is to take place between participants, rather than under a dynamic that would include the participants being interviewed directly by the researcher, this allows a freer exchange of ideas and less concerns about having the ‘right’ answer ready. (Przyborski & Wohlrab, 2014) This is important because attitudes and behaviors are linked to social contexts and can therefore be researched best in social situations such as focus groups—i.e. the ‘natural’ conditions in which people disclose information about themselves, especially in case the information presented concern things as sensitive as voting attitudes, privacy practices, the exercise of democratic rights and the awareness of one’s autonomy. And lastly, during group discussions (as opposed to an interview), social mechanisms such as group norms or cultural values can be observed. (Prinzen, 2018) This is especially valuable if one wishes to explore an unknown topic in a particular social setting and in a particular social milieu (such as young people from a certain geographical region, with a certain pre-defined degree of education). Many unexpected group mechanisms can emerge and enrich the discussion in ways that might not have even been predicted or hypothesized.

5.3 Sampling

Qualitative research requires purposive sampling. (Przyborski & Wohlrab-Sahr, 2014) In this case, the sampling followed according to predetermined criteria to represent a specific group of young people: young people (young adults, 18-24) living in the capital city of Slovakia (but may come from elsewhere), mostly studying (or having studied) at a university. These criteria (urban capital dwelling and a university background) were twofold—firstly, their selection was practical due to the fact that I myself am from the capital, know most people my age from the capital and found it easier to arrange venues and schedules within my hometown; and secondly, it is to ensure a higher degree of awareness about public affairs as well as the international political scene, since the capital city is where most public democratic institutions and universities reside, as well as where most periodical broadsheet media are published. While informedness about public affairs is something that transgresses geographical boundaries, cities and especially capital cities are places where more politically relevant events take place, while proximity to such events may play a role to awareness about them—as defined by the news value theory, specifically by news value proximity (Nähe) and relevance. (Maier, Marschall & Stengel, 2010) Furthermore, the education factor was chosen based on the Pew Research Center report that found out that people with higher educational achievements display a higher degree of satisfaction with democracy as a system. ("Views of democratic satisfaction across Europe", 2019)

While it is vital to keep in mind that such selection (purposive sampling) will not mirror reality 1:1, as is already established by the choice of qualitative methodology, it can nevertheless serve as an approximation to it in its particular context. (Przyborski & Wohlrab-Sahr, 2014) The participants were selected according to their availability (in terms of time and place) and contacted mostly through social media: Facebook student groups, Facebook messenger, WhatsApp friend groups, or recruited through friends, who study at universities in Bratislava or elsewhere (in such case, mostly abroad).

5.4 Qualitative Content Analysis

An evaluation methodology that has proven to be particularly effective in analyzing qualitative interviews, such as focus groups, is the thematic-structured qualitative content analysis according to Kuckartz (2018). This analysis proceeds in seven phases.

Following this approach, it is to will start with an initiating text work in **phase 1**. At this stage of the process, one is to read the transcribed interviews carefully, while marking all seemingly relevant text passages. All peculiarities and conceptual ideas for the evaluation should be recorded, notes and remarks are to be written down at the margins. At the end of this initial phase, one should write the first short case summaries.

The main objective of this approach is to create a thematic structuring of the collected data. The generating of main categories, which occurs in **phase 2**, and a further differentiation in subcategories can follow an inductive or deductive approach, but in most qualitative research projects, both methods come into effect—first a general idea of deductive categories derived from the research question, as the design of the inquiry predetermines certain themes, and then an ad hoc generation of further categories that arise from the transcript analysis. After developing, testing and defining the main analytic categories, one can start with **phase 3**, the first encoding process. During this phase the complete material is encoded. Text passages that have no relevant content concerning the research questions can be left out.

In **phase 4**, the encoded passages are to be compiled according to the categories they have been ascribed to. In order to further differentiate the main analytic framework, one has to determine subcategories inductively in **phase 5**. After all main and subcategories of analysis have been determined and defined appropriately one has to work through the complete material in a second structured encoding process. With the completion of this **6th phase**, the time-consuming task of structuring and systematizing the collected data is finished and the actual interpretation and working out of findings can finally be carried out in **phase 7**.

In order to ensure smooth proceedings of the content analysis and the integration of most of the aforementioned steps into one software, MAXQDA, a software for content analysis, will be used. As such, no steps of the encoding, category building, separating text sequences according to codes and subsequent analysis need to be done manually, but are done in one place and easily so. Data files can be exported from MAXQDA in both excel (numerical, statistical) and word (text) format. Although MAXQDA is often used for quantitative approaches, in this case, it will be used to sort the respective themes of focus groups into easily discernible categories which will then be examined in a qualitative manner, i.e. not in a statistical analysis of the quantity of quotes and their quantitative patterns, but identifying thematic patterns, pointing out their specifics, outliers,

noteworthy occurrences, and working towards an image of what young people in this specific cohort have to say on microtargeting and its effects on democracy.

5.5 Focus Groups Protocol

Before participants can take part on the focus group, they will be required to sign a consent form that will inform them about the use of their data, as well as the rights they have to their data under GDPR.² Once the consent forms are signed, participants will be thanked for their attendance, instructed on the proceedings on the focus groups (i.e. there is no wrong answer, do not speak over one another for easier transcription, only reveal as much as you are comfortable with, speak clearly, you can always leave the discussion, etc.), and the discussion can begin. All focus groups will take place according to the following protocol:

Part 1: Opening stimulus

Familiarize participants with the topic and trigger a spontaneous discussion

- *Show a photo³ of Mark Zuckerberg's Senate hearing - explaining how Facebook facilitated the leak of data - give them all a time to look at it*
- Ask: "Do you know who's in this picture? In what situation? What went on in here? What do you remember about it? Why was MZ called in front of the US Senate? What were they discussing?"
- Try to gently steer them in the direction of data leaks (unless they arrive at it themselves), selling big data, micro targeting (help them only if necessary)
- Do not stop until the word micro targeting (whether spontaneously or with support) is uttered, then move on to part 2 (unless it is not uttered at all because the participants are not aware of what it is)

Part 2: Micro-targeting

- Ask: what is micro-targeting? What do you know about it? (let them explain in their own words, unless they do not know what it is at all, in such case, explain what it is)
- Ask: What do you think about it? How do you feel about it?
- Ask: What do you think are its strengths and weaknesses?
- Ask: Are there any positives or negatives? If so, what are they?

² The consent forms are stored in both physical and electronic form and can be retrieved upon request.

³ Appendix 1

- Ask: Explain how you think micro-targeting is being used. (In order to establish a knowledge base of participants. This is only to be done if they have displayed any knowledge of microtargeting previously.)

Part 3: Micro-targeting and you

Once the general information about MT has been discussed, move on to the personal connection—how does microtargeting affect them? But do not make a connection with politics yet.

- Ask: How do you feel about your data being used for micro-targeting? Do you think it's being used at all? Do you connect this phenomenon with Slovakia at all?
- Ask: What do you think your data is being used for?
- Ask: Where are the borders - what is acceptable with MT and what isn't?
- Ask: What are you willing to do to stop what is unacceptable (as defined previously) happen to your data? What powers do you think you have as a citizen?
- Ask: Do you think you can protect your data? Do you think you need to? **Why? Why not?**

Part 4: Cards, meanings and associations

Following the intensive questioning defined above, loosen up the atmosphere with a little 'game.' Cards with words or phrases on them will be shown and the participants will be asked to either explain what they mean, or what they associate with them. There is no right or wrong answer.

- Brexit, Trump 2016
- Cambridge Analytica / AggregateIQ
- Russian bots / Russian interference
- Fake news
- Alternative media / alternative news
- GDPR
- Facebook / twitter
- Voting
- Democracy

Part 5: Micro-targeting and democracy

After confronting them with the idea of voting & democracy, while also bringing up a few notorious examples where these were heavily discussed together in MT (Brexit, 2016 US election, Cambridge Analytica, etc.), stir them into the direction of connecting democracy with MT.

- Ask: Do you think micro-targeting is being used to influence people in democratic processes? Do you think this has happened already? Do you think it only happened in the UK/US or that it also happens here? Is this ok?
- Ask: Do you believe the use of micro-targeting can affect our democracy in any way? How? Give me examples based on your experience, if possible.
- Ask: There will be **an election in Slovakia in February 2020**. Do you know who you will be voting for? How have you arrived at your decision? Where did you get the information about your preferred candidate? Where do you notice the most advertising about them?

Part 6: How do you feel about micro-targeting and democracy?

Having discussed what has been discussed, ask them the final questions:

- How do you think democracy can change with MT? Do you think it can change?
- How do you personally think about your democratic rights in light of these revelations?
- Do you feel safe about your data?
- In light of our discussion, has your opinion on anything discussed changed? Are you going to act differently now?
- In light of the upcoming election in February 2020, what do you think about MT? Will you be doing anything differently now that we have discussed this?

After the discussion, participants were thanked for their attendance. They were once again reminded of the use of their data with regards to privacy (recordings would only be used for research purposes, transcribed and not passed on further), while they always had the right to access, retrieve and retract (ask for deleting of) their data under GDPR.

VI. Results

Altogether, five focus groups were conducted, with 19 participants in total. The focus groups were held in the time period between 8 January 2020 and 18 January 2020, approximately 1.5 months prior to the parliamentary election held on 29 February 2020. Originally, 6 focus groups with approximately 30 participants (5 per focus group) were planned, but due to numerous cancellations of participants, time constraints (I moved abroad at the end of January) and conflicts of schedule, more focus groups could not be organized. This will be discussed as a limitation later on, however, when it comes to the contents of the focus groups, all groups provided thoughtful and valuable contributions. The focus groups were understandably carried out in Slovak, their translations will be used to refer to them in the body of the master thesis, while they are stored and available upon request in their original.

6.1 Initial Case Summaries

The first case summaries were drafted after the transcripts were made and read, in the form initial comments and reflective remarks on their contents. They do not focus on specific focus groups and their participants yet, but on a general theme set by the execution of the practical part of the research this master thesis set out to do.

The first thing that stood out after reading through the transcripts is that in nearly every group (perhaps except group 2) there was at least 1-2 participants who had a good idea of what microtargeting was, sometimes down to meticulous details, including the specifics of the case against Facebook, the reason for Mark Zuckerberg's hearing, the nature of Cambridge Analytica's involvement in Facebook's data use scandal, the use of microtargeting, as well as an established stance towards microtargeting. There were even instances when participants already conducted preventative measures to protect their data, ranging from installing software to changing their habits of use of social media. Overall, the initial awareness of microtargeting was higher than expected, which also made the discussion more fruitful and thought-provoking for others. In some cases, due to participants' pre-existing knowledge, they often admitted having learned nothing new, despite me presenting detailed information on microtargeting, its use, and the case surrounding Cambridge Analytica's use of Facebook user data.

The other surprising factor was a stoic approach to the current political situation with regards to microtargeting, as well as the political outlook in general. Most participants were cynical when it

came to evaluating political practices, taking it for granted that political parties use non-ethical schemes to retrieve voter data. In nearly all groups (perhaps, again, except group 2 and especially in groups 1 and 5), this cynical approach extended towards democracy and democratic processes in general. Perhaps as a result of the Eastern European political climate, recent political scandals, and perhaps also due to microtargeting (as will be discussed later) participants did not celebrate democracy or its principles, instead, citing its flaunts, criticizing the exploitability of voter preferences by dishonest political entities, as well as the limits of intellectual abilities and critical thinking of most citizens that contribute to democracy being an inherently flawed governing system. All participants, however, agreed that democracy is the best alternative of all systems and did not call for a change in the current ruling system, however, they hypothesized about (and simultaneously cited the dangers of) different minimum requirements one would need to fulfil before being able to vote (such as intellectual abilities, paying taxes, etc.). As such, it should be said that the participants, perhaps due to their national context, were walking into these discussions with reservations about the nature of democratic processes and disillusioned about democracy itself. Such tends to be the nature of public opinion in young or unstable democracies, such as those of the previous Eastern Bloc—as was already established in the literature review.

6.2 Main Categories & Subcategories

The development of first categories (both deductive and inductive) followed based on the research question, the pre-defined structure of the focus groups protocol, as well as the first reading of the focus groups transcripts, i.e. all before the first encoding process began. The following categories (or codes, as they are referred to within the program used for the analysis, MAXQDA) were thus established in this manner:

Research question based, deductive, established prior to proceedings:

- Microtargeting and Slovakia
- Opinion on microtargeting
- Own experience with microtargeting
- Microtargeting and democracy
- Associations (+ all cards as subcategories to ‘associations’: Facebook, Twitter, Brexit, Trump 2016, fake news, alternative media, Cambridge Analytica, Aggregate IQ, Russian interference, GDPR, elections, democracy)

- Elections 2020

6.3 Inductively Established Categories

After the focus groups took place and after their initial reading, it became apparent that one needed to distinguish between one's own experience with and opinion of microtargeting, and between pre-existing knowledge of microtargeting—which were previously grouped into one too broad category. While there were always participants within the group who knew what microtargeting was, some did not, and for them, the phenomenon needed to be explained (whether by others or by me). Hence, awareness of it prior to participating in the discussion differed from one's opinion on it, as well as personal experience with it (some of those who could not explain the phenomenon initially could recall a few experiences with being microtargeted when prompted by others and by the interviewer).

