

CENTRE INTERNATIONAL DE FORMATION EUROPEENNE  
INSTITUT EUROPEEN • EUROPEAN INSTITUTE

SCHOOL OF GOVERNMENT



**Targeted Political Advertising and Data Protection Policies: A  
Comparison of Germany and the United States**

By  
Melinda Machado

**A thesis submitted for the Joint Master's degree in  
Global Economic Governance & Public Affairs (GEGPA)**

Academic year  
2020 – 2021

July 2021

Supervisor: Olivier Glassey  
Reviewer: Wulf Reiners

## **Plagiarism Statement**

I certify that this thesis is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation. I further certify that I have not copied or used any ideas or formulations from any book, article or thesis, in printed or electronic form, without specifically mentioning their origin, and that the complete citations are indicated in quotation marks.

I also certify that this assignment/report has not previously been submitted for assessment in any other unit, except where specific permission has been granted from all unit coordinators involved, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons.

In accordance with the law, failure to comply with these regulations makes me liable to prosecution by the disciplinary commission and the courts of the French Republic for university plagiarism.

### **Statutory Declaration**

*I hereby declare that I have composed the present thesis autonomously and without use of any other than the cited sources or means. I have indicated parts that were taken out of published or unpublished work correctly and in a verifiable manner through a quotation. I further assure that I have not presented this thesis to any other institute or university for evaluation and that it has not been published before.*

*22/07/2021 Melinda Machado*

*“You can have data without information, but you cannot have information without data.”*

*- Daniel Keys Moran*

## **Acknowledgements**

Thank you to my friends and family for supporting me in the many hours I worked on this project. Additional thanks to Professors Glassey and Reiners for taking the time to brainstorm with me and point me in the right direction.

## Table of Contents

<b>1. Introduction.....</b>	<b>7</b>
<b>2. Literary Review.....</b>	<b>11</b>
<b>3. Comparing the Election Systems of Germany and the United States .....</b>	<b>15</b>
3.1. Voting & Party Structure .....	15
3.2. Campaign Advertising Regulations .....	17
3.2.1. Germany .....	18
3.2.2. United States .....	19
<b>4. Who Owns Your Data and How Do They Use It? .....</b>	<b>21</b>
4.1. Data Brokers.....	21
4.2. Social Media Sites.....	23
4.3. Search Engines .....	25
<b>5. Targeting Techniques.....</b>	<b>27</b>
5.1. Psychographic Profiling .....	27
5.2. Microtargeting .....	29
<b>6. Existing Data Protections .....</b>	<b>30</b>
6.1. Germany .....	30
6.2. United States.....	36
6.3. Opt-Out vs. Opt-In & the Privacy Paradox.....	40
<b>7. Overall Risks of Targeting in Political Advertising .....</b>	<b>42</b>
7.1. Algorithms and AI .....	42
7.2. Manipulative and Misleading Advertisements .....	44
<b>8. Self-Regulation from Media Sites .....</b>	<b>47</b>
8.1. Advertisement Archives/Libraries .....	48
8.1.1. Facebook .....	49
8.1.2. Google .....	50
8.1.3. Twitter.....	52
8.2. Shortcomings of Ad Archives.....	52
<b>9. Examining Ad Archive Data .....</b>	<b>54</b>
9.1. Examining Ad Archive Data.....	54
9.2. Google 's Transparency Report.....	56
<b>10. Conclusion .....</b>	<b>61</b>
<b>Glossary of Acronyms .....</b>	<b>70</b>

## 1. Introduction

Targeted political advertising has been a topic of increasing interest in the past decade. With the development of the internet and the increased access to online sites and resources, campaigns have been given a new look into the lives of potential voters. Private industry advertising tactics have grown exponentially, gradually making their way into the political sphere. As internet users, we leave digital footprints as we search, shop, communicate, and interact online through cookies and account tracking. Extensive networks of companies collect that consumer data that can then be aggregated and combined to create detailed profiles of individuals (Christl, Kopp, and Riechert, 2017). The collection and analysis of these profiles can create an in-depth picture of who the consumer is and what drives their decisions. Insight on the consumer can be gained from all kinds of data and therefore all data has an intrinsic value (Dobber, Fathaigh, and Zuiderveen, 2019). Many firms operate in pursuit of that value. Shoshana Zuboff describes this phenomenon as surveillance capitalism, a system in which consumer actions are monitored online to be harvested and sold as a product (2019). As the internet continues to develop and evolve, what can be done with consumer data advances as well (OECD, 2013) (International IDEA, 2018). Mass data collection and the development of Artificial Intelligence (AI) have created a new world of possibilities for analyzing a consumer, or in a political context, a voter. Politicians who utilize targeting techniques know more about each voter than they ever have, enabling a level of connection and personalization that was not possible in the past.

When applied to political advertisements, advanced targeting methods create the ability for campaigns to advertise directly to voters at a personal level. Some of the advanced techniques that have been developed are psychographic profiling and microtargeting. Psychographic profiles use data to determine a user's personality, lifestyle, interests, opinions, attitudes, beliefs, and values (Revella, n.d.). These profiles can be extremely powerful as consumers have never had to manage the influence of personalization at this granular level before, and exposure to online advertisements is unmatched by traditional advertising techniques. Using a psychographic profile to target an individual or small group of consumers is called microtargeting. The implementation of these techniques is quite advanced and can be hard to understand outside the advertising industry despite their social, ethical, and economic consequences (Christl,

Kopp, and Riechert, 2017). Some argue that the level of personalization offered by modern targeting techniques can cross the line into manipulating the voter, using their unconscious biases, and thought processes against them (Bakir, 2020). This manipulation is vital to examine, especially within political advertising, as freedom of choice is an essential democratic principle. Data collection and analysis have become a regular business practice, and the last line of defense for consumers are data protection policies. Data protection policies determine the amount of data that can be collected and the purpose it can be collected for and directly influence the amount of access advertisers have to the voter (International IDEA, 2018). Understanding the consumer has always been of great value to advertisers and politicians alike, and therefore creating detailed profiles on voters to target them most effectively is a priority in advertising and campaigning. The proper way to manage data online is a contested topic with many opinions and many stakeholders. Nevertheless, the power of data collection and the possibility for abuse has continued to show itself. When we consider the necessity of free will in elections, powerful tools to sway voters need close examination. Data protections are an important factor in determining the strength and reach of targeting (International IDEA, 2018).

To examine how personal data protection policies influence the use of targeted political advertising, we will make a comparison between the United States and Germany. These two countries were selected because they offer a stark contrast in data protection models. The United States has minimal data protection policies and looser restrictions for internet development and conduct, which leaves a majority of protections to the interpretation of the Federal Trade Commission (FTC). At the same time, Germany is protected by the European General Data Protection Regulation (GDPR), the ePrivacy Directive, and the German MStV. It has one of the strictest standards of online regulations in the world. When examining these cases, it is essential to note that election proceedings are different in the United States and Germany. Therefore, a direct comparison between the two countries is complex and challenging to attain and many impacts to election systems must be examined. This paper will examine how data protection policies influence the use of voter targeting in political advertising by examining existing election systems, campaign regulations, data protection policies, and political advertising techniques to ascertain what outside features impact targeting practices that may not be



directly tied to data protections. Therefore, giving us a clearer picture of what is linked to data protection policies. In Germany, campaigns are party-run, and in the United States, campaigns are more candidate-focused. Germany is home to a multiparty system, while the United States is home to a two-party system. We see a difference in campaign financing and sheer size of the countries. In Germany, campaigns are financed in majority by the government, while in the United States, parties are run based on donor contributions and personal funds. Additionally, the United States has a population that is nearly four times the size of Germany. We must examine these differences when reviewing the development of targeted political advertising online, psychographic profiling, and how to implement data protection policies effects these techniques. Each of these features creates a slightly different campaigning atmosphere between the two countries, yet the possibility for voter targeting is present in both settings. Despite the many differences between the election proceedings in the United States and Germany, targeted political advertising is present.

Finally, we will review the Spending Tracker provided by the Facebook Ad Library and the Transparency Report data provided by Google to help establish current trends of political advertising targeted at voters in each country. A majority of advertising online is done within the duopoly of Google and Facebook, the two major digital platforms (Christl, Kopp, and Riechert, 2017). Facebook does not provide targeting features used by advertisers. They only provide an audience breakdown showing who the advertisement reached; what percentage were women vs. men, what percentage were in what age range, and what percentage were in a particular location. As a result, a review of targeting in Facebook advertisements would require the compilation of multiple outside data sets and was decided to be outside of this paper's scope. Trends in spending data, however, give us an idea of the cost of advertising and the quantity of ads invested in, allowing us an inside look at voter targeting costs. To assess significant trends in voter targeting, we will review the Google Transparency Report, which includes information on the targeting criteria selected by advertisers concerning age, gender, and location. In the scope of this paper, we will focus on the choice to use or not use multiple targeting factors as opposed to what specific ages, areas, and locations were targeted the most or the least. This review is comprised of all the available advertisement data on political or social issue ads delivered to German or American audiences from the beginning of the

Transparency Report in each location. When reviewing this data, advertisement targeting features in election years received special attention. In the United States, the election in focus is the 2020 presidential election. As the most recent federal election in Germany took place in 2017, before the creation of the Transparency Report, we will instead review 2019, the year of the European Parliament election as targeting for this election also took place on a national scale in Germany.

## 2. Literary Review

The major trends of research in the field of targeted political advertising are profiling, regulation, fake news, and ethics. While there has been much research on targeted political advertising, a majority of researchers focus on the United States exclusively, or on manipulation campaigns from foreign bodies. While many researchers discuss the ways that data protection policies can limit data collection, strong data protection policies are new to the political sphere and therefore there is limited data to properly study the impacts of these policies in the long term. Additionally, there are limitations in the study of this field based on the availability of actual targeting data for review and the secrecy surrounding targeting techniques that may be more extreme. Much of the research on this topic has been conducted in peer reviewed academic journals or in paper's produced by think tanks following trends or by journalist tracking scandals. As data protection policies are evolving over time research must continue in this field, therefore sources that were published in 2016 or later were given the most weight in my analysis.

There is a large amount of research in the field of targeted political advertising specifically after 2018 in relation to the Cambridge Analytica Scandal. This scandal had a substantial impact on public opinion of data collection and spurred interest in data protection policies. A brief summary of the scandal is as follows: Cambridge Analytica, a data firm owned by Robert Mercer, improperly collected data from Facebook to create profiles of 87 million Facebook users. A Facebook quiz developed in Facebook's API harvested data from quiz takers and their Facebook friends (Chang, 2018). Facebook's data collection rules at the time did prohibit the sale of this type of data. However, Cambridge Analytica sold this data anyway, and their connection to the Trump campaign drew massive attention to the uses and repercussions of mass data collection in the political sphere. The scandal drew connections to the 2016 US Presidential Campaign, the Brexit campaign, and other various campaigns around the world. This scandal brought public attention to the possibility of manipulative and misleading advertising practices fueled by advanced targeting techniques such as microtargeting and psychographics. This paper will not focus on this scandal for two main reasons: first being that extensive research has already been done on the incident and second being that the focus of this paper is the legal collection and distribution of data. As the data collected and used by

Cambridge Analytica was sold illegitimately it is not a main focus of this paper. However, some of the lasting impacts and fallouts of this scandal will be mentioned as it is so deeply ingrained in the topic.

When researching targeting trends and marketing techniques most resources are articles from US marketing firms offering their services or discussing strategies for businesses. Alexander Nix, a notable Cambridge Analytica actor, discussed some of the more extensive techniques that Cambridge Analytica used during presidential campaigns, such as the OCEAN technique and data harvesting, at the Concordia Annual Summit in 2016. This speech gives an inside look at some of the most advanced targeting strategies and how they were used in the US in a real case. However, following this scandal, firms that use more advanced targeting techniques are keeping their strategies quiet to avoid public backlash, and therefore current uses are harder to study. Microtargeting is discussed as a tool for both good and bad, persuasion and dissuasion, information and confusion, mobilization, and demobilization (Dobber, Fathaigh, and Zuiderveen, 2019).