Furthermore, while the focus groups focused more on microtargeting than on privacy (but both form an interconnected theoretical basis of this master thesis), the way the discussions evolved made it apparent that a separate category would be required to address the topic of privacy in and of itself. Too many remarks were made on specific practices that ensure more online privacy and protection of one's data (mostly spontaneously) to bulk them in the category 'own experience with microtargeting'. Lastly, although the question about whether anything changed for the participants following our discussion was always meant to be involved, it was not conceived as a coding category in the beginning. In the end, whether or not participants took anything away from the discussion (rather than what this was specifically) contributed meaningful input into the discussion, functioning as a basis of knowledge, firmness of conviction and persuasiveness in one's stance regarding microtargeting and privacy in the online digital era. Therefore, these three categories were added inductively, while the transcripts were first read and before they were first encoded.

Proceedings-based, inductive, established post proceedings:

- Own experience with data protection
- Pre-existing knowledge about microtargeting
- Change of heart ex-post

6.4 MAXQDA Analysis

Upon close inspection and evaluation, no new categories arose once the material was encoded, as the ones defined before the first encoding sufficed for the purposes of the analysis. Since the proceedings were qualitative, the categories were broad to include a degree of variety, but at the same time, due to the discussions taking place in relatively strict attendance of the protocol, what the participants said could have easily been assigned to all defined categories (and those developed after the initial readings).

MAXQDA was used to establish categories (called codes), assign text from all transcripts into these categories (encoding) and to export files that group respective codes together in excel format, making the analysis proceedings more organized and transparent. MAXQDA thus grouped phases 3-6 of the content analysis according to Kuckratz (2018) into one program.

All text (transcripts from focus groups) was systematically sorted into categories and after no other categories were being built (i.e. a point of saturation was reached in category building), the analysis could begin.

Category code system was exported from MAXQDA in excel format, pictured below.

Code System	Memo	Frequency
Code System		265
MT & Slovakia		23
Opinion on MT		44
Associations		75
	<i>Democracy</i>	5
	<i>Elections</i>	5
	<i>GDPR</i>	13
	<i>Russian interference</i>	10
	<i>Aggregate IQ</i>	4
	<i>Cambridge Analytica</i>	5
	<i>Alternative media</i>	5
	<i>Fake news</i>	6
	<i>Trump 2016</i>	5
	<i>Brexit</i>	5
	<i>Twitter</i>	7
	<i>Facebook</i>	5
Change of heart ex-post		5
Elections 2020		8
Democracy and microtargeting		15
Own experience data protection		48
Own experience with MT		25
Pre-existing knowledge about MT		22

Frequency indicates the amount of times a portion of text was coded under the corresponding category. 265 codes were identified in total. Main categories are indicated in bold, as are the corresponding numbers of codes. Category names in italics indicate subcategories, while the number of codes associated with them are also indicated in italics.

From the frequency of codes, it is apparent that most participants had something to say about their opinion on microtargeting and were also able to talk about their experience with data protection. These were the main themes maintained throughout the discussions. Some codes, though seemingly less frequent numerically, coded large portions of successive text instead of smaller portions scattered across the transcripts. As such, the frequency in and of itself is not enough to express the duration and attention paid to topics discussed. An in-depth analysis of what was said, however, can do that.

6.5 Analysis

Codes are listed and analyzed in their order of appearance in the focus groups as presented by me. In some cases, if the participants started discussing a different topic from the codes unprompted, the order differed, however, this was mostly not the case. The analysis will take on a thematic approach, i.e. will not be recollecting what was being said per group, but rather per topic (theme). This is due to the fact that in most groups and most topics, answers overlapped and were similar to those of the other groups, and thus do not need to be mentioned per every single group, but rather, as a theme. If, however, there is a case in which one group excelled beyond the standards of another, or when a member of a group made an especially relevant comment, the group number will be mentioned for a clearer style of reference. Participants were anonymized, although their gender is sometimes made apparent when they are referred to as he/she.

6.5.1 Pre-existing knowledge about microtargeting

Firstly, a base at which the participants understood microtargeting practices needed to be established in order to know where to take the discussion from there—for both me, as the interviewer, as well as for the participants themselves. Pre-existing knowledge about microtargeting was meant to be activated by showing them a photo of Mark Zuckerberg in front of the US Senate. Participants were mostly aware of who Mark Zuckerberg was and recognized him as the CEO and founder of Facebook, some (about 1-2 in each group) were at least vaguely aware of how the photo came to be—i.e. due to a hearing related to Facebook. ‘Information leak’, ‘information leak to Cambridge Analytica that led to misleading the public opinion’ / ‘targeted ads’ / Zuckerberg ‘had to

testify about whether the data was provided in a legal way’, while the data was used ‘for political reasons’, or for ‘influencing elections’. One participant from Group 3 made an immediate connection with the so-called ‘Russian interference’, several cited Cambridge Analytica spontaneously. Another participant from Group 3 knew there had been several such hearings and this was only one of them, claiming that the series of hearings was about determining ‘whether Facebook bears the responsibility for what is published on it.’ The most accurate explanation came in Group 4: ‘It was about manipulating Trump’s election through (.) I mean manipulating the outcome of the election through social media, based on data,’ while Trump’s campaign was thus ‘able to dynamically personalize content to different users based on their preferences.’ The participant used the example of gun control and Hillary Clinton, who supported gun control, as one of possible issues that could be targeted specifically to gun owners to sway their political leanings. His explanation captured the essence of what microtargeting is believed to have been used for in the US election with the help of facebook data. It later turned out that the participant who made the comparison had a background in digital marketing. Only one group (Group 2) did not identify the purpose of the hearing, instead believing that it was related to the US government wanting access to Facebook’s profile data. (Reminiscent of the case when the US government demanded that Apple grant them access to an iPhone of a customer involved in terrorist activity, an event group 3 made a reference to. Interestingly, a participant from group 3 also stated they trust Apple the most because they were the only ones to *admit* providing data to the US government.) Most participants were not sure whether Zuckerberg’s hearing was in front of the Senate or Congress, which was reasonable, since both Senators and Congressmen/Congresswomen were involved in the hearing; both were mentioned frequently.

When further asking about what microtargeting was, once the term was mentioned (or had to be mentioned by me, if the participants failed to arrive at it themselves) participants from most groups had a good idea, sometimes even understood the phenomenon in detail; while others struggled, saying they did not know the term, or only ‘very vaguely.’ ‘Is it something like cookies?’ / ‘It’s when you watch something on the internet and then it jumps out at you everywhere.’ A participant from group 5 explained it as the ‘collection of data from different sources’ by ‘organizations.’ When pressed about who these organizations were, she grew unsteady and cited everything from surveillance and eavesdropping, police, secret services, to personal contacts helping one to get information on someone else—‘one thing is connected with the another.’ While she may be right about the different forms of access to one’s private data, her definition did not explain microtargeting in enough detail, but nevertheless illustrated the confusion users often feel about the means of data collection, the collectors and who they are, and the means under which they operate

(i.e. are they legal or not, did we provide our consent or not). Shedding more light onto such confusions was the very purpose of this discussion. When further asked about whether she believed ‘they’ (all the forces she named) were ‘watching us’, she answered ‘YES. That can be, that can be.’ Another participant, however, responded to her by saying this data is mostly acquired legally and in possession of 4-5 of the biggest ‘BIG DATA’ companies.

Others in the group, as well as in other groups, made the connection between one’s online activity (‘whatever you do online’ / ‘the pages you visit, things you click on’) and constructed user profiles based on collected data (‘they can measure how old you are, where you live, and so on’), which can thus be used to derive or determine a certain preference for a product, including a political preference for a political product. When speaking of it, participants claimed data-based targeting creates a ‘social bubble’ out of which we lose access to the others—ignorant of their beliefs and circumstances. Participants from group 5 were aware that microtargeting is largely useful to better the functionality of social media, such as Youtube (being targeted with videos one might like) but argued that people are often unaware of how they pay for such services—i.e. with their data. On its own, these participants did not disapprove of such collection, so long as it remains anonymous and cannot be tracked to the person who accumulated the data, which they believe is already possible (‘for example, google collects your location data and if they see which two points you commute between daily, they can easily find out where you live’). When it came to Cambridge Analytica, participants from group 5 cited the company being one of the few who used a ‘bug’ in facebook’s software, which allowed the company to gain access to not only the people who completed their personality quiz, but also their friends. They simultaneously expressed concern at people receiving news only from social media and called for a ‘better regulation’ of microtargeting connected to democracy. In general, participants from all groups were not unified on whether Cambridge Analytica gained access to user data legally (by getting user consent) or illegally—and if so, why this was illegal.

When it came to the actual content being shared and targeted at people politically, participants from group 4 believed it was ‘misleading at the least’ if not ‘completely false’, which is what made it an issue. Others argued political ad targeting must be regulated more tightly than any other advertising. Participants disagreed on how Cambridge Analytica and other such companies came to the possession of such data, whether ‘directly from users’ or through facebook acting as the middleman culprit. Overall, however, most groups arrived at sensible conclusions both when it came to what microtargeting was and why Mark Zuckerberg was being discussed in connection to microtargeting.

6.5.2 Opinion on microtargeting

While participants' opinions on microtargeting often transpired in other parts of the discussion, both previously and later on (i.e. in sections 'experience with microtargeting', 'pre-existing knowledge'), this section will nevertheless attempt to focus solely at their opinions, ethical dilemmas and moral confusions when it comes to the technique.

Most participants from all groups had mixed feelings on microtargeting. On one hand, they agreed that it can serve a good practical purpose. Sometimes, according to them, 'it makes your life easier', such as by recommending products one might like based on previous searches, or services one might need that are in their area. But there are several conditions where, according to them, microtargeting stops being convenient and becomes a problem. The first of such condition was when microtargeting is used for political advertising, the second what the data is being sold further to third parties, while the third condition is a lack of *informedness* or *awareness* about being microtargeted (a lack of *consent* is rarely the case - 'it's a sensitive topic because people think we didn't agree to it, but we did'). In the words of one participant: 'there should be rules that set what context the data be used in,' inasmuch there can be good contexts as well. When it comes to political microtargeting, several participants cited that is where they draw the line of good and bad uses: 'influencing the public opinion on a global scale is not morally digestible' / 'what Cambridge Analytica did was immoral' / 'I don't see a problem with microtargeting but with abusing data,' wherein by abusing data they meant meddling with democratic processes. The reason for their distaste for political microtargeting was what they saw it as adding more fan to the fire of unobjectivity and disinformation, i.e. by 'creating bubbles' and giving people 'tunnel vision' when they are provided with information that is not diversified, while the people themselves are not aware that the information is not diversified. Small 'disinformation media,' according to group 4, 'don't have enough money to target everyone, and microtargeting helps them see who they need to target and how they can grow their customer database.' According to them, microtargeting in such contexts can work nefariously, but slowly. '[microtargeting] can subconsciously change your mind on things, make you more bigoted.' A participant from group 3 used the example of prejudices to make her point — 'when you only see Muslims as being terrorists or Polish people only stealing jobs in England' for quite some time, this idea may cement itself in your mind. 'An ad is dine, but this is not,' she concluded.

A possible solution would be to read more, and from various sources, many claimed. 'There will never be such thing as objective news but you can come close to it' by consuming information from various trusted sources, said a participant from group 4, but as they also admitted themselves, this is

not entirely possible with microtargeting. As one participant from group 3 countered—‘but [people] don’t realize the information they get when they search for something is also targeted at them.’ As such, one participant from group 4 compared microtargeting to only reading a very biased source of information, such as a one-sided medium. While the information such a medium offers is not an outright ‘lie’, it is ‘not reality either’. A participant from group 2 voiced the opinion that this is ‘partly a Slovak problem’ that people are not educated enough on this matter, while in order to make truly ‘free decisions,’ argued a participant from group 4, they would need to know that they are being targeted and not making their choices based on objective information. This reflects the point made about decisional autonomy in the literature review, and how it is lacking under conditions created by microtargeting.