As this paper relies heavily on the implication of data protection policies and in the United States and in Germany several data protection policies were reviewed including the GDPR, the MStV, the ePrivacy Directive, the CCPA, FTC regulations, and several FTC decisions. As well as government sites that aim to educate on the uses of these policies. There is extensive literature on the lack of overarching data protection policy in the United States. One of the most critical of the current state of data regulations in the US is Shoshana Zuboff. In her book, *The Age of Surveillance Capitalism*, she makes a strong stance against allowing companies to profit off consumer data (2019). Even in the case of regulation there is still the issue of consumers not taking the steps to be proactive and protect their best interest online, this is called the Privacy Paradox (Eskens, 2019) (Kozyreva et al., 2021). The privacy paradox is often discussed as a human fault. However, this is dismissive of the power of good regulation. If voters can only be offered good options than their faults are less likely to lead to a manipulative end. Most of the research in digital German campaigning is related to how digital tools have enhanced canvassing (Kruschinski and Haller, 2017) or how they have helped parties build a presence in online spaces (Jungherr, 2016). Some papers praise the protections of the GDPR, listing it as the most effective data policy, arguably turning a blind eye to some of the gaps left in data protections that need further policy development to address (Crain

and Nadler, 2019). A policy paper by Dr. Jaursch reviews some of these gaps notably the risk of distorted public debates, the need for restrictions on behavioral microtargeting, and the need for obligated transparency for platforms. These gaps are important to note especially in digital policy where things can change so quickly.

As the internet and AI develop many scholars are examining the risks and implications of data collection. Algorithms and machine learning offer opportunities in a variety of fields. There is a large amount of literature about the ethics of AI, big data, and personal data processing. These articles discuss the threats of political speech tailored to the individual level (Ruohonen, 2020), the ways in which persuasive communication can become psychologically manipulative (Bakir, 2020), and the power of datafication of interactions online to create value (Christl, Kopp, and Riechert, 2017). The OECD published a digital economy paper, *Exploring the Economics of Personal Data* that attempted to quantify the value of personal data and the data economy in general. This is an interesting piece of literature as we can see that personal data has influenced the market but quantifying it's worth is an interesting challenge, despite being published in 2013 this paper was reviewed for this project due to its lasting relevance in examining the data's value.

The most directly comparable resource when analyzing campaign advertisements in both countries are the advertising archives created by Facebook and Google. Within this field, there have been studies of advertising archive data, but these studies are limited to the data that is shared by the platforms. One of the key features that is often left out is targeting data. As there is limited targeting information made available by the archives the extent of targeting use is not entirely clear. Despite this there have been studies on targeting and microtargeting. As microtargeting is hard to measure exactly these studies have often had to infer which ads were distributed using microtargeting. In these studies, ads have been identified as being microtargeted based on estimates by examining other characteristics that are provided by the archive. For example, one study from NYU which reviewed microtargeting in United States elections defined microtargeted ads as advertisements with less than 1,000 impressions and/or a cost of less than \$100 (Edelson et al., 2019). Another study from Northeastern University researchers that reviewed Facebook targeted political advertising by cross referenced the general data provided by Facebook about ad targeting a crowdsourced political advertisement archive that was

created by ProPublica to discern targeting trends (Ghosh, Venkatadri, and Mislove, 2019).

February 1st, 2021, Facebook made targeting data available for 1.65 million social issues and political advertisements via their Facebook Open Research and Transparency platform (FORT) including ads that ran in the three months prior to the United States Presidential election on November 3rd, 2020. Currently, access to the dataset is restricted to academic researchers only at the Ph.D. level or higher. Despite requesting access, I was excluded from accessing these data sets due to the master's level of this project. This data set offers new insight into the detailed targeting of political advertisements in the United States, but no comparable data has been released for Germany. As this data was only recently released extensive studies around its implications have yet to be released. Further examination of this data is likely to indicate more trends in targeting practices.

There are limited studies on how targeting is used outside of the United States and there is often only discussion of extreme circumstances of targeting scenarios as opposed to studies of trends in targeting usage as I will discuss in this paper. In majority targeting trends are discussed as hypotheticals or in scandal cases in the past tense. I hope to add a visual of the present moment in targeting in each country by capturing the spending habits of advertisers as provided by the Spending Tracker in the Facebook Ad Library and the trends of targeting that are provided by the Google Transparency Report. In my comparison of Germany and the United States I have attempted to review information that gives insight on the many features that impact political campaigning in each country, the way data collection occurs, how data can be used, and the ways in which data protections might impact targeted political advertisements.

### **3. Comparing the Election Systems of Germany and the United States**

To fully understand the varying implications of data protection policies on targeting in the US and Germany, we must first understand how their electoral systems compare. To compare their similarities and differences, we will review their representation systems, their party structures, and their campaigning advertising regulations. These features impact the effectiveness of targeted advertisements in each country and create different opportunities for political advertisers to communicate with voters. Both Germany and the US have regulatory frameworks for campaigning outside of data protection policies. It is essential to understand these existing operations of elections and campaigns to fully understand digital campaigning and the place that targeted advertising has in the system. A review of these systems will help us obtain an initial understanding of the elections in each country.

#### **3.1. Voting & Party Structure**

First, we will examine the different representation systems at the federal level in Germany and the US. Germany uses a proportional representation system where a parliament called the Bundestag holds federal power. This system awards seats in parliament to parties based on both direct votes for candidates and the total portion of the votes that each party received. Within this system, voters submit one vote for a member of parliament and one vote for a party with no candidate specified. These two options allow voters to split their vote if they would like and vote for a candidate from a different party than the party they assign their second vote to. Once the votes are counted in each state, the winning local member of parliament and a group of members from each party join the Bundestag based on the portion of seats won by each party. Party members are extremely valuable as they help to determine the overall breakdown of the Bundestag, where the chancellor and legislation are decided (Palese, 2018). The United States, on the other hand, has a representative democracy system in which voters vote exclusively for candidates as opposed to parties. Therefore, the reputation and likability of each party representative candidate is directly tied to the votes for that party. Individual candidates determine the party distribution of the House of Representatives, and the Senate voted into office, and direct votes also determine the president. There is no party representation outside of direct candidate appointments and no ability to split votes. The different

dynamics in each election style create different opportunities for targeting. Targeting is especially relevant in elections where key areas or voters are of particular importance (International IDEA, 2018). For example, targeting is used more in the US swing states that often determine national elections. In these states there is an additional incentive to target voters in these states to persuade them to vote for a party's candidate or dissuade them from voting at all. In proportional voting systems, like in Germany, targeting is less impactful at a national scale as small segments of the population are less powerful in swaying the electoral system (International IDEA, 2018).

Second, we must consider the number of political parties in each country as this plays a role in how targeting may be used. The United States has a two-party system that is made up of Republicans and Democrats. There are smaller parties also present in this system, but only two major parties compete for votes. In a two-party system, it is much easier to influence votes in a candidate's favor. To do so, a campaign must only convince the individual not to vote for their opponent. By convincing a voter not to vote for their opponent, they increase their overall percentage of voters regardless of whether they abstain from voting, vote for their candidate, or vote for a 3rd party candidate. In Germany, there are currently six parliamentary groups representing eight parties represented in the Bundestag: the CDU/CSU, SPD, AfD, FDP, The Left Party, and The Greens/Alliance 90 (Parliamentary Groups, n.d.). This more significant number of active political parties makes targeting more difficult. If a campaign targets a voter to dissuade them from voting for a specific candidate or party, they have many alternatives to choose from. Not only that but swaying their vote will likely adjust the proportions of the Bundestag a minimal amount. In the United States, dissuading a voter is a lot more powerful. It has a more direct impact on the outcome of an election. In Germany, persuading voters to vote for a candidate may be a more impactful method. However, the possible impacts of profiling and targeting in Germany should not be entirely discounted based on their party system; this system can still encourage the spread of polarizing ideas, create societal tension, and allow wealthier parties to control the narrative online (Jaursch, 2020). These factors create a risk to free and fair elections, and it is essential to be proactive in containing these problems.



### **3.2. Campaign Advertising Regulations**

As the world transitions to become more digital, our lives and interactions are becoming more digital as well. In digital advertisements, politicians can use the strong wording and convincing messaging of the past that would have been delivered via speech, pamphlet, radio, etc. but deliver this content to voters at unprecedented speeds and specificities. Digital campaign advertising is pivotal in understanding the digital campaigning system. Campaigns have become increasingly reliant on what has been dubbed computational politics or “the application of digital targeted-marketing technologies to election campaigns” (Alghizzawi, 2019). These technologies have been utilized for positive impacts such as mobilizing voter turnout, engaging young people, raising money, and supporting grassroots ground operations. However, they have had some complex impacts on voter’s data privacy and have recently been seen as having the possibility to be manipulative or coercive (Alghizzawi, 2019).

As campaigns continue to turn towards digital means of communication, we have seen the availability and granularity of data become a cornerstone of campaigning (International IDEA, 2018). With commercial access to data more readily available than ever, political parties can bolster their profiles by combining commercially collected data, publicly available voter data, and their own data collected by canvassing with consumer data to create a detailed overview of a voter (OECD, 2013). Digital tools have also enabled growth in market segmentation, opinion polling, targeted campaigning, and direct marketing (Bakir, 2020). All of which strengthen political advertisement. Differing campaign stakeholders use differing techniques. Candidates and PACs rely more on the targeted lists and lookalike functions of targeted advertisement, while for-profit media tends to rely more on targeting by interest (Edelson et al., 2019).

Another important trend indicates that better-funded campaigns are more likely to target based on sensitive private information. In contrast, lower funded campaigns are most likely to target based on focused geographic areas (Ghosh, Venkatadri, and Mislove, 2019). The number of political advertisements has been on an upward trend in the last decade, indicating an increased hunger for this type of media. There has also been an adjustment from ideology-based politics to issue-based politics, increasing the need for campaigns to understand what issues are important to their voters (International IDEA, 2018). Datasets are becoming increasingly important in finding these hot button issues.

We have seen considerable investment in online advertising in the digital sphere. Political advertising regulation has been criticized for being too focused on old methods of communication, allowing corporate regulations to dominate, and having too few regulations in general (Jaursch, 2020). In some cases, mirroring traditional advertising rules and regulations within digital platforms may be an easy and effective way to expand campaign regulations. However, this type of regulation leaves gaps for practices that do not exist within a traditional framework. The two types of regulations we will focus on are regulations of funding and broadcasting restrictions. Both countries have different strengths and weaknesses in these fields, and campaign regulations have room for expansion, especially in online and digital campaigning. To understand the differences between the regulations in each of these countries, we must briefly examine an outline of existing regulations.

### **3.2.1. Germany**

In Germany, campaigns are financed in majority by state funding, membership fees, donations, and sponsorships. State funding is one of the big differentiators of campaign finance between Germany and the US. Government contributions are decided based on the number of votes the party received in recent elections, party membership dues, and donations received and generally fulfill the majority of a campaign budget (Party Funding, n.d.). Every year party's receive "0.83 euro for each valid vote cast for the respective party list or, if a list for that party was not admitted at the Land level, each valid vote cast for a party in a constituency or polling district" and "0.45 euro for each euro received from other sources (membership dues, contributions from elected office-holders, or lawfully obtained donations)" with the caveat that "only donated amounts of up to 3,300 euros per natural person will be taken into account" (Funding of Political Parties, n.d.). Campaign budgets in Germany are typically much smaller than they are in the United States. For example, the CDU, the party of the acting Chancellor of Germany, was estimated to spend €164 million in 2017 the last federal campaign year while US parties will spend billions (Breakdown of CDU Expenditures Germany 2014 to 2019, 2021). Despite this, there are no formal limits on private or corporate donations, and there are no formal limits on campaign spending though transparency is expected with major donations (Funding of Political Parties, n.d.). Though German campaign budgets are

often smaller than US budgets, they still spend a large amount of capital on political advertisements. For example, it is estimated that German parties paid €1.5 million for online advertisements during the 2019 European Parliament Elections (Jaurisch, 2020).

Advertising laws are very specific in Germany. An agreement among states indicates that radio and television advertising spaces cannot be bought and are instead allotted on public broadcasting stations based on the share of votes received in the last election. With better-represented parties receiving more time slots and lesser represented parties receiving fewer, additional ads can be purchased but are considered expensive (Schultheis, 2013). Additional restrictions are applied to visual campaign tools such as billboards and poster, which are limited to a brief period of display prior to a campaign and rules are decided at the local level (Jaurisch, 2020). Based on these limitations, digital campaigning offers an opportunity to access voters that they may not have had before. The MStV has recently expanded the limits of broadcasting regulations into the online sphere. However, at this time, there are no election-specific advertising regulations determining how campaigns interact with individuals online. Online interactions are instead restricted mainly through budget, time, and expertise constraints (Kruschinski and Haller, 2017).

### **3.2.2. United States**

The United States electoral system is funded primarily by donors. There are clear contribution limits based on who the donor is and what type of fund they are contributing to. For example, an individual donor can donate \$2,900 to a candidate committee which a national party committee can donate up to \$5,000 to the candidate's committee (Understanding Ways to Support Federal Candidates, n.d.). These numbers can add up to huge sums. NPR's spending tracker of the 2020 election estimated that then-presidential candidate Joe Biden raised \$1.69 billion from donors and former president Donald Trump raised \$1.96 billion from donors (McMinn, Hurt, and Talbot, 2020). There have been developments in policy to help with transparency in advertising, such as requiring disclaimers and disclosures and limiting the use of soft money. One of the most straightforward rules in the United States related to election advertisements is the requirement to include disclaimers that the advertisement is political and specifying who paid for it. Specifically, disclaimers are required on any public communication, which

includes broadcasts both cable and satellite, newspapers, magazines, outdoor advertising facilities, mass mailing, phone banks, and communications placed for a fee on another person's website, as well as two digital means of communication that are not considered to be public communication, e-mail and public websites of political committees (Advertising and Disclaimers, n.d.). There has also been some discussion of a possible expansion of political advertisement regulations. For instance, the US Federal Election Commission has asked for public comments on whether it should develop new disclosure rules for online advertisements (Alghizzawi, 2019).

Television and radio advertisements are regulated by the Federal Communications Commission using the Bipartisan Campaign Reform Act of 2002 and the Federal Election Campaign Act of 1971 (FCC, n.d). These acts are more focused on the financing of campaign advertisements instead of limiting content or run time of advertisement. The Bipartisan Campaign Reform Act is an amendment to the Federal Election Campaign Act of 1971 and was also implemented to limit 'soft' money or money that is not subject to federal law. Soft money cannot be tied directly to a political candidate and therefore cannot be monitored as closely. The Act prohibits explicitly: "(1) national political party committees from receiving or using soft money in federal elections, (2) state, district, and local political parties from receiving or using soft money for federal election activities; for specified activities, including voter registration drives and get-out-the-vote activities, these parties can use non-federal funds, and (3) federal candidates and officeholders from raising or using soft money for federal election activities"(Bipartisan Campaign Reform Act, 2002). This act is the most significant limitation to campaign spending in the United States. However, it has a minimal impact on campaign advertising spending overall as long as advertisements are appropriately funded and disclosed. Like in Germany, digital advertising is an expanding sphere in the US.

## **4. Who Owns Your Data and How Do They Use It?**

In order to create the most comprehensive profiles on voters, advertisers need access to data. Data is most valuable in bulk, and therefore the mass collection of data is a growing industry that relies on a large number of companies collecting data on consumers that can then be combined by data collectors to be rented and sold to others (Christl, Kopp, and Riechert, 2017). Approximately 74% of commercial advertisements in the United States rely on targeted data (Edelson et al., 2019). With so much data out there to target consumers, it can also easily be used to target and categorize voters. The more detailed the information available for each voter the more accurately campaigns can target them (International IDEA, 2018). Access to data is different in Germany and the United States, but the data owners are mostly the same. Having the data of a nation can make an advertiser a very powerful influencer. The exact value of data is difficult to ascertain, but it is clear that data is increasing in economic and social value as business models relying on personal data increase (OECD, 2013). The data economy creates an atmosphere in which personal data is harvested from various sources and sold and traded in various ways. The three prominent data collectors that we will examine are data brokers, social media sites, and search engines.

### **4.1. Data Brokers**

Data Brokerage is an old profession that has taken on a new life as technology developed (Rieke et al. 2016). Privacyrights.org, a site that tracks data broker activity, lists 231 active data brokers in the United States (2021). There is no official registry of data brokers in Germany. However, the data economy in Europe is booming. A 2020 study by the European Commission estimated that the EU data economy would reach a value of €550 billion by 2025 (Cattaneo et al., 2020). The most considerable growth in the data economy within Europe is estimated to be had by countries with the most robust economies, Germany included (IDC and Open Evidence, 2017). However, data brokers do have more obstacles in countries that have strong data protection policies since data cannot be traded as easily. When it comes to advertising, data brokers are collectors that aim to gather individual data and create comprehensive profiles of target markets and demographics, and ultimately target the best consumer for a good or service. Data brokers often buy and sell from each other to create more comprehensive profiles on individual

users, communities, or devices. This data can be volunteered, observed, or inferred (OECD, 2013). Data brokers collect data from many sources such as public government information, consumer data provided by commerce sites, activity data collected from apps and devices, information shared by individuals on public domains, credit and account data, and more. Data brokers collect information to be bundled and sold to other parties such as banks, advertisers, and campaigns. This information can be combined with online tracking and locational tracking and be analyzed to look for trends in behavior for a voter or a type of voter. Data brokers sell both "actual" and "modeled" data. Modeled data can take several forms, including segments, lookalike models, and scores (Rieke et al. 2016).

Segments are groups of individuals with similar characteristics that are categorized together based on their similarities. For example, these may be groups like retirees who live alone or individuals under 30 who work in a particular field. Some market segments are broad, and some are specific. In the United States, it is common for these segments to be given catchy nicknames during the presidential election. For example, Bloomberg News published an article in September of 2020 stating that nine types of voters would decide the election: Double Haters, Tired Trumpers, Racial Justice Voters, Minority Mold-Breakers, Coronavoters, Swinging Seniors, Hurricane Maria Refugees, Florida's New Enfranchised and Shy Trumpers (2020). Segments that are the most persuadable to switch candidates, parties, or stances on a specific issue are often targeted in political elections, receiving more focus than voters who are more likely to be set in their ways. While this can be an efficient practice for a campaign, it is also discriminatory to voters who do not fit the desired demographic because they often receive less information or attention from candidates.

Another tactic used by data brokers is lookalike modeling. Lookalike models use data collected from a wide array of sources to predict a person's future actions based on the actions of other people with similar data and the choices they have made. For example, if a voter is designated within a segment of interest to the electoral party, a campaign may seek out lookalikes, other users who act and engage with similar sites, live in similar areas, shop in similar places, etc. Lookalikes can be determined by a combination of many different factors. The more data collected; the more factors can be reviewed for correlation (Bakir, 2020). Based on the compared data with the designated subject, any number of data points may be used to determine whether they are similar enough to have

an estimated equivalent response to the product or in the case of political advertising, a candidate or party.

The final category of data collection and analysis offered by data brokers is score prediction data. Scores predict the likelihood of a person completing a particular task or exhibiting a certain behavior based on previously collected data from the consumer. Some examples of scores in practice are credit scores, fraud scores, and stress scores, which predict the likelihood to default on loans, the likelihood that a transaction is fraudulent, and the likelihood that a person's stress might affect their health, respectively. In a campaign setting, it may be possible to determine a score as to how persuadable the subject may be or how likely they are to vote for a specific candidate. For example, the UK's Labour Party created a series of scores measuring factors like major areas of concern and likelihood to vote for the Labour party and used these tactics to target voters (International IDEA, 2018). The more data that data brokers can collect, the higher the likelihood that they will be able to predict or anticipate future actions, and the more valuable that data will be to their consumers.

#### **4.2. Social Media Sites**

Social Media sites are great collectors of personal information. They collect information provided to them by users, such as their emails, birthdays, 'like' data that allows sites to identify what they are interested in and data from linked accounts with other apps and services. Facebook has many apps that interact with its users on several types of devices and can track activity even when a user might not realize they are interacting with the social media site. These data points create a relatively robust amount of information directly tied to a name, email, and specific profile (Chester and Montgomery, 2017). This data can be incredibly useful when targeting users. Social media sites have an additional advantage in targeted advertising because they are the collectors of data and the advertising platform that engages with users, which means they can link advertisers to consumers in-house. This direct-to-consumer link allows them to use the consumer data they have collected without selling the data to advertisers (Christl, Kopp, and Riechert, 2017). Facebook offers three options to potential advertisers: core audiences, custom audiences, and lookalike audiences.

Core audiences can be tailored based on location, behavior, demographics, connections, and interests (Facebook Advertising Targeting Options, n.d.). Behavior is an umbrella that, according to Facebook, encompasses things like device usage and prior purchases. Demographics is advertised as the opportunity to "[c]hoose your audience based on age, gender, education, job title and more" (Facebook Advertising Targeting Options, n.d.). Exploration of the Facebook Audience Insight page, where advertisers build advertisements, shows options for customization based on rather specific features such as the age of a user's children (if any), life events such as 'new relationship' or 'away from family' and, perhaps the most interesting for this paper, politics with five categories ranging from 'very liberal' to 'very conservative.' It is not specified within the Facebook Audience Insight page how they make these determinations about people. There are no listed criteria for separating a 'liberal' profile from a 'conservative' profile or even from a 'very liberal' profile. This is an example of how advertisers can develop campaigns based on traits that users have not disclosed but instead have been inferred using predictive analytics (Crain and Nadler, 2019). Additionally, the list of interests available for selection is quite extensive. It features broad categories like entertainment that break down into much more specific categories such as specific types of board games, video games, and movies. A call for information from the public organized by ProPublica in 2016 indicated that Facebook used approximately 52,000 attributes to classify its users (Angwin, Mattu, and Parris Jr., 2016).

Custom audiences can be built based on a provided contact list, users of an advertiser's app, or people who engage with an advertiser's Facebook page. This feature makes it possible to use these tools in conjunction with data provided from other places, such as a data broker. For example, an advertiser or campaign could use a list of emails, cookies, or social media handles of a specific target audience provided by a data broker to create a custom or lookalike audience on Facebook (Bakir, 2020). Lookalike audiences, which we have previously discussed in the data broker section, are created by Facebook, requiring only a source audience (Bakir, 2020). These tactics allow for extensive targeting on social media, using what platforms know about users and their connections to provide advertisers with better audiences for their products. All of these options allow for precise targeting down to the individual level.



### 4.3. Search Engines

Similar to social media sites, search engines collect data on individual users as they use their products. Searches run, sites accessed, and app information are collected to track a user's patterns and lifestyle (Bakir, 2020). One of the most influential search engines is Google, which also runs an advertising platform. Google displays advertisements within its platforms, including Google search sites, YouTube, and third-party sites that use Google Ads. In an ad help document published to the Google support page. Google is similar to Facebook in that it can allow users to run advertisements using their data without selling it to them. Which allows for them to face less regulations about the transfer of data. Google offers many different targeting options to advertisers.