Another important issue made with regards to microtargeting and autonomy is a lack of time, and a lack of tech literacy. While participants generally agreed that one must search for information themselves, some also realized that this is an unrealistic expectation to have of all citizens, while many are not even aware of all the settings they could change to be tracked less (i.e. location settings in iOS, as mentioned by one participant from group 3). ‘Then [people] get the government they deserve,’ a participant responded. When prompted about education on data literacy, a participant from group 2 thought this should be the case, but only for ‘older people’. In other words, she seemed to believe that younger people are in no such need, despite the fact that these discussions revealed repeatedly the gaps in knowledge that even younger people from an educated background have. For instance, participants frequently showed confusion and ignorance when it came to providing consent to data collection. ‘I didn’t say they could use it’, one participant from group 1 argued with regards to data collection. ‘Yes you did,’ was the response, and an explanation about general terms and conditions of use of social media followed. Others from group 3 argued that no one has the time to read the terms and conditions (‘someone calculated it would take I don’t know how many months’), but that social media are law-savvy enough to set the terms and conditions in a way that makes it the users’ fault legally if they did not read them nevertheless. Several other participants seemed unsure about to what extents their consent went and whether or not big data companies and companies like Cambridge Analytica did anything wrong, or whether their ‘crime’ was simply that of an ethical character.

What most participants could agree on, however, was the use of microtargeting for marketing purposes, especially those from group 4 saw it as a smart business and marketing tool. As such, they said that no good tool can sell a bad product, or, on their words, a political ‘throttle’ (they used specific examples of Slovak politicians, but quickly came to realize that they are nevertheless popular). ‘It’s good business,’ commented a participant from group 2. Another one filled her in -

‘you can decide if you buy it or not, it’s up to you’ as they talked about basic consumer goods. ‘It’s an absolutely legitimate method for marketers,’ said another from group 3. ‘But the other side, the privacy issue, that is something I don’t have a clear opinion on.’ / ‘I decided to click on it, I can also decide not to. But the service is usually worth it,’ admitted a participant from group 4. A participant from group 3 wondered about what she could do to not be tracked and figured the only thing was not using a phone or google, but admitted herself that that will not be the case. Another participant suggested two versions of social media like facebook as a solution—one paid, for those who do not wish to be tracked, and one free for those who do not mind. The participant emphasized the fact that we are paying for facebook currently, with our data. Another from the same group suggested that ‘it’s impossible NOT being followed or watched these days,’ so her solution would be nameless data. ‘You’re not important enough to be hunted down that way,’ she thought, but admitted that even the awareness of the possibility is making her uncomfortable. A participant from group 2 kept up the theme of anonymous data. ‘No one cares about my little data, but it feels uncomfortable that they’re out there.’ If being followed and watched was a given, then, according to a participant from group 3, at least private messages should be off limits. She had an experience of receiving content based on subjects she only discussed in her private messages and felt ‘threatened by that.’ She compared the phenomenon to deception, which numerous participants labeled as problematic about microtargeting—i.e. ‘telling us they don’t use our data for something and then using them for it anyway.’ Several participants felt deceived by data collectors in that sense.

When prompted about the good purposes and uses of microtargeting, they had interesting points to make as well. Data can be used well ‘for creating AI and maybe some house robots,’ according to one from group 5. Others countered that such things already exist (citing google home and Amazon Alexa) but that the data such devices and services collect can be used in ways that users ‘definitely wouldn’t like.’ Others, from group 2, argued about use of data for ‘media literacy’ and ‘bettering democracy, educating us on topics I’m interested in (3) but then I wouldn’t know much about the other topics ((laugh)).’ As such, microtargeting proved to be a cyclical issue that brought participants back to the original issues they attempted to provide solutions for. Furthermore, participants from group 2 and 3 talked about using microtargeting (term used erroneously, as what they meant to say was ‘data collection’) for public safety, such as finding out that someone is building a bomb based on their searches or spreading child pornography. Group 4 used the ‘public safety’ argument as well. (One participant mentioned an ‘absurd’ news story from the UK, where a chemistry teacher became the target of public authority suspicion because he purchased materials that could be used for building a bomb, but only used the materials for his teaching.) A participant from group 2 offered an anecdote about her neighbour who received childhood pornography and

was questioned by the police as a result—without having alerted the police himself. Another participant from group 3 discussed whether data protection in some cases can be counterproductive and offered an anecdote from Germany, where, supposedly, GDPR is interfering with the police following sensitive searches, such as the ones mentioned above.

6.5.3 Own experience with microtargeting

Most participants had a conscious experience with microtargeting that they were able to recall spontaneously or after microtargeting was explained to them. They experienced being targeted across the world based on searches and purchases they have made in entirely different places. Some were also able to justify why they in particular were being targeted with a specific product or service. To such experiences, they reacted both positively and negatively. One participant from group 1 appreciated the practicality. ‘I mean sometimes when I something interests me I click on it and I look’ / ‘I noticed this basic thing, where if a person finds a flight, immediately this pops up, from what I saw, cars for hire and hotels in the area [...] when I’m shopping for perfumes it shows me different ones, which I don’t mind (.) at least it’s somewhat relevant to what I’m doing or what I looked for before and has higher chances of interesting me (.) than I don’t know, if they target me with a yoyo or something.’ Others noticed being targeted based on books they bought online, products for their dog, and perfumes again. As such, participants realized the practicality microtargeting has for advertisers—and not just when it comes to product targeting, but also product optimization. ‘You can set all these parameters on a product, make it more competitive, change features (.) so [microtargeting] can also be pretty useful during the phase before releasing the product,’ said a participant from group 4.

Several participants realized they possess a certain degree of agency when dealing with online ad targeting. ‘You CAN affect what you’re seeing. But you will still be seeing something. Usually stupid stuff.’ / ‘If we are aware of someone collecting this data, we can influence what is shown to us.’ / ‘Sometimes I just click on horrible ads to see what idiot would pay for that to show. So now I have terrible ads ((laugh))’ / ‘If I have the option to choose the (.) suggested ads then I just cancel it.’ Other reflections on microtargeting included participants in group 4 criticizing the monopoly-establishing behavior of digital giants like Google, for having used to ‘FORCE’ users to watch Youtube and other Google-owned products and services through their browsers, Chrome. ‘Google is a big supporter of these sharing things and it’s one of the reasons why you’re being followed by ads.’ / ‘Google chrome used to FORCE users to use it if they wanted the full functionality.’ In such cases, one reportedly did not have the choice to opt out of their data collecting policy, such as by using browsers which do not sell user data to third parties, which these participants found unfair.

When asked about what they believed their data was being used for, participants mostly agreed on product sales and less so political marketing. ‘If you google (.) I don’t know, a new Mercedes Benz, this is why you’ll see it on other sites.’ Some made somewhat irrelevant references to demographics-based targeting, such as seeing the billboards of certain parties only once they left the capital city—but such targeting has been the practice for decades and predates microtargeting, while also differing from it in its real-time adaptability and accuracy. But the geographic divide exists online, as well, according to a participant from group 3, who claimed ‘I am a liberal and live in this liberal bubble (.) that makes us forget about these threats that are outside’, by which he was referring to right-wing and populist parties influencing voters on social media. The bias between what was ‘acceptable’ and ‘unacceptable’ voting behavior (based on established parties of the mainstream versus the anti-system parties of the fringes of the political spectrum) became apparent for this particular cohort of participants. Some participants were being targeted with large amounts of political advertising, while some were not being targeted at all, which led them believe that they are not the desired target group, as discussed in group 4. One of the group realized he received political targeting from a party because he liked his friend’s facebook page, while the friend was a member of the party. Others reported being targeted inaccurately by parties they never affiliated themselves with or planned to vote for, such as right-wing or populist political movements. ‘Clearly [microtargeting] has some flaws.’

A participant from group 2 hypothesized about a generational gap in viewing and being affected by microtargeting, claiming ‘we’re all used to these ads because we go through facebook and instagram all the time’ but described how her mother comes to her with distress whenever she sees a targeted advertisement on her instagram. Another participant from the same group added: ‘I think the older generation is easier to influence with these ads’ particularly due to their lack of experience with the format.

6.5.4 Own experience with data protection

After having established what participants are and are not comfortable with, with regards to microtargeting, it was time to examine their habits and whether they reflected their concerns.

When asked whether they feel the need to safeguard their data, participants said both yes and no. If they said yes, they added things like ‘I like my privacy, but why (2) I don’t know why, I’d have to think about it’ / or ‘I don’t want to be identifiable’ but would not mind being a part of a data bundle. Yet, most others from all groups said they did not care much (‘I don’t care that they have data on me’) and were not willing to do much to change the status quo, if only to minimize the extent to which their data was being collected, mostly aware that a complete avoidance of microtargeting in

today's day and age is extremely difficult. 'It's my fault', said a participant from group 4 about being tracked, aware of data collecting on one hand, and still used the services that did it on the other.

When asked what measures they take specifically to avoid being tracked, various responses were given. 'Nothing' was one, but of the more proactive, Adblockers, VPNs, Tor, turning off various cookies (cross-linking cookies that pass on data between websites; regular website cookies), logging off of Facebook and messenger daily to avoid passing on their data from other services to Facebook (most others from the group 3 were shocked at hearing this), never staying logged into Facebook when watching Youtube or Google, using an alternative email to receive spam information, deleting records from Google (voice recordings) that became accessible after GDPR was introduced, not putting their phone number into Facebook, minimizing the use of Facebook, watching the content they make available online due to potential job searches, and more. Still, several participants admitted their measures were imperfect. Those who said they log off from Facebook's messenger or minimize their presence on Facebook admitted they don't do the same with WhatsApp or Instagram, both of which are owned by Facebook, thus 'it's the same.' A participant who logged off from Facebook admitted she knew some websites stored one's data (search history) and could provide this to Facebook even with the log-in delay. They also admitted the impracticability of this, i.e. being unreachable to friends, or not having access to the latest updates from university or friend circles if they opt out of using Facebook entirely. 'That's the network effect,' a participant from group 5 argued. 'You want to be normal, you want to do normal things,' another from the same group explained why they gave in to using social media and services that collect their data, reflecting that they felt like they were 'missing out' when not using the same services everyone in their social circle were using to stay in touch. 'If there was a paid social medium, I'd have no friends there,' joked a participant from group 5. Not using a phone was the bottomline of what one could do to avoid data collection (nearly) completely, but was proposed ironically, as a joke, making it obvious no one from the group was willing to take such precautions and make such sacrifices to their comfort and sociality.

A participant from group 5 admitted 'we don't know enough' to combat data erosion to places where they do not want their data to be. This lack of awareness became apparent as participants asked one another what their protective measures meant and entailed. One from group 5 asked whether using adblock meant her data would not be collected at all, the more experienced explained that it does not mean that, only that her data will not be targeted back at her in advertising. The participant who asked seemed dissatisfied with this answer. A participant from group 1 confessed she turned off cookies on Youtube, thinking it had a profound effect on her data safety, while others

from the group made fun of her supposed naïveté - ‘oh, my sweet summer child,’ they commented. She retorted ‘in my eyes that equals protecting my data, but I don’t know as much about it as you do.’ In group 5, participants inquired with interest about a browser mentioned by one participant, which supposedly does not sell collected data to third parties, blocks tracking softwares, and does not save one’s history. At the same time, they admitted such browser was less comfortable to use due to limited functionality (after finding a restaurant they wanted to visit, they could not simply click on a button to be transferred to google maps and see where the restaurant was on a map). When discussing why more people were not aware of such information, group 5 claimed ‘because they don’t want to us know’ (meaning big data companies and marketers who use our data) and because ‘people don’t care’, or think their data collection is harmless because ‘they have nothing to hide.’

The terms and conditions that one agreed to as a part of using social media were a controversial topic in some groups. In group 1, a participant argued why she can’t ‘stop them from tracking me, I mean what if I didn’t agree to it?’ while the others told her she did—by agreeing to terms and conditions. ‘Then at least they shouldn’t sell them further.’ With others in group 3, they created what they referred to as ‘cyclical problems.’ ‘If I don’t accept [terms and conditions], I won’t be able to update my phone software, apps, nothing.’ ‘It’s like bullying,’ another participant agreed. But while by some, this was presented as a matter of having no choice, others argued ‘you ALWAYS have a choice’ and compared agreeing to terms and conditions of use to agreeing to not steal anything when entering a TESCO. ‘There is a FUNDAMENTAL difference,’ others countered. ‘You can still go to TESCO if you want to steal something, but you can’t use an app without agreeing to being tracked.’ In the same group, an interesting situation occurred. The same participant who argued against terms and conditions being ‘enough,’ admitted to having failed to read the informed consent form she had to sign prior to taking part on the research. The participant who made the TESCO argument countered - ‘see, and [the interviewer] can shoot us now, maybe that’s what you signed.’ Although said as a joke, it illustrates the impracticality of terms and conditions and the lack of foresight users have when ticking them off in order to get to the service they wish to use.