'Reasons you might see an Ad' breaks down into three categories: your info, your activity, and other info. User info is specified as information in their google accounts like age range and general location. A user's activity is more complex, noting their search history, their previous search activity, their activity when they were signed into Google, ad interactions, the types of websites they visit, the types of mobile apps they use, and their activity on other devices. Other information includes examples of time of day and information given to an advertiser (Why You're Seeing an Ad, n.d.). These specialization features paint a picture of how Google collects user information to be sold to advertisers. Some data is collected directly while other data is inferred. When reviewing my personal advertising data within Google, I saw that I am grouped into categories, including renters, education status: bachelor's degree, and parental status: not a parent. All of this information is correct, but I have not shared it with Google directly. Further investigation into how I was sorted into these categories led me to the message, "Google estimates this demographic because your signed in activity on Google services, and on other websites and apps, is similar to people who've told Google they're in this category." (Ad Settings, n.d.). Meaning that this data has been inferred about me and not collected directly.

Google does allow you to turn ad personalization off and to remove the data previously collected about you. However, as we will discuss later when addressing the privacy paradox, users do not always act in their best interest or even in their expressed interest concerning data privacy. Current restrictions for Political Advertising on Google limit advertisements to targeting based on age, gender, location, and contextual targeting options: ad placements, topics, keywords against sites, apps, pages, and videos (Spencer,

2019). Despite these limitations, we can see capabilities far more advanced offered in general advertising. These advertising techniques were also available for political advertisers until they were reduced in November of 2019 due to public backlash (Spencer, 2019).

## **5. Targeting Techniques**

Targeting has become more advanced as more data has been made available for collection and analysis. The better understanding a campaign has of a voter, the better they can tailor messages to them specifically. Two targeting techniques that have become particularly advanced are psychographic profiling and microtargeting. Consumer data feeds these tactics, and they have been under scrutiny for violation of a reasonable assumption of privacy (Dobber, Fathaigh, and Zuiderveen, 2019) (Bakir, 2020) (Ruohonen, 2020). Political campaigns quickly picked up advertising techniques as they transitioned to increasingly digital presences. Microtargeting and psychographic profiling are techniques that began in the United States and have spread throughout the world, gaining popularity as the method proves itself successful (Dobber, Fathaigh, and Zuiderveen, 2019). Psychographic profiles have been compiled as advertising resources worldwide, and with the development of more complex profiles, microtargeting has become more precise. These techniques generally feed off of each other. Psychographic profiles provide the information that fuels microtargeting techniques, and then A/B testing or experiments are used when applying microtargeting. The results can then be fed back into the psychographic profile bolstering its effectiveness in the future.

### **5.1. Psychographic Profiling**

Psychographic profiling is a technique developed for advertising to get advertisers in touch with the most relevant customers for their product. The study of psychographics encompasses the complex understanding of each consumer by categorizing people based on their attitudes, aspirations, and other psychological criteria. Online psychographic profiles are built using data generated by internet users through location services, social media profiles, purchased profiles from data brokers, and any information given to an app or third-party service (Chester and Montgomery, 2017). Psychographic profiling is not necessarily a strictly digital practice, but online is where they are most effective and malleable leading to better results. The digital realm has also been established as a great place to harvest data that gives insight into a person's psychographics as multiple data streams have been found to make these profiles more effective (Bakir, 2020). Advertising techniques that appeal to consumers on more profound and more personal levels are more convincing and compelling (Crain and Nadler, 2019).

In the past, psychographic profiles were more general and based on more significant segments of people. However, in recent times, psychographic profiles have been exponentially enhanced by mass data collection capabilities online. For example, when designing a television commercial offline, an advertiser may use psychographic methods to determine its content. They can estimate the interests of a channels assumed viewers based on the channel's content or use the time of day the commercial will run to guess who will be watching and tailor the content to appeal to them. Online advertisers have more control and more options as to where to input an advertisement to reach precisely the types of people the ad was created to impact. An online advertiser using psychographic profiling might tailor an ad to appeal to a consumer's specific interests, wrap it in their favorite colors, use a tone that has led them to purchase in the past, and deliver that advertisement to them on their favorite website. A massive amount of online data can be monitored to track psychographic features. As storage capacity increases in the digital realm, so does the ability to collect comprehensive data sets and analyze trends (OECD, 2013). The advancement in artificial intelligence bolsters these targeting methods, allowing platforms to adjust the presentation of advertisements in real-time based on response factors.

Politicians and their teams have also picked up psychographic profiling as a tool to reach potential voters more efficiently and tailor messaging to them in the most effective ways. This method gives campaigns easier access to a specific audience via specific demographic segmentation beyond the capabilities of traditional canvassing techniques (Chester and Montgomery, 2017). Due to the demand for the most effective campaigning methods, many data brokers have begun offering their services to businesses and campaigns (International IDEA, 2018). Data is vital to psychographic profiling, and more data gives campaigns more insight into their potential voters. How much access data collectors have to a voter's data to build out psychographic profiles varies based on the country they are in and the data protection policies that apply. Further examination of these differences will be developed in the sections to come.

## **5.2. Microtargeting**

Current advertising techniques take into account the profiles of every individual user and attempt to serve them the most relevant ads. Microtargeting practices are fueled by detailed psychographic profiles, as discussed above. These practices allow advertisers to gain information from various sources, including online and offline sources. They can include cross-targeting multiple devices, which can connect a user's online presences and help establish trends in behavior and then use that compilation of data to target a user (Chester and Montgomery, 2017). Psychographic techniques outside of explicit profiling have been used for decades, using emotional messaging to trigger a response from the consumer (Chester and Montgomery, 2017). Microtargeting techniques are unique in their level of personalization and the large scale at which that personalization is achieved.

Microtargeting takes the information advertisers know about a voter or small group of voters and uses that information to tailor what they present to them. With entire academic branches and corporate firms aimed at studying and developing market research, microtargeting tactics are more influential than ever (Ruohonen, 2020). These techniques are used by many advertisers online, and though they were initially created and developed by commercial advertisers, they have gained traction in the political advertising field (Chester and Montgomery, 2017). Based on the wide range of possibilities when it comes to microtargeting, all consumer data becomes valuable (Dobber, Fathaigh, and Zuiderveen, 2019). The International Institute for Democracy and Electoral Assistance identifies two main factors that contribute to effective microtargeting. The first is reach, or how much data has been collected and directed towards targeting an individual, and the second is precision. Precision is mainly affected by the legal frameworks and what targeting is allowed (International IDEA, 2018). Both of these factors rely on data protection policies, and therefore, we can see the direct tie between data protection policies and the impact of microtargeting. Consumers are often unaware of exactly what characteristics they are being targeted for and how their responses might affect future targeting making it a controversial practice (Bakir, 2020).

## **6. Existing Data Protections**

There are three e-privacy models prevalent in the modern world. The first is the US model, which is relatively unregulated, focusing on the importance of free speech and autonomy. This model does not include overarching data protections and has led to the world of surveillance capitalism as discussed in the introduction in which the capitalistic system and enterprises drive e-privacy practices. The second is the European model, which focuses on large-scale regulation, the GDPR. The third model is the China-Russia model that features the most control and surveillance limiting what users can access and having large control over their data. In the context of this paper, I will compare the existing data protection policies of the first two models, the US and the EU through a German lens. Data protection laws can contribute to the ability, or lack thereof, to collect personal data and develop psychographic profiles on voters. When personal data cannot be collected or stored as easily, targeting becomes more difficult to execute. Therefore, the threat of targeting based on psychographic profiles is directly linked to the data protection policies in that country. Data is split into two groups: Personally Identifiable Information (PII) and Non-Personally Identifiable Information (OECD, 2013). Personally Identifiable Information is the most important to protect and is widely expanding as it becomes easier to link a person's real identity to their data. Protecting non-PII data is difficult because it only takes one link to an individual to deanonymize a group of data that has been connected previously. Once a link has been made any connection between the PII data and the non-PII data breaks the anonymity of the latter (OECD, 2013). As data becomes easier to string together psychographic profiles become easier to create and targeting becomes more accessible. In order to address how microtargeting may be influenced by data protection regulations, we must understand what regulations are currently in place in both the United States and Germany.

### **6.1. Germany**

Germany, as a part of the EU, has more stringent Data Protection laws than the United States. The EU considers the protection of personal data to be a human right and therefore has a strong data policy. Through the European Union, Germany participates in the General Data Protection Regulation (GDPR) which came into force in 2016 and required compliance by May 25th, 2018, and the ePrivacy Directive, which was originally

implemented March 15th, 2006, and was updated on November 25th, 2009, and is soon to be replaced by the ePrivacy Regulation (EU Directive 2002/58, 2002). The GDPR features protections like the right to erasure, the right to restrict processing, and the right to object. The GDPR is a document aimed towards uniting European Data protection standards and is built on seven principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability (GDPR, 2016). The document has a rather wide scope applying to all data collection within Europe or outside Europe when European citizens are the subject of data collection. There are two important definitions within the GDPR that relate to profiling and targeting. The first is profiling which the GDPR defines as: “any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subjects performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements where it produces legal effects concerning him or her or significantly affects him or her” (GDPR,2016). Having a clear definition of what profiling is creates a much stronger case in data protection disputes. The second is personal data which is defined as: “any information relating to an identified or identifiable natural person... who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (GDPR, 2016). This definition helps to build a clear picture of how large the realm of personal data is and helps to establish a clear picture of PII.

Any data that can be tied to you can be used to influence you. These definitions are important because compiling this information is the basis of how psychographic profiles are built and in turn how they can be used for targeting within election advertising. Within the document there are several mentions of profiling protections such as in Article 9: Processing of Special Categories of Data which prohibits the processing of personal data that reveals race, ethnic origin, political opinions or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life, or sexual orientation (with some exceptions), Article 15: Right of Access by the Data Subject, which specifies that a data subject has the right to access their personal data and

in the case of profiling the significance and consequences of that profiling for the subject and Article 21: Right to Object which states that “[w]here personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that is related to such direct marketing” (GDPR, 2016).

The most common way for users to allow their data to be collected in compliance with the GDPR is by opting in to data collection but there are five other methods that can be employed to allow the processing of personal data. Those options are when: “(1) processing is necessary to satisfy a contract to which the data subject is a party, (2) you need to process the data to comply with a legal obligation, (3) you need to process the data to save somebody’s life (4) processing is necessary to perform a task in the public interest or to carry out some official function, or (5) you have a legitimate interest to process someone’s personal data” (Wolford, n.d.). Option number five, legitimate interest, is the most flexible of all the options but can be difficult to understand due to the limited definition. A general understanding of legitimate interest implies that data that can be stored and processed under the legitimate interest exception: has a clear benefit, has little risk of infringing on privacy, and is used in a way that data subjects may reasonably expect. The GDPR specifically allows use of the legitimate interest exemption in advertising (GDPR, 2016). But the extent to which data can be stored and processed for advertising depends on the legal interpretation of what a reasonable expectation of that data usage is.

The GDPR can restrict the ability to microtarget voters in political campaigns by allowing data subjects to review and retract their data, therefore, weakening voter profiles and targeting models and making comprehensive targeting less effective. Another way in which the GDPR limits targeting is via storage limits for data. Though there is no official limit on how long data can be stored, data storage must be justified by the use of the data and must consider the legal requirements and limitations for the data (GDPR, 2016). There are only two ways to maintain data without adhering to a data limit. Firms must either anonymize the data or justify that it is being kept for public interest, research or statistical purchases (GDPR, 2016). In specific regard to political parties, the GDPR restricts the storage of data to users who: are members, are former members, or people who have regular contact with the party. There are also additional stipulations that require



‘appropriate safeguards’ of information. Again, these restrictions are unclear due to the lack of clear definition of regular contact and appropriate safeguards, leaving room for interpretation and therefore added risk to the consumer. Any room for interpretation can be seen as room for manipulation, users will always bend the rules to their best interest which is why clarity is so important in these matters.

The ePrivacy Directive is an older data privacy document that also has implementations in European data protections which maintains that communications online reflect fundamental human rights (Digital Privacy, 2021). One of the main protections of the ePrivacy Directive is the insurance that users must grant permission before cookies are collected online. Additionally, the European Commission adopted a proposal for an ePrivacy Regulation to replace the Directive in 2017. One of the concepts introduced by the ePrivacy Regulation is the concept of regulation by design, which allows you to select from multiple levels of privacy protection from high to low privacy (Digital Privacy, 2021). European telecom lobbyists warn that too much regulation on data collection will effectively destroy the European data economy which has led to conflict in passing this regulation (Christl, Kopp, and Riechert, 2017). European states are still negotiating the final draft of the ePrivacy Regulation, and it is not yet in force in 2021. However, it is anticipated to enter into force soon.

In fact, very recently, beginning on July 6th, 2021, Facebook has adjusted its cookie consent policy for users in the European region and evolved their prompt to contain two controls: “Our Cookies On Other Apps and Websites” and “Cookies from other companies.” These controls allow for users to decide whether “Facebook can record web and third-party app data received about them through its business tools” and whether “other companies can set or read cookies from their devices when using a Facebook product.” (How Updates to Our Cookies Consent Prompt and Privacy Controls in Europe May Affect Your Ads and Reporting, n.d.). These are a good representation of regulation by design and offer powerful options for European users on Facebook. These changes may have a substantial impact on advertising on the Facebook platform. In the Business Help Center article announcing this update Facebook warns advertisers that they may see decreased performance in their advertisements as audiences decrease over time. This move towards autonomy over data was prompted by evolving policy rules in Europe and specific mention of “updated regulatory guidance on the ePrivacy Directive.” (How

Updates to Our Cookies Consent Prompt and Privacy Controls in Europe May Affect Your Ads and Reporting, n.d.)

The European Commission has also proposed a Digital Services Act (DSA) in tandem with the Digital Markets Act (DMA) in order to update and unify European Regulation on digital services (The Digital Services Act Package, 2021). The DSA and the DSM have two main goals (1) “To create a safer digital space in which the fundamental rights of all users of digital services are protected” and (2) “to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally” (The Digital Services Act Package, 2021). The DMA is proposed to address the lack of competition in digital markets and applies to platforms with 45 million or more monthly active users. The DSA is being focused on consumer protections and transparency and therefore impacts a larger number of stakeholders (Jaurisch, 2020). The DSA is more likely to address concerns of privacy in advertisements than the DMA and therefore is more relevant to this paper’s focus. An impact assessment of the DSA published by the EC states that “The goal of that directive is to allow borderless access to digital services across the EU and to harmonize the core aspects for such services, including information requirements and online advertising rules, as well as setting the framework for the liability regime of intermediary services.” Development of the DSA offers the most opportunities for specific and expanded protections against targeted political advertisements. The European Commission also seeks to address transparency issues, specifically listing “User-facing transparency of online advertising” as a new obligation under the DSA (The Digital Services Act: Ensuring A Safe And Accountable Online Environment, n.d.). As the DSA is still a proposal and is being actively developed many see this as an opportunity to determine clear and direct regulation of advertising and is an indication of the continued development of European data protections.

Germany also has its own country-specific digital regulations beyond the protections provided by the EU through the Interstate Media Treaty (Medienstaatsvertrag – “MStV”) which was ratified by all 16 states in October of 2020 and entered into force in November of 2020. This document was an overhaul of the previous German Interstate Broadcasting Treaty and has a wider scope to include modern-day broadcasting techniques like internet advertising. The MStV addresses several different aspects of

online media including user interfaces, media platforms, and video advertising. This is a large expansion of media oversight in Germany and has been aimed to cover the digital realm, “the new German State Media Treaty will not only govern the broadcasting of “classic” television and radio services but also new forms and formats of communication and broadcasting, such as video-on-demand services, social media platforms, app stores, search engines, user-generated content and blogging portals as well as electronic language assistants and news aggregators” (The New German State Media Treaty - Legal Requirements on Telemedia, 2020). This expansion of scope will allow more regulation of online targeting by limiting the use of psychographic profiling.

The MStV includes a few specific regulations that may directly impact political advertising online. For example, social media platforms are required to ensure transparency by disclosing “the criteria of access and deletion of content on a media intermediary and disclosure of the central criteria of the aggregation, selection and presentation as well as on the weighting of content” and “information on the functioning of the algorithms used and (significant) respective modifications” (The New German State Media Treaty - Legal Requirements on Telemedia, 2020). This allows for more transparency in targeting and may therefore limit targeting methods that may be more extreme or personal. This treaty comes as one of the first of its kind and signals the government's willingness to take on big tech firms. As this is a relatively new regulatory document we are still waiting to see if it is seen as successful in the long term, but it does continue the German tradition of strong data protections. Two major concerns of the document are the vagueness of terms and specificities on items such as discrimination and the possibility of censorship. The success of the treaty will depend on how clearly rules can be defined to platforms and how strictly they are enforced (Nelson and Jaursch, 2020).

## 6.2. United States

The United States has a much more relaxed history with data protections. They do not have an official definition of profiling or an overarching data protection policy. Instead, companies are mostly left to self-regulate and data policies are more prevalent at the state level. Based on this limited regulation, the United States has been a hotspot for targeting scandals in the last decade and has been a testing ground for tactics that spread around the world. A majority of the regulations related to data protections in the US are limited or are aimed more closely towards traditional forms of media. We see a combination of sector-specific laws, state legislative laws, and industry-specific laws as our legal framework for data collection (Rieke et al. 2016). These offer minimal protections in the digital sphere and have allowed for the flourishing microtargeting industry that is present in the United States today.

Only three of fifty states, California, Nevada, and Virginia, have enacted comprehensive data privacy laws, and only two states California and Vermont have enacted laws that pertain directly to data brokers. However, we do see that initiatives are increasing at both the state and federal levels indicating that this issue is becoming more or a focus for legislators and indicating possible future development in this sphere. Though few states have successfully passed data protection laws we do see an increase in discussion and votes on these types of issues. As of 2020, there are 16 states that have data protection laws of some sort, and 30 states and Puerto Rico have considered some sort of data privacy laws (202 Consumer Data Privacy Legislation, 2021). These laws differ drastically across states and less than half of US states are protected by them creating significant gaps at the state level.

California has the most comprehensive data protection policy, the California Consumer Privacy Act (CCPA) which was enacted in 2020. The CCPA allows for consumers to opt out of data collection for sales purposes and guarantees access to data collected by a company and the right to deletion if necessary. Additionally, the CCPA is being reinforced by the California Privacy Rights Act (CPRA) in 2023. The CPRA defines 'sensitive personal data' and allows for users to opt-out of data collection altogether (Clark, 2021). This helps close a loophole in data collection, where data was not being sold externally but was still being used to target individuals within the collection site and will impact prominent data collectors like Google and Facebook. Additionally,

the CCPA defines data brokers as “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship” (California Consumer Privacy Act, 2018). Data brokers are required to register with the attorney general and their practices are recorded and monitored. Although California seems to be taking major steps to combat data exploitation the rest of the United States still sees minimal protections.

Another state that has instituted stronger data protections is Washington, which has disclosure regulations in place that require a level of disclosure that Facebook has not been able to fulfil. Instead, they have limited advertisements in the state of Washington. Facebook states: “Ads must not run in or be targeted at the state of Washington when the ads relate to Washington's state or local elected officials, candidates, elections or ballot initiatives. In addition, ads must not run in or be targeted at the state of Washington when the ads relate to Seattle legislation” (Ads About Social Issues, Elections, or Politics, n.d.). This case draws attention to the limits that can arise in advertising when there is no overarching standard, states with more stringent advertising requirements can be excluded from the political advertising space altogether. This creates an environment where it is disincentivized to pass regulatory policy because states who do so are removed from the system. Therefore, giving those who oppose data protection a reason to oppose these mandates. A broader country wide mandate may be a solution to these situations of state-based exclusion allowing for protection for a larger group would incentivize platforms to comply as opposed to limit service as limiting would have more impact on profits at a larger scale. Based on the general policy trends in the United States it is likely that we will see more states adopt data privacy legislation in the coming years.

Federal regulation proposals have been increasing as well. In March of 2021, Congresswoman Suzan DelBene proposed a new national data privacy law. Congresswoman DelBene indicated that passing a law at the national level was becoming increasingly important as more states began to create their own data privacy laws and that creating one overarching law was important to avoid patchworking and difficulty in application (2021). Creating continuity in this field is important for both platforms and consumers as it will offer the most seamless experience from ad creation to ad presentation. Additionally, the Honest Ads Act was proposed in 2017 by US Senator's Mark Warner, Amy Klobuchar, and Lindsey Graham. This Act was proposed to decrease

foreign interference in online election advertising but would be applicable to online advertising as a whole. In the summary of the proposal posted on Senator Mark Warner's website three points are highlighted: (1) including digital advertisement in the Bipartisan Campaign Reform Acts definition of 'electioneering communication', (2) requiring digital platforms with 50,000,000 monthly visitors or more to maintain a public data set of all electioneering communications containing a copy of the advertisement, targeting data, number of views, publication data, advertisement rates, and contact information of the purchaser, and (3) requiring platforms to make a reasonable effort to ensure foreign actors do not purchase advertisement to influence American voters (Warner, 2019). Having access to a public data set of targeting data would be a very influential tool to monitor targeting. Facebook made the first announcement of their advertisement archive in the days following the proposal of this act followed soon after by Google. Some have seen these archives as a tactic to push off official regulation and instead self-regulate, though Facebook has made comments to the contrary (Leerssen et al., 2018). The targeting data presented in the existing ad archive structures is not shared to the extent that would have been required by the Honest Ads Act. The bill gained little traction in 2017 but was reintroduced in 2020, it is yet to be seen if the bill will become law in the future.

The United States Federal Trade Commission has the widest jurisdiction over commercial entities. This jurisdiction has been used to protect online consumers from unfair data and privacy practices. The FTC enforces privacy laws and mechanism for enforcement in the US (FTC, 2021). Included in this jurisdiction is the right to investigate companies for violating consumer privacy by improperly collecting, using, sharing, or improperly protecting users' data (FTC, 2021). To date all cases brought against social media platforms have been prosecuted by the FTC. FTC section 5(a) protects against "unfair or deceptive acts or practices in or affecting commerce" and is the main source of the FTC's authority (FTC, 2021). Using this authority the FTC has prosecuted hundreds of data protection cases and has called on the US Congress to create additional privacy and data security legislation enforceable by the FTC (FTC, 2021).

Two of the FTC's major data collection and privacy cases were directly related to targeted advertising and microtargeting. The first was a case with Facebook that was settled in July of 2019 for a \$5 billion dollar penalty. In a July 2019 Privacy & Data

Security Update provided by the FTC, they summarized the case as follows: “The complaint alleged that Facebook violated the Commission’s 2012 order against the company by misrepresenting the control users had over their personal information and failing to institute and maintain a reasonable program to ensure consumers’ privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users” (Federal Trade Commission, 2020). The second was a law enforcement action against Cambridge Analytica. This action was summarized by the FTC as follows: “The FTC’s complaint alleged that Cambridge Analytica, Nix, and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voter profiling and targeting” (Federal Trade Commission, 2020). In this case, the FTC Commission filed a default judgment in which they asserted that Cambridge Analytica violated the FTC Act through deceptive conduct. This order created more regulatory obligations for Facebook in the future and made attempts to create more protection for the data of users (Hu, 2020). However, it does not create any added protections for users against the algorithms and AI which were used by Cambridge Analytica to target voters. These cases have helped to establish the FTC as the enforcer of privacy and data protection cases but still leave room for growth in protecting the freedoms of voters and democracy.