When asked about why those who minded the collection of their data did so, interesting responses were given. ‘I don’t want them to have my characteristic built based on my data,’ said a participant from group 4. Another from the same group joked whether he does not want his ‘categories’ (i.e. porn categories) being accessible, to which the first participant responded they would not mind being a part of a bundle, but do not want to stand out. Group 2 argued that if someone wants to find something about ‘you, they will’. ‘We all have an account in the bank,’ a participant from the group

argued, ‘you can’t avoid being tracked.’ GDPR came up spontaneously in two groups. One participant from group 4 claimed one of the things protecting data is his ‘right to be forgotten under GDPR’ while a participant from group 5 said the directive has increased the awareness of data protection, which they saw as a good thing, but otherwise did not feel protected by the EU as a result. One thing that could be improved further, according to a participant from group 3, was making the option to retreat from an agreement (i.e. unsubscribing from a newsletter) easier. ‘It’s hidden, written in small letters and you have to click six times YES I’M SURE’ before unsubscribing from a service. Others countered that this would indeed be practical, but bad for business. This raised an interesting dilemma—should the customer’s interests be subordinated to the business objectives of a company, or the other way around? Participants did not arrive at a conclusion.

Several cautionary tales related to data collection were mentioned. One by participant in group 5, who found out google had been storing short snippets of recordings they made without his awareness via his phone speaker. The other was a member group 4 confessing he was called by research companies several times about things he did online, being unaware of how they gained access to his number. The third was more of a theoretical one, and came again from group 5. China and its surveillance system was used as the ultimate precautionary tale of what can happen when data collection and surveillance systems are ever-present and under the control of a central body—be it the Chinese government or one big data company.

6.5.5 Microtargeting and Slovakia

Initially, participants were asked about whether they believe microtargeting is prevalent in Slovakia as well. All responded that they believed so with various justifications. ‘It’s happening everywhere.’ / ‘I mean why wouldn’t it be here? If you have access to data, why wouldn’t you—’ / ‘Undoubtedly. It’s happening here.’ / ‘These days everything is so interconnected.’ ‘Yes, the globalization.’ ‘You don’t even know who owns all these websites.’ / ‘Like, if you travel to the other end of the world and still see things you searched for in the past (.) then it has to be global, no?’ / ‘I mean it’s not as intense in Slovakia but it’s becoming so [...] from the consumers’ point of view, it’s going to only get worse.’ / ‘It’s less present here [...] microtargeting is something less viable in less democratic countries (.) but it’s definitely going to grow here as well.’ Some reasoned that if facebook is global, so is microtargeting. ‘I don’t think facebook would come up with something like that and just intend it for a small population. It’s a world-wide app.’

Some made a direct reference to the upcoming election, although they were not prompted to. ‘With the election it’s going to happen more often.’ / ‘The closer we get to the election, the more of a topic

[microtargeting] will become.’ Some participants were already receiving vast amounts of political advertising—both from parties they aligned with and those they disagreed with. ‘I get these ads before every youtube video, I mean in the beginning it was mostly PS (party) and ok (.) I admit opinion-wise I am relatively close to them (.) but now I notice that it’s mostly anti-campaigns targeted at undecided voters.’ / ‘When I scroll facebook or instagram and watch cat videos, these days I get a lot of ads from SMER and Harabin.’ Several joked about being supporters of populist and far-right parties based on how often they were targeted by their advertisements through social media. ‘I mean I got an ad from SMER so it must be accurate ((laugh)).’ One participant claimed to be an inaccurate representation for the type of political advertisement he is targeted with because he uses adblocker.

Besides giving specific examples, participants discussed how and to what ends microtargeting can be exploited. Most groups agreed that for various reasons, fringe groups and extremist parties exploit such methods most often, whether because they do not receive enough media coverage for budget or political reasons, or because ‘polarization is always easier’. ‘Kotleba is going to exploit this so hard’ because his voters are ‘young and stupid’, and, according to the participant who made this claim, thus ideal targets for microtargeted ads on social media. A participant from group 5 complained how the shutting out of moderate voices by extremist parties may lead to moderate citizens believing they have no other option but to vote for an extremist party in order to be represented. ‘A citizen who is maybe a bit more Christian might not even see KDH (classical Christian democratic party) ads because the ads have made it so that he only see content from Kotleba (leader of far-right party) and so his worldview is skewed because he might not even know that KDH can represent his interests.’ Others pointed out the stark differences between the capital and the rest of Slovakia, which extremist parties might try to exploit. ‘You can see it when you leave the capital, a lot more of the billboards are about Kotleba.’ They discussed a case in which a Kotleba politician vowed to shoot a thousand bears if elected in an attempt to appeal to voters who live in small towns under the Tatra mountains and are common targets of bears looting their trash. ‘And this is it, we don’t see [the other ads] so we think it’s gonna be ok, a good party’s gonna win ((laugh)) but in the end (.) outside of Bratislava it’s something else entirely.’

Some wondered about why they themselves are targeted the way they are. A participant from group 3 admitted to have performed an ‘experiment’ with her Dutch friend. Together, they typed the word ‘Fico’ (name of the then-largest ruling party) into their messenger chat and saw that the Dutch friend soon received targeted ads for Fico’s party, SMER. Another participant had a theory about his age being the cause for being targeted by extremist or populist parties. ‘My theory is that many young people are undecided or decided not to vote at all and so (.) they’re not the existing voters but

new voters who represent a huge conversion potential.’ Age, however, can work in opposite ways as well. In group 4, participants discussed the age of targets ideal for microtargeting. One participant claimed microtargeting is useless for the then-ruling SMER party, since their voter database is made up of older people ‘fifty and older’. Another participant countered by saying ‘you’d be surprised by how many of these people are on the facebook. Look at our grandma.’

Overall, participants were convinced that they themselves, as well as the country they live in, are not immune to microtargeting techniques, although, due to the size and geopolitical context, perhaps more so than their Western counterparts. Many recalled being targeted and even had a solid awareness of who might find microtargeting most useful (as supported by literature on the topic) and why this is so.

6.5.6 Associations

The purpose of the association activity was to trigger the connections between said associations and the general topic of the focus group, and to thus elaborate and broaden the scope of the discussion. I believed that some of knowledge participants had on microtargeting and data protection would need to be activated to form connections they themselves were not aware of prior to joining the discussion (i.e. that microtargeting is related to fake news, the companies involved in microtargeting, several key elections connected to data collection and microtargeting, etc.). They were thus presented in an additive order that was meant to establish a connection between what was already discussed (base of participants’ knowledge about microtargeting, their experience with it as well as with data protection), and move on to the bigger picture; unless matters like the connection between microtargeting, election interference and democracy had already been established before spontaneously.

Furthermore, the associations activity was supposed to loosen up the atmosphere, similarly to the initial photographic stimulus; change up the flow of the conversation from discursive to impulsively saying the first thing that comes to one’s mind. Participants were encouraged to reveal what they associated with the phrases spontaneously, and psychologically, this also served as a telling method revealing something about their inner mental world. While they naturally influenced one another with their respective answers (as was the intention), the activity was meant to help them bridge microtargeting with democracy, elections, and their own sense of privacy online. Since this is a qualitative content analysis, the emergence of associations will not be reported on numerically, but rather, thematically—unless the numerical character of appearances is of particular relevance.

Facebook

Participants from all group associated Facebook with being a social medium, and thus with their social circles and the communication within them. Common associations were facebook's 'messenger' as a means to communicate with friends and acquaintances, another common association was facebook's flagship 'blue color', 'contact' to others, 'statuses'. A participant from group 4 associated Facebook with a 'loss of identity' (though they did not explain this further), while a participant from group 2 made the connection between Facebook and the other social media that it now owns, specifically WhatsApp and instagram, citing their 'monopoly' on communication. When mentioning messenger repeatedly, participants were prompted whether they recalled any advertising on messenger. Most were surprised that such a thing existed, and further admitted they do not watch messenger stories of their friends. When prompted about whether they trust Facebook with their data, most said no, but when probed about why they use it nevertheless, participants cited convenience, circumstances, staying in touch with friends, or being kept up to date with the latest updates from university, which are often published in Facebook groups. A participant from group 5 complained he had to create his Facebook after he did not receive information about a lecture being cancelled and came to university in vain.

Twitter

It should first be established that twitter is not a very popular social medium in Slovakia, whether among the general population or among politicians. This was probably one of the reasons why a few people in each group immediately associated twitter with 'Trump' and his tweets—perhaps prompted by the previous discussion about microtargeting and data leaks might have been used to fuel Trump's voter databases. Some mentioned the characteristic length of characters that defines tweets, others mentioned the blue bird icon. Several participants admitted to never having been users of twitter, one participants branded the social medium as an 'American phenomenon', again, making their perception of the distinction of use apparent. One participant associated twitter with memes. When asked whether they heard that twitter banned political advertising in late 2019, none admitted to having heard it, although they commented on this positively, claiming, 'there are too many simpletons on social media' and that 'fake news is what I mind the most' in relation to the recent social media scandals.

Brexit

Following the discussions about the two social media most associated with political content, two political events now most notoriously discussed in terms of voter manipulation, election meddling and the deliberate spreading of misinformation based on social media user data were pulled out. The

test was to see whether participants would make a connection between these events and microtargeting as well as the social media discussed above. Brexit was described from the onset as a ‘mistake’, an ‘error’, and an ‘ongoing and never-ending saga that we will all pay for.’ (The focus groups were recorded before the UK ultimately began its process of leaving the EU in February 2020.) A participant from group 1 admitted to having heard about microtargeting being used in the British referendum campaign from the HBO documentary *The Uncivil War*, claiming it was awe-striking to see how data can be used to target people. Another participant responded to that comment by saying she is afraid of the potential this gives to fringe political parties, since ‘it’s easier to target hate’ and ‘polarization is always easier’. Names of prominent politicians connected to Brexit were dropped, including Nigel Farage, Theresa May and Boris Johnson. When prompted about whether Brexit is somehow related to data protection, a participant from group 2 wondered about whether Britain will have to introduce their own data protection laws, akin to EU’s GDPR, but elaborated the matter no further. Participants from group 4 saw Brexit as a financial loss for the EU that we will all pay for in the end. Overall, few people made the connection between Brexit and microtargeting; likely, it had not been mentioned enough yet.

Trump 2016

The positioning of this card after those with Facebook and twitter was meant to trigger the discussion about how social media were used by Trump’s team in his 2016 campaign. A participant from group 1 made this connection instantly, claiming the campaign had used data collected by data mining companies and this affected the results ‘considerably’. Another participant from the same group claimed this improved the campaign’s ‘leverage’, esp. when compared to Clinton’s 2016 campaign, giving Trump a ‘strategic advantage’ his opponent supposedly did not have. Others associated the phrase with ‘utter mistake’, an ‘incomprehensible’ twist of events, and recalled feeling sick the morning when the election results were made official in Europe. One participant recalled having been taught by a professor who went to protest the election results in Washington D.C., others mused about how and why the results of the election happened. As such, they clearly had their own associations (both serious and light-hearted) with the event, which suggested that it had been an important one to them—despite the geographical distance. To all, Trump 2016 was not a positive association, on the contrary. Some had a few pop culture references ready, such as South Park, while others were reminded of his campaign merchandise and claims, such as the red MAGA hat and ‘build the wall’ campaign slogan. In short, most participants did not make the immediate connection between the Trump 2016 campaign and microtargeting, instead, they reflected on their immediate impressions of Trump’s presidential victory and how that tipped the scales of the global political arena.

Fake news

Fake news, a phrase popularized by Donald Trump in the recent years, was used deliberately right after the Trump 2016 campaign. The immediate associations made were either ‘social media’, ‘Facebook’, or ‘Russia’, perhaps owing to Slovakia’s domestic political situation, and likely also to the Trump 2016 campaign that was notoriously accused of having been aided by Russian interference. Some participants gave examples of media they considered to be the spreaders of fake news, both English-speaking and Slovak. Two participants named Fox News, one ironically named CNN, then specified that they are fake news according to Trump. A participant from group 2 said the inclination to fake news was characteristic for Americans, because they ‘need the drama’ and want ‘something to believe in’. When prompted about whether data has something to do with fake news, several participants confirmed the connection, explaining that thanks to data, one can ‘target’ users with fake news made especially for their user cohort, while a participant from group 2 wondered about the role of one’s place of residence within the fake news cycle. According to her, if one lives in a secluded rural area, they have less opportunities to fact check news, while people residing in cities have access to more information and thus also higher chances of avoiding being fooled by fake news. This, according to her, contributes to the opinion gap between the urban and rural-dwelling citizens. Group 4 named whom they considered to be Slovak-specific spreaders of fake news, including far-right politician Kotleba, the social democratic ex-prime minister Fico and his party Smer, as well as their then-running campaign ‘Novy Smer’. Group 2 made the desired connection between fake news and elections, claiming you can ‘get to power thanks to fake news’, making an example of a claim in which the far-right LSNS party promised to shoot a thousand bears, which it would not have the power to do based on current hunting laws. And yet, if someone lives in a region where bears often come into the city and go through trash, they claimed, this might convince them.