Additionally, US citizens receive some protection from older data regulations that prohibit certain data collection and dispersion such as the US Privacy Act (1974), Health Insurance Portability and Accountability Act (1996), Children’s Online Privacy Protection Act (1998), and the Gramm-Leach Bliley Act (1999). These acts are focused around sensitive data such as disability data, data of children, and health data and less focused on the general data a user produces while online. The variety of frameworks provided at the state and national levels make US data regulations hard to interpret for both consumers and companies online. Yet, despite the clarity it could bring, many media platforms opt for self-regulation techniques as opposed to creating an overarching policy at the national level (Ruohonen, 2020).

### **6.3. Opt-Out vs. Opt-In & the Privacy Paradox**

The way in which a choice is presented matters greatly to the outcome. When it comes to opting in vs option out of data collection the preselected option holds an important place in determining what data is collected. One of the major differences between the United States and Germany's data collection legislation is the opt-out vs opt-in models. In Germany, we see the opt-in model for data collection that requires you to turn on cookies and tracking. Based on this model consent must be freely given and therefore users must turn on the tracking themselves. The US has an opt-out system, in which there is no federal law that requires consent before data collection (Crain and Nadler, 2019). A representative survey of public attitudes and actions in Germany and the US indicated that in both countries 82% of citizens claimed to be somewhat or very concerned about their data privacy while only 59% of Germans and 62% of Americans adjusted their Facebook privacy settings, only 47% of Germans and 53% of American's changed their privacy settings on Google and 20% of Germans and 17% of Americans made no privacy adjustment on online platforms (Kozyreva et al., 2021). Based on this study the gap in acceptability is largest in Germany.

This inconsistency between people's privacy attitudes on the internet and their privacy behaviors has been deemed the 'privacy paradox'. This privacy paradox often shows us that actors might not be driven to act in their best interest despite indicating that they are aware of their best interest. However, we still see that when given the option to adjust advertising on online platforms less users take the additional time in effort than indicates they are concerned about data collection. Therefore, being required to opt-in is a stronger protectant than having to request to opt-out. This is also proven by the basic principle of nudging. Nudging is defined as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives" (Thaler and Sunstein, 2008). Nudging case studies, which review opt-in vs. opt-out programs, such as organ donor sign ups, have indicated that when offered two options if you are required to check the box to opt in you are less likely to do so, while if you are required to check the box to opt out you are also more likely to do so (Johnson and Goldstein, 2003).

Within the concept of nudging, we must examine choice architecture, the idea that the way in which a choice is presented to you impacts your decision-making process



(Thaler and Sunstein, 2008). Digital Nudging adds a new layer to choice architecture because of the flexibility of online design and the ways in which they can be adjusted to influence your decision making. In the case of data protections, it is often in the best interest of a company or site to collect your data, so they are incentivized to design a digital interface that is most likely to obtain your consent. Opting-in to data collection allows for sites to collect and use your data as they see fit and is one of the main contributors to the creation of psychographic profiles. Therefore, the opt-in vs. opt-out method is an important piece in combating the use of targeting, as opt-in regulation reduces the supply of targeting data (Crain and Nadler, 2019).

## **7. Overall Risks of Targeting in Political Advertising**

Targeting has always been a goal of advertisements. Finding the right audience for an advertiser's message is vital. Just as finding the right voters is important to a campaign. Targeting can be an asset to smaller campaigns or campaigns that aim to mobilize voters who might otherwise not have voted (Chester and Montgomery, 2017). However, the risks of targeting in political advertisements are most pronounced when they cross the line from mobilization to persuasion (Kreiss and Barrett, 2020). When advertisers become too powerful in influencing consumer opinions, consumers lose the power of freedom of choice. With increased investment in developing the data industry, personal data can become a means of monitoring trends and creating influence on an extreme degree. AI is used to produce and edit ads at quicker rates than ever before, algorithms decide what you see, and ads that have been designed to appeal to voters inner most personality can be used to manipulate or mislead them. The advancement of AI and the manipulative techniques that advertisers can employ are closely tied together. The imbalance of power between the advertiser and the consumer creates an environment where personal data can be weaponized against consumers, targeting weaknesses and unknown biases. This weaponization can have severe consequences in the political sphere and can be a threat to democratic frameworks (Crain and Nadler, 2019).

### **7.1. Algorithms and AI**

Political candidates have often used the tactic of appealing to voters on important issues, one of the earliest examples being John F Kennedy in the 1960s, who would use opinion data to shape his speeches. However, online personalization can be achieved at a large scale creating a more dangerous power (Turow et al., 2012). Instead of researching the masses, the introduction of AI allows for unprecedented research at the individual level. AI has played an increasing role in political campaigns and advertising alike. Algorithms help serve the best advertisements to the most applicable voter by taking advantage of the large amount of data provided by the digital consumer and comparing and contrasting data markers to predict outcomes and monitor trends. When powered by AI, advertisement tailoring adjustments are made so quickly and efficiently that they can be misrepresentative to voters. Through algorithms and machine learning, AI can review

enormous amounts of information far beyond the scope of a standard human review and make educated guesses about how an audience will respond to an advertisement.

An example of an advanced AI technique is A/B testing. A/B testing is a tactic in which an audience is presented with two or more versions of the same online product to determine which product receives a better response (International IDEA, 2018) (Crain and Nadler, 2017). This type of advertising experimentation in the extreme can constitute "sending out hundreds of thousands of slightly different versions of the same message to different population segments to test patterns in their responses, such as how quickly they click, how long they stay on a page, what font and colour layout they like" (International IDEA, 2018). A/B testing uses machine learning algorithms to take in a variety of response factors and adjust accordingly. The 2016 Trump campaign ran up to 50,000 versions of advertisements per day to test responses and refine consumer ads going forward (Lapowsky, 2016). This level of personalization would not be possible without the introduction of AI into campaign advertising which allow multiple ads to be created and delivered at lower costs than traditional advertising and for responses to be recorded more easily. The effects of A/B testing, how and when consumers are being reviewed can be challenging to understand. Users may not realize what response they have to particular advertisements. When these responses are recorded and added to their psychographic profiles, they can lead to advertisements tailored to such a personal level that they are hard to ignore. When political advertisements use this tactic, they can identify what type of content a consumer or group of consumers is most likely to engage with—allowing advertisers to target them more effectively. This creates a higher risk of voters being exploited or manipulated by campaigns.

Additionally, algorithms often determine what advertisements are shown to consumers—creating the 'Algorithmic Filter Bubble' problem where users only see content targeted to them, creating a false sense of consensus or reality and leaving out the opinions and information that others might provide (Bakir, 2020). 'Algorithmic filter bubbles' also leave stakeholders outside of the bubble unaware of presented messaging, as ads are only shown to clusters of voters (International IDEA, 2018). Therefore, if a candidate is subject to a negative campaign advertisement there is a smaller chance of the opposition getting to respond to the ad or even knowing that it is out there. Another issue with algorithms is that they often boost more popular content. Boosted content can be

especially concerning when it amplifies radical and extreme ideas. This type of content is often boosted as it is most shocking and therefore engaged with more frequently (Kozyreva et al., 2021). Algorithms and AI have significant power over what a consumer sees, and yet they are not well understood by the public, creating an imbalance of power in advertising influence.

The use of algorithms in decision-making and planning has increased, and with it has come one of the risks of targeting in elections, the black box effect (Hu, 2020). A black box is "anything that has mysterious or unknown internal functions or mechanisms" (Black Box, 2021). To contextualize this in an online setting, think of how AI uses algorithms to collect inputs and produce an output such as a political advertisement targeted at a specific voter. It is challenging as a voter to figure out how the output is created and what inputs were used to get there. Predictive analysis is used to recognize patterns quickly and accurately in data and can then be used to adjust what is shown to a user in real-time (International IDEA, 2018). Predictive analysis creates an environment where the consumer is targeted based on their unconscious biases and trends beyond their comprehension. When voters cannot understand or even trace how decisions are being made for them, they are experiencing a black box effect.

## **7.2. Manipulative and Misleading Advertisements**

As profiling techniques have become more advanced and Artificial Intelligence has been introduced into the field, advertising has become smarter. Smarter advertisements are generally more persuasive to users and, therefore, more effective. Politicians have always used strong wording to attract voters. However, advertisements that are personally tailored to and targeted at a consumer have an increased chance of being manipulative or misleading. Persuasive communication can become manipulative when the goal is deception or reaction (Bakir, 2020). Manipulative and misleading advertising techniques are closely related and are not mutually exclusive and the range of intentions for these actions can be vast. Tactics that are used to persuade or dissuade voters are essential to examine in a political context especially when they are being targeted based on their personal data.

Microtargeted advertisements using psychographic profiles create a strong base of information to determine what issues and causes are valued by a consumer. Once these

core values are determined, they can be easily exploited by campaigns on a digital level creating advertisements that trigger a specific and calculated reaction from the audience (Nix, 2016). The ability to create unique variations at a mass scale allows for more voter persuasion. For example, suppose a campaign identifies that a particular issue, such as climate change, is significant to their targeted voter. In that case, political advertisers could selectively show the user ads that have stronger climate-related messaging. A concentrated amount of this messaging could mislead the audience to believe this issue is of high importance to the candidate even though it may not be (Dobber, Fathaigh, and Zuiderveen, 2019). Campaigns can implement these techniques across a vast range of voters, attempting to sway their votes. This technique can be misleading to voters as the advertisements may not accurately represent the candidate's values and priorities. Fueled by consumer data, campaigns know more about voters than they might realize. Therefore, opening the consumer up to more powerful techniques of persuasion.

Beyond misleading content, advertisements can create an active response from consumers based on many factors. They can be manipulative if they are targeting them based on their mood, personality, or traits. Psychographic profiles have been developed to track personality traits via emotional analytics. Famously Cambridge Analytica used a five-factor model to determine personality traits. This tactic was named OCEAN and reviewed five traits: openness, conscientiousness, extroversion, agreeableness, and neuroticism (Nix, 2016). These traits were assessed by collecting and reviewing enormous amounts of personal data and then using them to design advertisements that might best appeal to the user based on these underlying emotional conditions. The extreme data collection environment that has developed on the internet creates an atmosphere in which advertisers design campaigns around characteristics and traits that have not been self-disclosed (Crain and Nadler, 2019). Cambridge Analytica used the OCEAN technique to target vulnerability in people's decision-making based on their central personality traits. Through psychographic profiling emotional responses can be datified and used to manipulate consumers by targeting their personality. This technique is used by advertisers to drive behavior and to influence consumer actions or, in the case of elections, votes (Nix, 2016). With so much information about a consumer's decision-making, campaigns can manipulate voters' emotional reactions, making it is harder to make clear and independent choices.

Political advertising can also be used by actors, both foreign and domestic, to manipulate the perspective of individuals. Deceptive advertising is the highest on social media due to the low barrier of entry, low cost, and minimal fact-checking (Edelson et al., 2019). This type of manipulative advertising generally focuses on amplifying group-based identity threats to create behavior from their target audience (Crain and Nadler, 2019). These tactics target individuals' vulnerabilities in order to create influence (Crain and Nadler, 2019). Many of these campaigns aim to amplify existing pressure points in politics, leaning on existing resentments and anxieties to influence audiences (Bakir, 2020). Both persuasion and dissuasion techniques can be used in conjunction with psychographic profiling and microtargeting. Dissuasion is generally more controversial of the two options in online advertising because it creates more opportunities for manipulation through coercive advertisements. The level of personalization available in targeting negative advertisements has developed past your standard smear campaign. With the assistance of microtargeting individual voters can be delivered the negative advertisements of competing politicians that will affect them most personally. Persuasive advertisements are a more digestible idea to most consumers as politicians have always campaigned and tried to win your vote (Dobber, Fathaigh, and Zuiderveen, 2019). However, the risks of both methods need to be taken into consideration when reviewing the possible issues and the necessary protections for voters.

## **8. Self-Regulation from Media Sites**

Search engines and social media sites have taken strides to self-regulate in the backlash of targeted political advertising scandals. Self-regulation has been criticized as a last effort to fend off regulation from governments. Social media sites and browsers make a majority of their money from advertisements, and they are therefore incentivized to protect their ability to develop advertising tools as they wish. Self-regulation can leave users vulnerable to sudden changes or unknown risks as users do not have an advocate in the private sector. Due to the globalized nature of the internet, it is much easier for media sites to make their own restrictions than to have to take into account a multitude of restrictions based on their users' physical locations. However, as data protection policies continue to develop some sites, like Facebook, are requesting clearer guidelines from the government to alleviate some of their burden (Leathern, 2020). The most common tactics of self-regulation are requiring advertisers to register and creating advertisement archives to increase visibility and transparency into political advertisements that are displayed on their platforms. Yet we still see many varying policies and definitions in the political advertising sphere across platforms. There is a lack of standardization that can make rules and regulations confusing to consumers (Kreiss and Barrett, 2020). For example, when we compare definitions of political advertising across platforms, we see variations. See Figure 1. Google has the most specific definition indicating specific candidates, measures, initiatives, or propositions while Twitter and Facebook have broader definitions that include social issues and ads of any type made by political officials. Google is also the only site of the three that distinguishes between Germany and the United States when defining political advertisements.

Figure 1. Definitions of Political Advertising

What constitutes a political advertisement?		
Platform	United States	Germany
<b>Facebook</b>	Advertisements made by, on behalf of or about: a candidate for public office, a political figure, a political party, a political action committee or advocates for the outcome of an election to public office. Advertisements about: any election, referendum, or ballot initiative, including "get out the vote" or election information campaigns, any social issue in any place where the ad is being run, or Advertisements regulated as political advertising.	
<b>Google</b>	Ads that feature: A current officeholder, or candidate for an elected federal office including federal offices, current officeholders or candidates for a state-level elected office, or member of a state legislature, a federal or state level political party, a state-level ballot measure, initiative, or proposition that has qualified for the ballot in its state.	Ads that feature: a political party, a current elected officeholder, or candidate for the EU Parliament, a political party, a current officeholder, or candidate for an elected national office within an EU member state, members of a national parliament and presidents that are directly elected, a political party, a current officeholder, or candidate for an elected national office within an EU member state, members of a national parliament and presidents that are directly elected, a referendum question up for vote, a referendum campaign group, or a call to vote related to a national referendum or a state or provincial referendum on sovereignty.
<b>Twitter</b>	Content that references a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive, or judicial outcome. Ads that contain references to political content, including appeals for votes, solicitations of financial support, and advocacy for or against any of the above-listed types of political content, are prohibited under this policy. Ads of any type by candidates, political parties, or elected or appointed government officials.	
Sources: (Ads About Social Issues, Elections Or Politics, n.d),(Political Content - Advertising Policies, n.d) (Political Content, n.d.)		

### 8.1. Advertisement Archives/Libraries

Online advertisement is a vast market, selling more advertisements than traditional mediums, making them harder to monitor (Crain and Nadler, 2019). As political advertising online has become more controversial, advertisers like Facebook, Google, and Twitter have taken steps to address the transparency of what advertisements are posted on their platforms. In order to do this, each of the platforms has created its own collection of present and past advertisements. Advertisement archives were initially created to build transparency into campaign spending and offer some accountability to advertisers as others can see what they have posted (Leerssen et al., 2018). In the past advertisement, audiences were limited to the targeted audience, which created the filter bubble problem and limiting who could see and assess advertisements (Bakir, 2020). With the introduction of archives, the public, rival campaigns, and legislators can monitor political advertising when they deem necessary. The rules and regulations within these archives vary slightly between platforms, but the intention seems to be the same: creating accountability through transparency. Each of the platforms that we will discuss openly



references the importance of transparency in political advertising. Twitter is a special case because they instituted a ban on political advertising altogether. Reviewing the archives is an essential clue in understanding the shape and influence of political advertising online. The ad archives are created within the companies, and though they feature some similarities, they are not consistent across platforms.

### **8.1.1. Facebook**

Facebook's ad archive was launched in May of 2018 and included political advertisements published from that date forward in the United States; the ad archive has gradually expanded over time. Political advertisements in Germany are archived beginning April 2019. The Facebook ad archive includes advertisements run on Facebook, Instagram, Facebook Messenger, and Audience Network. The Facebook team has been very vocal about its commitment to transparency as the antidote to malicious advertising (Preparing for Elections, n.d.). Facebook allows access to all advertisements that are active at the time of the search, as well as ads about issues, elections, and politics that are no longer active. Special rules apply to advertisements that fall into the category of 'issues, elections, and politics.' Ads within this category are stored for seven years within the archive and can be searched by keyword or advertiser name. Search results can then be filtered or sorted by country, page name, status, disclaimer, and impressions. After selecting an ad, the viewer will be able to see additional information about the ad, including whether the account is active or inactive, if the ad has received a disapproved notice, a range of impressions, the amount spent on the ad, demographic information, geographic location of the audience shown the ad, and the platform that displayed the ad. The Facebook Ad archive also includes a spending tracker that allows viewers to compare the overall spending of advertisers who post advertisements within the issues, elections, and politics category. This feature allows a review of lifetime spending and last week's spending for each advertiser.

Facebook has developed a page within the About Facebook information specifically dedicated to how they are preparing for elections. This page lists four main actions: empowering voters, preventing interference, fighting information, and increasing transparency. The ad archive is listed as an act of transparency along with the election spending tracker. To highlight their commitment to transparency, Facebook states: "We

provide an industry-leading level of transparency around political advertising and pages so you can see who is trying to influence your vote” (Preparing for Elections, n.d.). The Facebook team further elaborates on the importance of transparency within their ad library use document, stating that: “[t]ransparency is a priority for us to help prevent interference in elections” (What is the Facebook Ad Library?, n.d.). Facebook does not limit the targeting of political advertisements. Instead, they indicated that they reached out to many stakeholders and determined that these tools were too crucial to NGOs, non-profits, political groups, and campaigns to reach key audiences. Therefore, targeting was not limited or removed (Leathern, 2020). They also indicate that through research they have conducted, “85% of spend by US presidential candidates on Facebook is for ad campaigns targeted to audiences estimated to be greater than 250,000” (Leathern, 2020). While these numbers are encouraging, it is still essential to understand and monitor the 15% of advertisements that fell into a smaller range. For context, in the 2020 presidential election in the United States, the winner was decided by just a 4.5% margin, and some Senate races were decided by less than 2%, which means that a small number of targeted advertisements could have a significant impact in this type of system. There was no information given in this context about the audience sizes in Germany or the EU. Facebook has also recently taken a strong stance against self-regulation, stating that “Ultimately, we don’t think decisions about political ads should be made by private companies, which is why we are arguing for regulation that would apply across the industry” (Leathern, 2020). They lean on accountability and transparency as a counter to malicious advertising techniques instead of limiting the ability to target users.

### **8.1.2. Google**

Google has created an ongoing Transparency Report that tracks Political Advertising on Google. The Transparency Report includes data from the US starting on May 31, 2018, and data from the EU beginning on Mar 21, 2019. The report collects advertisements purchased through Google Ads and Google Display & Video 360 that appear on Google, YouTube, and partner properties. The Transparency Report home page states, “Our goal is to provide greater transparency in political advertising on Google, YouTube, and partner properties. In order to help everyone understand the ads they see online, this report includes information about verified advertisers’ spending on ads related

to elections” (Political Advertising on Google, n.d.). The Transparency Report includes ads published by verified advertisers only. Verification processes differ by country but are fairly minimal. The United States requires advertisers to identify themselves as individuals or organizations and have a billing address in the United States to be verified (Election Advertising Verification, n.d.). Germany requires advertisers to identify themselves as individuals or organizations, verify that they are a registered organization, and have a billing address in the EU (Election Advertising Verification, n.d.). Within the Transparency Report, advertisements can be viewed overall or by selected countries searched by verified advertiser name. Once an ad is selected, viewers can see who paid for the ad, how long the ad ran, the amount spent, impressions, and ad format.

Additionally, this report is the only one that includes targeting information, and viewers can see if the ad was targeted towards a specific age group or gender and the locations in which the ad was broadcast. The Google support page indicates that targeting in political advertising is limited to the following information: “In locations where advertiser verification is required to run election ads, only the following audience targeting may be used for election ads: Geographic location (except radius around a location), age, and gender. Contextual targeting such as ad placements, topics, keywords against sites, apps, pages, and videos is also allowed” (Political advertising on Google FAQs, n.d.). The Transparency Report also allows viewers to search by the advertiser and see the total amount spent and all ads published by a specific advertiser on one page. Following the rollout of the GDPR, Google committed to complying and made updates to its consent policy, its third-party ad services, and its data collection, retention, and deletion controls (Helping advertisers comply with the GDPR, n.d.). These controls were mainly created as tools to help advertisers comply with the new regulations. They specified clearly in their Google Ads Data Protection Terms: Service Information which Google Ad’s services fall under data controller services and fall under data processing services.

### **8.1.3. Twitter**

In November of 2019, Twitter banned all political content in advertisements stating that “Twitter globally prohibits the promotion of political content. We have made this decision based on our belief that political message reach should be earned, not bought” (Twitter, n.d.). Therefore ads that reference any political messaging categories are prohibited. Special mention is made to solidify the ban on appeals for votes, solicitations of financial support, and advocacy for or against political content (Twitter, n.d.). Twitter has an archived tracker of political advertisements that includes political ads run from May 2018 to November 2019 and issue advertising from August 2018 to November 2019. Despite this ban on political advertising, Twitter is still viewed by many as a highly political platform, and there is still a large amount of political content and messaging through personal and campaign accounts (Jungherr, 2016). However, these messages cannot be boosted or placed in users’ feeds via payment; they must be spread via the traditional platform system, likes, and retweets. Twitter is the first central platform to ban all political advertising and gives an interesting view into one of the many options available to mandate political advertising. Removing political advertising content is a stance that has faced criticism as online political advertisements are seen as a cheaper option for political actors to speak, allowing the most significant amount of participation from candidates (Kreiss and Barrett, 2020).

## **8.2. Shortcomings of Ad Archives**

Advertising archives are a great step towards transparency; however, they are not a perfect solution and could use further development. Leerssen et al. highlight three main areas of criticism in ad archives: (1) scope, (2) verification, and (3) gaps in targeting data (2018). Scope issues arise based on differing definitions of what constitutes a “political advertisement” or a “social issue” and how hard it can be to examine these ads on a large scale. Verification can be an issue when ad buyers seeking to misrepresent themselves are included in archives. The existing requirements for registering as a political advertiser online make it possible for users to register incorrectly or to represent themselves as someone else falsely. Finally, and most relevant to this paper is the lack of proper identification of targeting data used in advertisements. For example, viewers cannot see the exact targeting categories used for a specific advertisement on the Facebook or Google

archives at this time. Google shows limited targeting data (age, gender, location), and Facebook only shows actual audience characteristics. Adding comprehensive targeting data would be extremely helpful in allowing users to see how or why they might be being targeted.