Alternative media

Fake news, defined as misinformation and disinformation spread deliberately to skew public opinion in order to achieve or contribute to a political outcome, often appear in so-called alternative media, who exist in contrast to traditional or established mainstream media. They often lack the structures and characteristics of traditional media but nevertheless position themselves as their direct competitors, who, unlike traditional or mainstream media, spread the ‘real truth’. Some participants in several groups did not know what alternative media meant, asking for further definitions or examples from others, which their fellow participants usually provided, others easily provided a version of the definition cited above. When prompted with the names of famous

alternative media, some participants added more input, such as ‘we don’t really know what’s true anyway. Some media say this and some say that, and I guess everyone has to make up their own mind.’ Some defined the phrase ‘alternative media’ as a ‘buzzword’, others branded them as ‘conspirational media’, while some claimed it’s an issue of ‘self-branding’ by the media in question, elaborating this explanation as follows: ‘...in the sense that there are mainstream media (.) that push a certain agenda and then there are alternative media who show everyone the ‘real truth’.’ The rest of participants oscillated between naming who they considered alternative media and ironically naming mainstream media, which are viewed as conspirational pieces by people who read alternative media. In the Slovak context, several prominent alternative media were name-dropped repeatedly, i.e. Zem a Vek, Infovojna, Kulturblog, and an up-and-coming right-wing teenage commentator (Livia Garcalova from Kulturblog) was named as well, while her name was always met with expressive and distasteful reactions; a Marxist pro-Russian Slovak politician famous for his controversial Facebook statuses (Lubos Blaha) was also named repetitively. One participant admitted to have written their thesis on the topic of Russian disinformation in Slovakia and explained the divide-and-conquer character of misinformation spread by Russian bots and trolls whose primary aim is supposedly to destabilize the belief in any renowned source and to spread a sense of ‘chaos and uncertainty’, ‘mistrust and questioning’ in the general population, because in a ‘world where no information can be definitely right, any information can be wrong, so any of their information can be as true as anything else’. ‘Alternative truth’ was a phrase that appeared often in the transcripts.

Cambridge Analytica / Aggregate IQ

While Cambridge Analytica was recognized by many participants (due to also having been discussed previously, which led to mostly affirmative definitions, such as ‘what we discussed before’), Aggregate IQ was not recognized by any of the participants—which is why these two associations were grouped into one during the transcribing and analysis part. The only case when participants displayed a degree of recognition was either when Brexit was mentioned (group 1), or when the parallel between Cambridge Analytica was established (group 4). Speaking of Cambridge Analytica, those who recognized it said it and the scandal related to it was the ‘trigger for this discussion’ about privacy, which was a ‘good thing’. Some identified it as a ‘data mining’ or ‘big data’ company, ‘an incredible analytical company’. Others said they have heard of it but do not know what it is exactly. Two participants offered closer explanations. The first one from group 1 said they have ‘500 points on every single person in America’, which was not entirely accurate (in fact, it was 5000+ data points on 2500 Facebook users that allowed them to form a relatively accurate picture on the general US population), while another participant from group 4 explained

that they bought data points from Facebook and compiled these for Trump's 2016 campaign, while suspicion about their involvement in other political events also existed—such as a coupe in Kenya, the civil war in Venezuela, and others. Other participants from group 4 asked whether this is verified information or conspiracy theories—the response was that it is 'SUSPECTED'. Most of the knowledge participants had about the two companies came from the recent Facebook data privacy scandals, or popular culture productions about the issue, such as the Netflix documentary *The Great Hack*, which focused on Cambridge Analytica's multilevel activities, or the HBO documentary *The Uncivil War* that scrutinized the role of data in the 2016 British referendum campaign from the perspective of Dominic Cummings, the Leave campaign's chief.

Russian interference

Russian interference was often cited as one of the intrusive election interferences involved in the 2016 US presidential election, and successively became the subject of a years-long investigation. Although nothing substantial came out of it thus far, Russian support of right-wing politics within Europe and North America is a long-reported issue. The participant whose dissertation thesis focused on the Russian misinformation within Slovakia explained that according to his findings, Russian influence usually focuses on social divides and spreading misinformation through social media, and that this practice has a long tradition that predates social media as a communication channel, and is now related to a larger phenomenon called the hybrid wars, which came to be as a result of Russia not being able to win actual wars. Hybrid wars do not require physical violence, but can be fought online and divide a population from within. Another Russian interference technique, cited by the same participant, was *kompromat*—a method in which compromising information on a person is used to either blackmail them or for character assassination, while the information usually consists of a combination of true and fabricated facts, making it particularly difficult to tell truth from lies; and how the Russian media machinery, connected to politics, works as one to establish an arena where nothing is true or verifiable.

Other participants said that while this phrase most reminds them of the 2016 US presidential election, it is a phenomenon that extends beyond it, explaining it as Russia interfering with foreign politics to contribute to a result that favors their international position or their strategic business ambitions, such as building oil pipelines in Europe (Nordstream was mentioned in two focus groups independently). Another participants from group 5 said he felt that at some point, it felt like Russia was being used as a 'scapegoat' for every problem within the Western World and that this, to such degree, seemed unfair to him. Others were careful to phrase the issue in legally acceptable terms, i.e. '...there exist indirect suspicions (.) that such influences come from the territory of the (.)

Russian Federation but nothing can be absolutely attested for in the sense that it's true.' The names of pro-Russian politicians were dropped, such as the Czech president, Milos Zeman. One participant says that if the Russians were to influence an elections, they would have understandably employed data mining in order to target their content. Other strategically viable regions for Russian intervention were named by a participant from Group 2—Turkey, and the Middle East, which she attributed to their interest in local oil reserves. Overall, participants were aware of the techniques and strategic territorial goals of the suspected Russian interference in international politics and made the connection between influencing foreign politics and microtargeting.

GDPR

As a part of this association, participants were reminded that they signed a consent form prior to their participation that listed the rights they have as EU citizens under the directive. Still, very few knew about their rights, even after having (supposedly) read them less than an hour ago. This was meant as an exemplifying lesson of how easily consent forms are overlooked. Out of those who knew about GDPR before, they listed the following rights: the right to be forgotten (cited most often), control of one's data (not specified more closely), right to data erasure, right to obtain one's own data, having more oversight on how data are stored, having one's data protected. 'Necessary evil', 'a misunderstood law', and 'nuisance' were mentioned several times in relation to the GDPR. Some participants were already active professionally next to their studies and experienced the preparations for GDPR either while working for companies that had to incorporate GDPR into their internal data policies, or legal companies that helped other companies make the transition. As such, those who were familiar with the details claimed it was for a good cause but carried out in a very lengthy and mundane manner. Some claimed that 'nothing has changed except all this added bureaucracy', 'there was all this drama about it and now nothing changed', or 'even if we read disclaimers, they're written in a way that no one understands'. Others claimed to have read the GDPR when it came out but could not cite the details anymore. One participant appreciated the fact that GDPR thematized the topic of data protection to a degree that is productive; another from group 1 appreciated that he was now being able to see who uses his data and what for; a participant from group 2 said she was now able to delete her data from social media, which she had tried several years ago without success.

Another from group 5 caused a stir when they said they were able to access recordings made by their phone without their consent by google and stored online. He was able to delete these and turn off the setting for the future after GDPR came into force. Most others were shocked at hearing this. Another participant from group 1 showed clear confused when trying to explain data protection

under GDPR, claiming that it works on one hand, in that she restricts her data use on some websites, but simultaneously, her data are being provided without her consent to third parties by those very parties, and she used the example of Cambridge Analytica to prove this point. It was interesting to see that even law students struggled to understand the purpose of the directive and its effect on the society at large, even being at a loss to remember what the directive entailed. It seemed that either their university paid the introduction of the directive no special attention or the students failed to remember it. One such student joked that she was ‘absent’ when it was being explained. Participants from group 4, who worked next to their studies, complained about the lack of transparency and guidance from the EU when implementing the directive, esp. when a business had cameras that recorded customers and visitors; while they were not able to agree how high the fine for non-compliance was. A participant from group 1 said he also had to implement GDPR on his websites as a freelance graphic designer but that he believes it is up to the individual to keep a watch over their data and does not feel the EU is able to do much there. A participant from group 3 complained that the option to opt-out of data collection should be made easier and more visible on websites than it is today.

Overall, the intent of the directive was evaluated positively and as a good first step, but other than that, participants either lacked substantial knowledge about it to make informed statements, or expressed their grievances with the amount of bureaucracy and paperwork that it took to implement it, without any meaningful results or changes—however, they did admit that it was too soon to tell whether the directive was a good step or not.

Elections

While all participants agreed about the important nature of elections, they cited corruption as one of the first associations with elections. Others cited a ‘fragile institution that upholds democracy’, ‘voting for a lesser evil’, a ‘civil duty’, a ‘presentation of public opinion’, an ‘illusion of free will’; or the numerous themes of the electoral campaign that had been taking place at the time—including prominent slogans, parties, claims, etc. A participant from group 1 elaborated their cynical stance to elections by saying that ‘on one hand they are amazing because they have this amazing potential but on the other they’re incredibly frustrating because they never fulfil this potential [...] and in Slovakia (.) as well as in other (.) countries, very often I don’t believe people are informed enough to know what they are actually voting for.’ Others responded jokingly to this by saying that IQ should be measured as a prerequisite to allowing people to vote. Participants from group 4 talked about the ‘illusion of choice’ and saying ‘it’s beautiful to have this illusion of choice but must people are so dumb that [elections] don’t have such a huge effect.’ / ‘It’s like Christmas, it’s once

per year, or once per four, and it keeps you happy for the rest ((laugh))’ / ‘Yes, it’s something you dream about, and then comes the disappointment’ was the response. A participant from group 2 cited Slovakia’s current president’s presidential campaign and how her sudden jump in popularity in the polls ‘must have had something to do with the advertising and collecting data’ back in 2019. Few made the connection with microtargeting at this point.

Democracy

The last association brought the discussion back to where it had all started—a concern for democracy. Before embarking on the next section dedicated to democracy and microtargeting, this association was meant to prime participants into defining democracy and its most important pillars. Many participants displayed signs of cynicism. Churchill was quotes numerously as someone who had said that democracy had its flaws, which became apparent as soon as one talked to a regular citizen, but that it is simultaneously the best system that there currently is. Most other responses could be included under such umbrella category. Furthermore: ‘the only system that has the principle of self-destruction in-built’, ‘populism’, ‘imperfect system, but we don’t have anything better’, etc. Participants from group 4 criticized the corruption potential that allows politicians to bribe ‘stupid’ people by as little as ‘cigarettes given out in front of the local town hall’, and pointed out how self-destructive democracy can be on the example of Viktor Orban, who won elections repeatedly and then changed the rules of voting (district borders) in a way that ‘cemented him in power.’ They also discussed whether it is better to have a system like the US’s electoral college or a European-type majority vote. A participant in group 2 made the connection to microtargeting by claiming that under democracy, one should not be penalized for what they post or publish under their freedom of speech, and it should not be used against them. When discussing the ameliorations for democracies, one participants debated the idea of inventing a system of achievements that would grant one the right to vote (i.e. paying taxes, contributing to the society, being reasonably intelligent) but simultaneously added that such a system of exclusions can backfire easily and is flawed by default.

6.5.7 Democracy and microtargeting

Based on the previous discussion, the first question related to microtargeting and democracy was whether participants believed microtargeting could have an influence on democracy, and in what way. They univocally agreed that it can, but in different ways. Some said they believed it has already happened. An example for this happening, as cited by participants in group 3, was when after the 2018 murder of investigative journalist Ján Kuciak, anti-government protests were organized on facebook, and eventually forced the prime minister, interior minister and chief of

police to resign and started a momentum that gradually led to a political change in Slovakia. Another argument claimed that if one is targeted with one piece of information (paid by the highest bidder or one most-skilled on social media), it can skew one's opinion and thus who they vote for. Spreading fake news can therefore contribute to electoral results that would not have otherwise happened. When discussing what this means for democracy, participants from group 5 claimed that 'it's one thing if I am targeted for a t-shirt, I can decide that I don't want to buy it, but a vote is something else' because 'it gives politicians and political parties the power to abuse it', 'especially extremist parties'. A participant from group 1 believed that stopping someone from spreading information on social media would be limiting free speech, but another contested this by claiming that 'stopping an ad from being on TV is one thing but being targeted to ONE SPECIFIC person because YOU searched for something is something else' and debated whether this could still be considered free speech. The author of the initial remark rebutted by saying a person is responsible for being influenced as such, if they choose to consume information presented to them uncritically. Another participant argued whether anyone has enough information to counter the targeting processes—which is an argument that resonated throughout several focus groups, including a call for better education in the area, which came from group 2. 'The simpletons are the easiest to influence.' In several groups the argument was made that 'simple' people who get all their information about democracy from the media are the most vulnerable because they 'are not able to form an opinion on their own'. When prompted about what democracy meant to them, several interesting responses were recorded. 'Democracy is a feeling you have', and 'some people think democracy means you can put anything out there, say anything, but then data mining companies abuse this and no one should be punished [targeted] just for putting something out there'.

Whether or not microtargeting has the power to change the form of democracy was a contested factor in most groups, but several people made the argument that false information spread on social media may get a party or a person elected who might push for changes that will eventually lead to authoritarian changes, citing the far-right candidate Marian Kotleba as an example, since he supposedly often uses democracy to defend his far-right claims. 'If we take the example of the US [...] it's definitely these people with inclinations to the far-right, so let's say they vote for Kotleba or Harabin or SHO [...] and if Kotleba joins some coalition then he can absolutely go after the RTVS (public news station) for broadcasting a show about the holocaust.' A participant from the same group countered—'it may change who you vote for but microtargeting won't change much about the JUDICIAL system and the fact that Fico (prime minister) and Kocner (businessman accused of financial crimes and assassination of a journalist) go for coffee together.'

6.5.7 Elections 2020

After it was established in most groups that microtargeting may be able to change or affect democracy and even, in some cases, our understanding of it, the discussion was directed towards a specific example—the then upcoming 2020 parliamentary election. The first question was whether the participants already knew who they would be voting for—without naming their preferred candidate or party, if they felt uncomfortable revealing the information. Most either said no, or that they are deciding between two parties (while, as participant from group 1 commented ‘and I think we all know which two these are’ to the others’ amusement).

The second question was how participants arrive at their decision on who to vote for. Most said they either look at the parts of party programs relevant to them (i.e. a medical student focused on the proposed medical reforms), by the public media discussions that precede elections (‘seeing how they present themselves and how they debate’), or by the principles that the preferred party aligns with (i.e. environment, judicial reforms, being pro-LGBT), or by voting *against* someone (i.e. corruption / ‘fascists’). Members of group 4 claimed they use the method of exclusion when choosing their party.

Thirdly, participants were asked where they mostly see the advertisements for their preferred candidates and parties. The most common answers were social media, esp. facebook, Instagram and Youtube, billboards on the street and TV. A participant from group 5 said he deliberately ignores political marketing by muting it when it appears before a Youtube video, then dislikes it, and is proactive by looking up information about political parties and candidates on his own. Another member from the same group joined him by saying he uses an ad block to tune out such advertising. Participants from group 1 expressed their frustration about the fact that, in their opinion, the people most susceptible to online advertising delivered based on microtargeting, are the people who they wish wouldn’t vote at all. A participant said that ‘out of practical reasons, I would like it if [political microtargeting] wasn’t allowed at all, and for the same reasons, I would want the party I like to win, yeh. But (.) when it comes to democratic principles, then (.) the responsibility to vote for those that we want to vote for, and not (.) for those that we allow to manipulate us, has to be left up to those who vote, and not up to the state.’

6.5.8 Change of heart ex-post

Most participants did not claim that anything changed for them following our discussion. Of those few who did, they vowed to pay more attention to what they post online because ‘everything stays on the internet and [they] can (.) easily find it’, others said they learned about new terms (i.e.

adblock, VPN, cookies), another participant said she will go and read ‘an article’ about how to protect herself better online, since she claimed she knew nothing about microtargeting prior to participating and had never even heard the term before. Others said they did not feel so affected by microtargeting that they would have a need to do something about it. One participant from group 3 and another from group 1 said they learned a bit more about GDPR, vowing that they will pay more attention to whom they offer their data to (i.e. to what company, which they can read up in the updated terms and conditions of use under GDPR). A participant from group 2 said she believes no matter what she does, if someone wishes to access her data, they will, which she does not mind about as long as it is used for providing her with content she is interested in; and so it makes little sense to be proactive about data protection.

VII. Conclusion

After coding and analyzing all focus group transcripts, and seeing no further need to create additional categories or subcategories, all categories were analyzed, conclusion from the respective categories were made; and a general conclusion of all categories was observed.

Overall, it should be noted that nearly all participants possessed at least a basic understanding of microtargeting (if not under that name) and displayed some knowledge on data protection practices, even if these were evaluated as basic or naive by other group members. The awareness of both microtargeting and data protection measures varied across participants and groups, from largely ignorant to informed to the degree that they could practically cite the findings of investigations into the matters related to data breaches and microtargeting being used for political purposes. Those who were more advanced in their awareness of data protection measures were usually also more advanced in general technological proficiency, which was often related to their choice of profession or university degree; while those who were more aware of microtargeting techniques and the scandals related to it were also more aware of the political scene and world events. On the other hand, those who were less aware excused themselves by saying they read the news less or by saying they focus on their demanding studies in a field that is not connected to politics or public affairs (such as medicine or plant biology).

Nevertheless, only a few participants made the spontaneous connection between microtargeting and political targeting (unless prompted) in the very beginning of the discussion, and, more importantly, it seemed that only a few of them worried about democratic processes and how they could be impaired by microtargeting as a result, lending credibility to the conviction that they did not think much of the issue beforehand. When asked about this specifically, they admitted that microtargeting has the potential of meddling with politics and democratic processes, but offered no initiative to counter this reality besides their individual dispositions to staying informed and being precautionous. But to be precise, no participant was entirely comfortable with or approving of microtargeting being used to potentially deceive voters with half-truths and purposeful disinformation, yet they often believed themselves to be exempt from these strategies, owing to their intellect and experience (which, ironically, turned lacking in several aspects). Although participants were not inherently trusting towards democratic processes, instead displaying a fair amount of cynicism and disillusionment about both elections and democracy, they did not seem to believe that microtargeting would have a profound effect on democracy itself, only, possibly, on the results of

democratic elections (as any other marketing strategy), which could then affect the form of democracy, if, for instance, an anti-democratic candidate got into power and had their way with the system (like Viktor Orban in Hungary, as they explained). Their trust in the processes, as well as in democracy itself, did not seem altered as a result of this knowledge—perhaps because it was already lacking (at least in their national context—they were unhappy with democracy in Slovakia, not necessarily with democracy itself).

Interestingly, when viewing microtargeting as a threat, participants viewed it as a threat to them specifically, and viewed themselves as those that can lose the most to it as a result. They assumed that microtargeting is very useful for political marketers who aim their content at undecided voters and those who have an inclination to support fringe-groups (but also presented how a moderate person can be persuaded to support the more extreme via microtargeting when the option to support the moderate is obscured). In other words, groups they define themselves in opposition to (and, as also stated, *vote* in opposition to), and groups they see as inherently harmful to the political system (i.e. more than just a different opinion streak) and to the country. Some were even able to perceive and admit this bias, admitting that they would prefer if their chosen party or candidate would win, but simultaneously admitted they would not meddle with the democratic processes—despite proving to be cynical towards democracy and its processes on a whole. Their self-proclaimed words—democracy is the only system with its self-destruction in-built—thus resonated with their own beliefs and moral codes.

From a less political point of view, participants admired the ingenuity of microtargeting as a marketing tool and a business tool; often benevolently understanding of why marketers employ it in their market research and market targeting activities. As such, they did not seem flustered or alarmed by microtargeting, rather accepting it as something that is largely inevitable with our internet usage and with the pace at which marketing uses our data, but can be curbed to some extent with conscious behavior patterns. When it came to discussing their conscious behavior patterns, however, most admitted that they accept their own portion of the blame in their data being used for targeting, due to the fact that they still choose to use the services and social media that collect their data (Facebook and the other companies it owns came up much more often than twitter, which is an obsolete medium in Slovakia), and due to the fact that they do not read terms and conditions of use (not even those in the informed consent provided before the focus group). While there was some confusion as to what data mining companies can and cannot do with respect to their data and its collection, all participants agreed on the multiple advantages of being microtargeted based on their preferences and claimed that to some extent, this was convenient for them. Based on experience,

several participants were able to piece together a comprehensible understanding of data targeting, coming up with specific examples of both how and why their data could have been used to fuel specific campaigns that they saw appear in their feed. They also offered a few suggestions on the positive ways that marketing could be used in—such as education and the strengthening of democracy.

When it came to data protection, the degree to which participants were willing to dedicate time and effort to proceed with caution on the internet differed greatly. Some did close to nothing, others had various softwares installed and practiced what others saw as an overabundance of caution with regards to their social media use (i.e. logging out of Facebook, not using it together with other services). Most participants had lacking knowledge on how to effectively protect their data and showed little motivation to learn more due to the belief that anyone who wished to access their data could do so anyway—preventative measures were not popular with this sort. Although several participants were shocked and surprised at what they found out (i.e. Google storing voice recordings it made randomly), and vowed to pay more attention their internet practices, it is questionable to what extent their declarations made in the focus group mirror reality outside of it.

When prompted, many participants agreed that microtargeting should not be employed in political advertising the same way it is employed in the propagation or sales of consumer goods or services, and were able to outline both ethical and legal concerns about this being so—from subjective feelings (i.e. feeling uncomfortable) to complex moral arguments (free speech and autonomous self-deliberation vs. protecting the greater good). Nearly all participants who were worried for the future of democratic processes simultaneously expressed that this is because it is the parties they least align with (for reasons of populism and being on the opposite site of the political spectrum) that they believe can benefit most from microtargeting, thus the bias of their cohort (liberal, progressive-thinking city-dwelling young people with an ongoing university education) showed.

As for the choice of research method, focus groups and the group-discussion format proved useful in how they influenced the group dynamics and encouraged exchange of information and practical knowledge. Overall, it was pleasant to see how participants enlightened one another on their own experiences as well as educating one another on what different things mean (cookies, tracker, microtargeting) and gave one another tips how to avoid or minimize being targeted (ad blocker, browsers that do not sell data to third parties, etc.). The research format allowed participants to interact with one another spontaneously and naturally, without being prompted or nudged, save for the initial prompt and the questions they were given. Once started, they were able to keep up the

conversation on their own and did not rely much on my guidance or symbolic conversational encouragement (nods, hums, etc.).

VIII. Discussion

This master thesis research was prompted by a need for a broader, informative and inclusive debate about microtargeting, data protection and the experience that microtargeting leaves people with, particularly with regards to some of the most important tenants of liberal democratic societies—democratic rule, liberalism, personal freedoms, autonomy, and free thought. The meditation on this topic was prompted by real-world events, including the benevolent data operations social media giants like Facebook were accused of together with other big data companies and data mining entities such as Cambridge Analytica; as well as popular culture pieces that enlightened the everyday observer on the functionings of political campaigns and other operations based on dynamic, real time, personalized and shockingly accurate data collection. Paired with the pressing importance of such questions in the light of the then-approaching general election in Slovakia that a lot of hope and expectations were placed into, following the murder of investigative journalist Jan Kuciak and the massive anti-government protests that followed it, the general mood foretold a monumental opportunity to observe a relatively novel phenomenon in a rather unexplored population. Thus, the idea to observe how microtargeting affects people's view of democratic events was conceived.

The choice of region was natural to me—I know most about my compatriots as well as about my country, which might on one hand put me in a position of quick conclusions and on the other, allow me to forget that I myself am only cognisant of a very particular subgroup of my nation. Nevertheless, Slovakia and the CEE region in general present a very interesting phenomenon, in that they are both not explored enough and very different from the rest of the Western world, an opportunity I set out to explore with as much scientific objectivity as was possible. Several events have made it apparent within Slovakia what potential social media has to mobilize, and to what extent young adults are willing to mobilize themselves for political purposes. As such, it became especially interesting to observe today's tech-savvy young Slovaks in how they approach and deal with the challenges of the modern digital world that shape their democratic functioning.

Five focus groups with 19 participants were successfully organized and carried out. All had a slightly different set-up and thus always illuminated a new portion of the society, but all were conducted strictly according to the established protocol in a need to maintain and uphold the trustworthiness of the chosen method. For the same reason, the choice of codes and justification of their order and how certain excerpts were added to the codes are discussed at length in both the Method and the Results section.

The focus groups shed a lot of light on the participants themselves, the group dynamics of each group, as well as, most importantly, the issues that were being discussed. The format of the focus groups probed most intensely into questions related to microtargeting and data security, asking participants about their awareness of both topics, their own experiences and practices with microtargeting and their own data protection, and used different association activities to explore the depth of their knowledge on the main two topics as well as relevant related topics—from social media companies, world events, to democratic principles. The associations were also meant to examine to what extent participants take an interest in political topics or events that shape the public discourse, and to what extent they follow the news. Participants varied in every other aspect than those they were chosen for—from their choice of university degrees and professions to their degree of awareness of events, to the gender dynamics, to personal characteristics, such as shyness, expressiveness, or the inclination to observe and debate others—whether as partners or as competitors.

To answer the main research question, microtargeting did not seem to have a profound positive or negative effect on these young people's trust in democracy as seen in these focus groups; if only it confirmed their already cynical views about how easily corruptible and vulnerable democracy and its institutions can be to corrupt power-hungry politicians, marketing strategists, political campaigners and high bidders. According to a poll performed in Slovakia, people with a higher degree of education tend to view democracy in a more favorable light. (GLOBSEC, 2020) While this thesis did not make comparisons between different levels of education, as all participants were university educated, when one views education in a broader sense (informing oneself about current events), the more informed and less ignorant of the groups (those who knew more about current events and responded to questions more readily) viewed democracy somewhat cynically, but were assured in the conviction that it was the best practice and said this explicitly. Those with lower levels of informedness about current events only displayed distaste, but without the redeeming inclinations. With regards to the Slovak parliamentary election that was about to take place, participants were certain that microtargeting techniques were being used, and in part attested to this being so based on their own exposure to targeted ads and justification on why they were chosen for these; and believed the prevalence of microtargeting would only increase in use in the upcoming years. Nevertheless, this did not seem to disturb them too much, only to reaffirm an already existing conviction.

To answer the sub-questions, microtargeting did not seem to lead to an increased sensation of being surveilled, as that sensation was already present among most the participants under the awareness of data collection; and although some vowed to change their behavior patterns based on the novel

information they received during the discussion, it is questionable whether all and any reactions shown within the focus groups could have outlived them and been translated to any changes in behavior. Furthermore, the participants' distaste for political microtargeting did not seem to affect their own actions, merely, it made them feel threatened in their political climate (they believed it gave power to those they did not want more power going to). Although many were practicing safety precautions with regards to data collection already, nearly all participants admitted that it was impossible to not be targeted, and one had to at best learn how to live with it and to make microtargeting work for them, instead of against them. Not much was added to the existing discussion about political autonomy; while participants felt uncomfortable by being targeted in matters of democratic affairs, they did not see themselves as the 'vulnerable' sort who can be seriously affected by microtargeting techniques. Whether an illusion or reality, this seemed to serve as a self-defense mechanism against most negative implications of data collection and targeting. And yet, despite some of the undeniably negative views and implications of microtargeting that were being discussed in connection to social media collecting their data, participants claimed they use the services nevertheless, because, in their own words, the benefits outweigh the risks. Benefits included staying in touch with friends or staying up to date with information from the university. This finding is in line with the privacy calculus model. (Trepte et al., 2017)

Existing research on microtargeting suggests that young people are the ones least bothered by microtargeting out of the whole population. (Dobber et al., 2018) While, again, this thesis cannot compare different demographics, it can attest that of those participants who were questioned, none seemed too flustered by the fact that microtargeting exists, they only had objections against certain uses of it; accepting it as a part of the deal that modern life and technology entails. Furthermore, research also suggests that those more familiar with the topic have more favorable views towards microtargeting. (Dobber et al., 2018) This seemed to be a trend—the more participants knew prior to joining the focus groups, the less they seemed bothered by what was discussed, at times nearly stoic. It was usually those who were presented with information novel to them that seemed most disturbed by it, and showed the highest willingness to change their habits as a result. But nearly all of those who felt uncomfortable with microtargeting being used to influence public opinion were motivated to think so based on their own political bias and perception of voters of far-right or populist parties. As such, the bias of the groups that had been defined for the research (university students living in the capital) became obvious not only in their understanding of microtargeting (in their words, a tool the populist and far-right parties can most benefit from) but also on their view of the world. They saw themselves as personally at risk, and yet powerless in the face of democracy—unless a tighter regulation of microtargeting for political content is established, an aim they seemed

to share across groups. In any case, despite often being informed and curious, participants did not offer any suggestions for functional solutions to the current challenges and problems related to microtargeting and data safety (not that they were expected to). In their own words, all such ideas for solutions only highlighted what a ‘cyclical problem’ microtargeting is and how measures intended to protect from it might only exacerbate its effects in the end.

Data protection was a salient topic for everyone, albeit to different degrees and levels of knowledge. Although participants claimed they would prefer less of data being collected, they also realized that for full functionality of online services, and with the way the society and technology is set up these days, such expectation is not realistic; instead opting to at least having their data anonymized and sold in bundles that would not be traced back to them. Anonymity and unlinkability, two very prominent terms related to digital privacy discussed in both the Introduction and Theory section (Torra, 2017), resonated throughout the focus groups. Participants repetitively said they would not mind microtargeting per se (with moderate objections to political microtargeting), if their data could not be traced back to them and if instead it was either completely anonymous (available under a disassociated number) or available in bundles. When prompted on why, most could not give a specific reasoning, only that they felt uncomfortable when they were traceable or linkable to data. In a similar manner consistent with previous findings (Esrock & Ferre, 1999), participants felt more uncomfortable with their data being sold to third parties than with the sole fact that it was being collected on them by social media. However, this did not mean that they trusted social media (they did not), only perhaps that they trusted third parties even less.

The specifics of the geographical location of research showed up as an influencing factor as well. Consistent with existing knowledge about Eastern Europeans and their view of democracy (Krastev & Holmes, 2019), participants displayed cynicism and a lack of trust towards democracy, but not necessarily to the institution as a whole, rather, towards the way it was being carried out by their government. Nearly all participants that voiced an opinion on democracy simultaneously expressed that they did not believe any other system was preferable. And although 38% of Slovaks would prefer a strong leader that could bypass a parliament (GLOBSEC, 2020), this did not resonate as a sentiment among the group at all. Further specifics of their nationality were perhaps the deeper knowledge of topics such as Russian intervention, as discussed by one participant; or the fact that Russian interference was often their top-of-mind association with fake news and political microtargeting. Slovakia is naturally more interconnected with Russian politics—both historically and contemporarily than many Western countries.

Demographic factors such as gender and choice of professional or academic field further also played a role in the degree of knowledge participants displayed, with men being generally more articulate on their practices of data protection (whether they actually knew more is uncertain, since group dynamics could have also played a role in the willingness to openly discuss a topic that is viewed more ‘technical’ and IT-related, and thus more stereotypically ‘male’), while being active in a study or job field close to what the focus group was about served as a good predictor of knowledge related to it—perhaps an obvious fact, but nevertheless worth pointing out. Existing studies also suggest that women view microtargeting less favorably (Dobber et al., 2018), however, this is not a finding this thesis could either support or reject; yet, women in general seemed less aware on details of microtargeting, which as a result made them less favorable towards it (but I believe the lack of knowledge plays a key role here, not gender; gender could serve as an indirect moderator variable). Participants from fields that circled around computer science, politics, international relations and security (mostly men) were more articulate and what they expressed had more nuance. When it comes to group dynamics, no apparent prejudices between group members with regards to gender or other demographic factors came up. Overall, the atmosphere of the focus groups was relaxed, participants were able to joke and laugh with one another, heard each other out, did not interrupt one another too much and were willing to consider the others’ point of view, at least on the surface. Due to what seemed like good listening skills and open-mindedness (though perhaps caused by the fact that they were so similar to one another in key aspects), participants were willing to explore serious topics in depth, not even shielding from expressing controversial opinions and readily willing to display their knowledge in front of others (though some needed to be gently encouraged).

While no all-encompassing conclusions can be made based on this thesis about the state of democracy in the light of microtargeting today, this is at least a first endeavour into the minds of educated young adults who mostly keep themselves informed on world events and are both able and willing to explore their own ideas as well as the general narrative on fundamentally important topics, such as democracy and the exercise of autonomy in the digital age. Several of the findings are consistent with existing research, while other findings were quite novel. This only further proves the need for more research into the topic.

8.1 Limitations

There were some more and less obvious limitations to the focus groups that were observed during the process of leading the focus groups as well as in transcribing the recordings. First of all, not as

many focus groups were conducted as was planned or as would be ideal. Due to conflicts in scheduling of all involved parties as well as organizational issues, a sixth focus group unfortunately did not take place in the end of January although it was in the plans and participants were being recruited for it through social media. One more focus group would have been ideal, but of course, more would have also been valuable (if perhaps a bit outside the scope of a single-researcher student thesis). Secondly, all focus groups were supposed to have at least 5-6 participants for enough variety of opinion and a lively discussion. Unfortunately, unpredictable circumstances led many participants to cancel their participation at the very last minute, often failing to show up when they promised to do so only a few hours before. This led to some focus groups only having 3 participants. This disadvantage was felt especially in focus group 2, where participants knew least about the topic of microtargeting and data safety—which is not alone a problem to be attributed to the numbers, but perhaps to how similar the participants were typologically, as a more varied sample failed to turn up. In future projects, this should be covered for by ‘spare’ participants, or by overbooking groups with more participants than intended to avoid a lack of participation—as more participants than intended could still be a fruitful condition, in contrast to too few participants.

Furthermore, another limitation to the study was the political and opinion bias. The bias of all target groups could be seen as both illuminating of their specific demographic on one hand, and as limiting on the other. Perhaps it was the louder ones who shut out the quieter (and dissenting in terms of views) ones, which alone would be an acceptable group dynamic that could reflect real life, however, at times, I noticed there was an opinion homogeneity that could be seen as detrimental to the general discussion (but does not need to be interpreted as such). Perhaps in future research, a more varied sample should be drawn to include participants from other political camps. Since I relied on social media and friend groups to spread the news, this served as a limiting factor to the heterogeneity of opinions and political views. A broader means of recruitment should be employed in the future to avoid this issue. Another issue related to the fact that many participants knew each other from outside the focus group was the loose atmosphere of some groups. Although this on one hand contributed to an attitude more willing to disclose and discuss on even controversial topics (hence the natural environment in which participants thrived), perhaps it was not the most professional setting that a focus group conducted professionally should be. With the limitations of a student work in mind, though, this is likely the less grave of limitations.

While I do not believe that another qualitative method would be as fruitful as a group discussion, for deeper analysis, individual interviews could be organized (however, these could prove difficult if participants knew nothing of the topic—hence the focus groups being preferable), and more

interactive activities could be included if more resources (and organizers) were available. Quantitative research, in my opinion, is still too early in this phase and would shut out too many nuances and subliminal factors that could have only been triggered in explorative conditions. More questions could be given on the topic of privacy as such. While this master thesis question the practices related to privacy online, perhaps more question about the participants' understanding of privacy and its multiple dimensions, as defined in the Theory section, would have also been thought-provoking and conducive to a better and broader discussion.

8.2 Suggestions for Future Research

Microtargeting, privacy, voter targeting and decisional autonomy in the age of personalized campaigns based on extremely precise data profiles, are all topics whose examination efforts will not be extinguished anytime soon. On the contrary, as more and more of our lives become subjected to data collection (smart devices and accessories, smart homes, AI cars, etc.) and optimization based on this data, the demand for more insights into the topic will surely only grow. It is therefore of essence to further explore the topic in any capacity, not just in regards to democracy and democratic processes; although, as was also supported by this master thesis, microtargeting can be seen as both a threat and a promise to democracy and the informational education related to it. This master thesis focused on a relatively small target group of people, and while their choice was deliberate and based on a theoretical framework, other groups should not be overlooked and should be examined in more detail. Young people, on the other hand, can be examined from different angles—i.e. with more focus on privacy, broader associations, and less so on democracy. Furthermore, adults, who find themselves between the digital dinosaurs and digital natives; older adults whose understanding of modern technology is limited on average, and who might be all the more vulnerable to microtargeting efforts, need to be researched as well on their understanding of privacy threats regarded to microtargeting, and their democratic decisional autonomy, since they still represent a very large portion society, a broad voter potential and a strong buying group. While Slovakia is a unique setting and should be examined more, other CEE countries (and not only those) are also of interest, as every national context leaves research at a very particular starting point, and every such context is worth a thoughtful exploration. And while the electoral period proved to be especially relevant to the topic, microtargeting and privacy could be examined under other monumental events, such as the Corona pandemic.

With the COVID-19 pandemic playing a huge role on our current lives, exploring the role of misinformation, fake news, conspiracy theories and foreign influences seeking to weaken the

stability of already fragile democratic countries is all the more relevant. Our privacy has been compromised for the benefit of public safety, and whether or not these measures will be reversible (whether for technical, practical or political reasons) is questionable. A world with even less digital privacy and even more surveillance, is always a challenging place for democracy, decisional autonomy and the free spreading of information to exist. All such factors should be kept in mind for the record of future research on data privacy and how citizens reconcile with the compromises they are forced to make for their safety and health.

IX. Bibliography

Books

- Alter, C. (2020) *The Ones We've Been Waiting for: How a New Generation of Leaders Will Transform America* (1st ed., pp. 197-198). New York: Penguin Random House LLC.
- Benn, S. (1971). Privacy, Freedom, and Respect for Persons. In R. Pennock & J. Chapman, *Privacy and Personality* (1st ed.). New York: Routledge.
- Calhoun, C. (2011). *Habermas and the Public Sphere* (2nd ed.). Cambridge, Mass: MIT Press.
- Flick, U. (2016). *Qualitative Sozialforschung: Einführung* (p. 128). Reinbeck bei Hamburg: Rowohlt.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (p. 105-117). Thousand Oaks, CA: Sage.
- Klingspor, V. (2016). In S. Michaelis, N. Piatkowski & M. Stolpe, *Solving Large Scale Learning Tasks* (1st ed., pp. 85-95). Switzerland: Springer.
- Kuckartz, Udo. 2018. Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung. Weinheim: Beltz Juventa. 4. Auflage.
- Maier, M., Marschall, J., & Stengel, K. (2010). *Nachrichtenwerttheorie* (2nd ed.). Baden-Baden: Nomos.
- Prinzen, K. (2018). Gruppendiskussionen und Fokusgruppeninterviews. In C. Wagemann, A. Goerres, &
- Przyborski, A., & Wohlrab-Sahr, M. (2014). Qualitative Sozialforschung: Ein Arbeitsbuch (4th ed.). München: Oldenbourg Verlag.
- Schoeman, F.D. (1992) Privacy and Social Freedom. Cambridge University Press, Cambridge.
- Torra, V. (2017). *Data Privacy: Foundations, New Developments and the Big Data Challenge* (1st ed.). Cham: Springer International Publishing AG.
- Trepte, S. (2012) In J. Schmidt, T. Weichert, *Datenschutz - Grundlagen, Entwicklungen und Kontroversen*, (1st ed., pp. 59–66). Bundeszentrale für politische Bildung.

Legal publications

- Council of Europe Press. (1995). *European Convention on Human Rights*. Strasbourg, France.
- European Union. (2018) *General Data Protection Regulation*. Brussels, Belgium.
- United Nations. (1948). *Universal Declaration of Human Rights*. Paris, France.

Journals

- Alhindi, W., Talha, M., & Sulong, G. (2012). The Role of Modern Technology in Arab Spring. *Archives Des Sciences*, 56(3), 101-112.
- Barbu-Banes, A. (2013). Microtargeting in Social Media: Definitions and Ethical Issues. *Studia Universitatis Babe-Bolyai*, (3), 83-90.

- 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*. doi: 10.1145/2389661.2389671
- Bennett, C. (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. doi: 10.1093/idpl/ipw021
- Bodó, B., Helberger, N., & de Vreese, C. (2017). Political micro-targeting: a Manchurian candidate or just a dark horse?. *Internet Policy Review*, 6(4), 1-13.
- Borgesius, F., Möller, J., Kruike-meier, S., Fathaigh, R., Irion, K., & Dobber, T. et al. (2019). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*, 14(1), 82-96. Retrieved from <https://www.ivir.nl/publicaties/download/UtrechtLawReview.pdf>
- Denham, E. (2018). *Democracy disrupted?* (pp. 3-57). London: Information Commissioner's Office. Retrieved from <https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf>
- Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2018). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. *New Media & Society*, 21(6), 1212-1231. doi: 10.1177/1461444818813372
- Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*. <https://doi.org/10.1177/2158244014522633>
- Endres, K., & Kelly, K. (2017). Does microtargeting matter? Campaign contact strategies and young voters. *Journal Of Elections, Public Opinion And Parties*, 28(1), 1-18. doi: 10.1080/17457289.2017.1378222
- Esrock, S. L., and Ferre, J. P. (1999). A dichotomy of privacy: personal and professional attitudes of marketers. *Bus. Soc. Rev.* 104, 107–120. doi: 10.1111/ 0045- 3609.00042
- Faizullabhoy, I., & Korolova, A. (2018). Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions. *Workshop On Technology And Consumer Protection*.
- Fox, A., & Royne, M. (2018). Private Information in a Social World: Assessing Consumers' Fear and Understanding of Social Media Privacy. *Journal Of Marketing Theory And Practice*, 26(1-2), 72-89. doi: 10.1080/10696679.2017.1389242
- Gil de Zúñiga, H., Weeks, B., & Ardèvol-Abreu, A. (2017). Effects of the News-Finds-Me Perception in Communication: Social Media Use Implications for News Seeking and Learning About Politics. *Journal Of Computer-Mediated Communication*, 22(3), 105-123. doi: 10.1111/jcc4.12185
- Hersh, E., & Schaffner, B. (2013). Targeted Campaign Appeals and the Value of Ambiguity. *The Journal Of Politics*, 75(2), 520-534. doi: 10.1017/s0022381613000182
- Isaak, J., & Hanna, M. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56-59. doi: 10.1109/mc.2018.3191268
- Kalla, J., & Broockman, D. (2017). The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments. *American Political Science Review*, 112(1), 148-166. doi: 10.1017/s0003055417000363

- Krasnova, H., Hildebrand, T., and Günther, O. (2009). "Investigating the value of privacy in online social networks: conjoint analysis," in *Proceedings of the Thirtieth International Conference on Information Systems, December 2009*, Phoenix, AZ, 173–191.
- Krastev, I., & Holmes, S. (2019). How liberalism became 'the god that failed' in eastern Europe. Retrieved 23 August 2020, from <https://www.theguardian.com/world/2019/oct/24/western-liberalism-failed-post-communist-eastern-europe>
- Kreiss, D. (2017). Micro-targeting, the quantified persuasion. *Internet Policy Review*, 6(4), 1-14. doi: 10.14763/2017.4.774
- Krotzek, L. (2019). Inside the Voter's Mind: The Effect of Psychometric Microtargeting on Feelings Toward and Propensity to Vote for a Candidate. *International Journal Of Communication*, (13), 3609–3629.
- Levy, S. (2008). Campaigns Get Personal. *Newsweek*, 151(17).
- Madsen, J., & Pilditch, T. (2018). A method for evaluating cognitively informed micro-targeted campaign strategies: An agent-based model proof of principle. *PLOS ONE*, 13(4). doi: 10.1371/journal.pone.0193909
- Mahmoodi, J., Čurdová, J., Henking, C., Kunz, M., Matić, K., Mohr, P., & Vovko, M. (2018). Internet Users' Valuation of Enhanced Data Protection on Social Media: Which Aspects of Privacy Are Worth the Most?. *Frontiers In Psychology*, 9. doi: 10.3389/fpsyg.2018.01516
- Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Informat. Sys. Res.* 15, 336–355. doi: 10.1287/isre.1040.0032
- Motta, M., & Fowler, E. (2016). The Content and Effect of Political Advertising in U.S. Campaigns. *Political Communication*. doi: 10.1093/acrefore/9780190228637.013.217
- Murray, G., & Scime, A. (2010). Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies. *Journal Of Political Marketing*, 9(3), 143-166. doi: 10.1080/15377857.2010.497732
- Noelle-Neumann, E. (1974). The Spiral of Silence a Theory of Public Opinion. *Journal Of Communication*, 24(2), 43-51. doi: 10.1111/j.1460-2466.1974.tb00367.
- Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *J. Consum. Affairs* 41, 100–126. doi: 10.1111/j.1745-6606.2006.00070.x
- Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. *Big Data & Society*, 5(2), 1-16. doi: 10.1177/2053951718811844
- Rubinstein, I. (2014). Voter Privacy in the Age of Big Data. *Wisconsin Law Review*, (5), 861-936.
- Rusch, T., Lee, I., Hornik, K., Jank, W., & Zeileis, A. (2012). Influencing Elections with Statistics: Targeting Voters with Logistic Regression Trees. *The Annals Of Applied Statistics*, 1(3), 1612-1639. doi: 10.2139/ssrn.2016956
- Summers, C., Smith, R., & Reczek, R. (2016). An Audience of One: Behaviorally Targeted Ads as Implied Social Labels. *Journal Of Consumer Research*, 43(1), 156-178. doi: 10.1093/jcr/ucw012
- Trepte, S., Reinecke, L., Ellison, N., Quiring, O., Yao, M., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, 3(1), 1-13. doi: 10.1177/2056305116688035

Ward, K. (2017). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal Of Media Ethics*, 33(3), 133-148. doi: 10.1080/23736992.2018.1477047

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal Of Consumer Affairs*, 43(3), 389-418. doi: 10.1111/j.1745-6606.2009.01146.x

Websites

As Democracy Wavers in Central Europe, Young People Consider Their Options. (2018). Retrieved 23 August 2020, from <https://www.ndi.org/our-stories/democracy-wavers-central-europe-young-people-consider-their-options>

Gehrerová, R. (2020). Ak by vo voľbách volili len mladí ľudia do 30 rokov, vyhral by Kotleba. Retrieved 4 February 2020, from <https://dennikn.sk/1667913/ak-by-vo-volbach-volili-len-mladi-ludia-do-30-rokov-vyhral-by-kotleba/>

Gizzi, D. (2018). The Ethics of Political Micro-targeting. Retrieved 1 November 2019, from <https://medium.com/datadriveninvestor/the-ethics-of-political-micro-targeting-c3b0be245607>

GLOBSEC. (2020). *Voices of Central and Eastern Europe: Perceptions of democracy & governance in 10 EU countries*. GLOBSEC. Retrieved from <https://www.globsec.org/wp-content/uploads/2020/06/Voices-of-Central-and-Eastern-Europe-read-version.pdf>

Herhold, K. (2019). How People View Facebook After the Cambridge Analytica Data Breach. Retrieved 1 November 2019, from <https://medium.com/swlh/how-people-view-facebook-after-the-cambridge-analytica-data-breach-4dc1261a0249>

How To Grow Your Business Through Online #Marketing. (2019). Retrieved 1 November 2019, from <https://www.blackbeardesign.com/blog/millennials-and-instagram/>

Joseph, T. (2019). Unregulated political advertising erodes trust in all advertising – Marketing Week. Retrieved 30 November 2019, from <https://www.marketingweek.com/tanya-joseph-political-ads-erode-trust/>

Kovach, S. (2019). Mark Zuckerberg vs. Jack Dorsey is the most interesting battle in Silicon Valley. Retrieved 1 November 2019, from <https://www.cnn.com/2019/10/31/twitters-dorsey-calls-out-facebook-ceo-zuckerberg-on-political-ads.html>

Laslo, M. (2020). Like It or Not, You're Being Tracked. Retrieved 20 August 2020, from <https://www.campaignsandelections.com/campaign-insider/like-it-or-not-you-re-being-tracked>

Love, D. (2011). The Shocking Drink And Incredible Coke History Of Subliminal Advertising. Retrieved 1 November 2019, from <https://www.businessinsider.com/subliminal-ads-2011-5>

Matuščáková, Z. (2018). Koľko stojí revolúcia? Účet Za slušné Slovensko bude nad 70-tisíc - Forbes. Retrieved 20 August 2020, from <https://www.forbes.sk/kolko-stoji-revolucia-ucet-za-pochody-za-slusne-slovensko-bude-nad-70-tisic/>

Ribeiro, F., Shaha, K., Babaei, M., Henrique, L., Messias, J., & Benevenuto, F. et al. (2019). On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook. *FAT* '19 Proceedings Of*

The Conference On Fairness, Accountability, And Transparency, 140-149. Retrieved from <https://dl.acm.org/citation.cfm?id=3287580>

Slovakia - Hofstede Insights. (2020). Retrieved 4 February 2020, from <https://www.hofstede-insights.com/country/slovakia/>

The world's most valuable resource is no longer oil, but data. (2017). Retrieved 1 November 2019, from <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

Views of democratic satisfaction across Europe. (2019). Retrieved 23 August 2020, from <https://www.pewresearch.org/global/2019/10/14/democratic-satisfaction/>

Film

Amer, K., & Noujaim, J. (2019). *The Great Hack* [Video]. USA: Netflix.

X. Appendix

10.1 Appendix 1



Photo retrieved from: <https://fas.org/congressional-science-policy-initiative/hearings/zuckerberg-20191023/>