Additionally, the lack of homogeneity between different advertisement archives and the lack of data usability makes overarching analysis difficult. Ad archives can be hard to view in bulk, and trends can be hard to ascertain. As API features for data analysis have been released slowly, they have been filled with bugs, and usability has been challenging to manage (Leerssen et al., 2018). As an individual user, ad archives can be overwhelming and hard to navigate. Consumers cannot view the ads that they have seen or the criteria from their profile that may have sent an advertiser to them. There have been efforts to collect targeting data through private sources such as the NYU Online Political Transparency Project. This project developed a plugin called the Ad Observer that collects advertisements across platforms and compiles them based on the user's self-identified characteristics of the plugin user. They developed this tool to collect a more comprehensive archive stating that targeting data was vital and absent from existing ad libraries (Ad Observer, 2021). This tool gives some interesting insight into more significant targeting trends by allowing users to volunteer their own personal data.

However, as it has been created based on the users who download the plugin, it is not a holistic picture of the issue (Ghosh, Venkatadri, and Mislove, 2019). There is likely some inherent bias based on who is willing to download the plugin, who is aware of the project, and who is concerned about this issue. There would also be an added benefit of creating a uniform set of advertisement characteristics to be collected across platforms to make bulk comparisons easier on a large scale. If all the data can be compared, results are less likely to be biased and more likely to show trends across platforms. Additionally, and most importantly, we must recognize that while the existing advertisement archives are helpful, there is no guarantee that platforms will continue to make them available or develop them further to create more user-friendly interfaces. Regulating these archives could be an essential step in ensuring reliable long-term access to advertising data in Germany and the United States.

## **9. Examining Ad Archive Data**

Ad archive data gives the most information that is currently available for examining political advertisements and targeting online. Within this section, we will review advertisement archive data from both Facebook and Google. As Facebook does not give access to the selected targeting characteristics, we will only examine that archive from a spending perspective. The Google Archive does include some targeting data that we will analyze to assess targeting trends in Germany and the US. When reviewing this data, it is important to remember its limitation. For example, the advertisement archives are new, only being created in 2018. The limited data makes it hard to examine what occurred, for example, before the GDPR, which required compliance in May of 2018 when Google's transparency report was only created in May 2018. Data from the EU only began being archived in March of 2019. That being said, the data gives us the best inside look into how targeted advertising is being used in real cases.

### **9.1. Examining Ad Archive Data**

Facebook's Ad Library tracks political advertising spending and is a good indicator for a partial spending count on political advertising campaigns. The Facebook Advertisement archive indicates that since spending began being tracked in Germany, April 2019 to the present day, June 2021, €42,515,918 has been spent on political advertising in Germany. For comparison, the United States ad archive, which began, May 2018 to June 2021, indicates that an astronomical \$2,623,119,129 has been spent on political advertising in the United States. Though advertisement spending is not distributed evenly over each day, determining the average dollar spent per day can help to visualize how much money is being spent overall. Based on the 870 days the German archive has been active, and the 1,150 days the US archive has been active this breaks down to an average of approximately \$62,496 (€52,684) being spent on political or social issues advertisements on Facebook per day in Germany and approximately \$2,280,973 per day in the United States (Ad Library, n.d.). When adjusted to a per capita value to account for the difference in size in Germany (83,240,525 people) and the US (329,484,123 people), based on populations provided by the World Bank, we see that approximately \$.000075 spent per capita per day in Germany compared to approximately \$.007 per capita per day in the US (2021). This indicates a much larger spend in the

United States than in Germany at just over 93 times the money spent per capita in a given day.

Additionally, I reviewed the top 10 all-time spenders in the Facebook Advertisement Archive (excluding Ads by Facebook or Instagram), which revealed some trends regarding the types of candidates who run political advertisements and their average cost per ad. To analyze this data, I downloaded the political advertising Spending Tracker data for Germany and the United States, this tracker includes the name of the advertiser, the disclaimer attached to the advertisements, the all-time spend amount for the advertiser, and the number of ads in the ad library that belong to the advertiser. In the United States, thirteen of the top fifteen advertisers were presidential candidates, vice presidential candidates, or political parties. In Germany, of the top fifteen advertisers, there were only two political parties. In the United States, the minimum average spend per advertisement was \$91.98, and the maximum was \$5,640.52, while the average was \$1,322.33 per advertisement. The highest number of advertisements per advertiser was 312,233, the lowest number was 4,286, and the average was 88,083. For comparison Germany's minimum average spend per advertisement was \$25.19 (€21.35), the maximum was \$4,247.89 (€3,600.56), while the average was \$1056.57 (€895.56) per advertisement. The highest number of advertisements per advertiser was 19,564, the lowest number was 177, and the average was 2,694. These numbers show us that the average spend per advertisement is relatively similar in both countries; however, the number of ads created by each advertiser is much higher in the United States. This may indicate more targeted advertisement as more ad variation means ads can be tailored to different audiences.

Figure 2. Top Advertising Spenders of All Time  
Data Source: (Ad Library, n.d.)

United States				
Page Name	Type	Amount Spent (USD)	Number of Ads in Library	Average Spend Per Ad
Mike Bloomberg	Presidential Candidate	\$ 63,326,402	181197	\$ 349.49
Donald J. Trump	Presidential Candidate	\$ 58,272,160	312233	\$ 186.63
Joe Biden	Presidential Candidate	\$ 55,442,795	58474	\$ 948.16
Joe Biden	Presidential Candidate	\$ 43,888,905	49550	\$ 885.75
Donald J. Trump	Presidential Candidate	\$ 33,246,876	301740	\$ 110.18
Stop Republicans	Political Party	\$ 26,007,849	6052	\$ 4,297.40
U.S. Census Bureau	Government	\$ 24,175,282	4286	\$ 5,640.52
Tom Steyer	Presidential Candidate	\$ 15,944,762	4468	\$ 3,568.66
Team Trump	Presidential Party	\$ 15,150,395	47672	\$ 317.80
Donald J. Trump	Presidential Candidate	\$ 15,146,651	164843	\$ 91.89
GOP	Political Party	\$ 12,337,289	79898	\$ 154.41
Mike Pence	Vice Presidential Candidate	\$ 12,227,183	47978	\$ 254.85
Progressive Turnout Project	PAC	\$ 12,149,343	5791	\$ 2,097.97
Senate Democrats	Political Party	\$ 10,934,408	16445	\$ 664.91
Democratic Party	Political Party	\$ 10,818,588	40620	\$ 266.34

Germany				
Page Name	Type	Amount Spent (EUR)	Number of Ads in Library	Average Spend Per Ad
Bundesministerium für Gesundheit	Government	€ 2,065,186	5873	€ 351.64
Bundesregierung	Government	€ 1,889,601	905	€ 2,087.96
Greenpeace Deutschland	NGO	€ 1,399,795	1896	€ 738.29
European Parliament	Government	€ 1,112,988	1084	€ 1,026.74
Campact e.V.	Citizens Movement	€ 1,010,298	2592	€ 389.78
Bundesministerium für Arbeit und Soziales	Government	€ 891,794	1173	€ 760.27
Verbraucherhilfe24	Legal Services	€ 666,558	579	€ 1,151.22
Plan International Deutschland	Humanitarian Organization	€ 640,637	559	€ 1,146.04
Bayer	Pharmaceutical Company	€ 637,300	177	€ 3,600.56
LichtBlick	Energy Provider	€ 605,133	2121	€ 285.31
Fraktion DIE LINKE. im Bundestag	Political Party	€ 565,360	1107	€ 510.71
UNICEF Deutschland	Government	€ 498,527	908	€ 549.04
CDU	Political Party	€ 417,623	19564	€ 21.35
UNO-Flüchtlingshilfe	Government	€ 385,262	1060	€ 363.45
WWF Deutschland	NGO	€ 364,490	808	€ 451.10

## 9.2. Google 's Transparency Report

In order to examine relevant targeting trends, I downloaded all the available political advertisement ad archive data that Google has available between the beginning of the ad archive and June of 2021, which totaled more than 806,000 advertisements. From there, I reduced the data down to reflect only advertisements that were directed towards German or United States citizens. The data reflects far fewer ads, 43,592, directed towards German citizens compared to the 590,926 advertisements addressed towards US citizens. However, it should be noted that German advertisements were not being recorded until almost a full year after United States ads were being archived. As previously noted, Google allows targeting based on age, gender, location (included and excluded), and contextual targeting based on search terms, search history, etc. Any targeting based on contextual data was not included in the data set, and therefore only age, gender, and location targeting could be reviewed.

The most used targeting technique in each country was location included, and the analysis showed that 99% of ads delivered to German audiences used location included



targeting, and 97% of US ads included location targeting. Age and gender targeting are much more common in the US, with only 4% of German ads using targeting based on age and 4% based on gender compared to the US's 40% and 34%, respectively. It is also much more common in the US to exclude a location when targeting advertisements, with 24% of advertisements using this method compared to only 3% of German advertisements. This indicates that location targeting is by far the most used targeting technique in Germany, with minimal use of other targeting methods.

*Figure 3. Use of Targeting Features Overall*  
*Data Source: (Political Advertising on Google, n.d.)*

All Time			
<b>Age Targeting</b>			
	Targeted	Not Targeted	Percentage
Germany	1837	41755	4%
United States	238156	352770	40%
<b>Gender Targeting</b>			
	Targeted	Not Targeted	%
Germany	1570	42022	4%
United States	198035	392891	34%
<b>Location Targeting (Included)</b>			
	Targeted	Not Targeted	%
Germany	43357	235	99%
United States	572098	18828	97%
<b>Location Targeting (Excluded)</b>			
	Targeted	Not Targeted	%
Germany	1193	42393	3%
United States	140264	449795	24%

The year with the most advertisements for each country was the year of the last major election. In the United States, this was 2020, the year of the last presidential election. The last major federal election in Germany was in 2017, before the collection of advertisements for the advertisement archive; however, we do see a big jump in the number of new advertisements during the European Parliament elections in 2019. In Germany, 2019 resulted in more than 30,000 more ads than the following year, and in the United States, 2020 brought more than double the political advertisements than the year prior. These measures indicate the heavy investment in digital advertisements by campaigns in election years.

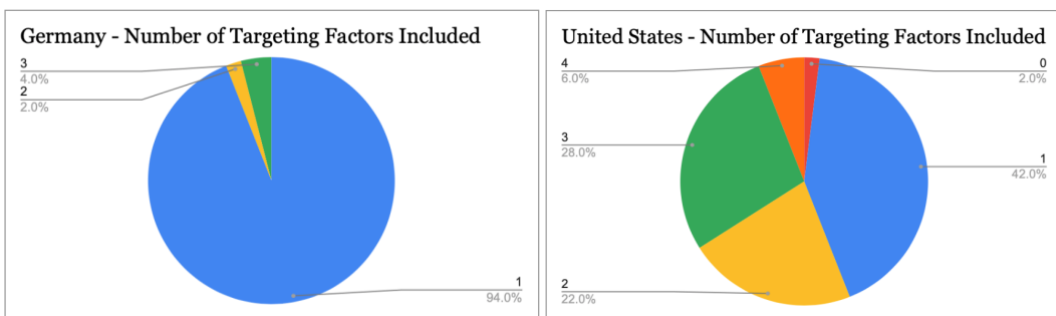
Figure 4. Number of New Ads Created Each Year – Election Years Shaded  
 Data Source: (Political Advertising on Google, n.d.)

New Ads Created Each Year					
	2018	2019	2020	2021	Total
Germany		38312	2823	2457	43592
United States	97148	152591	324321	16857	590917

Another interesting factor that was reviewed was the number of targeting factors used by each advertisement. In Germany, less than 1% of ads included no targeting, 94% of ads included one targeting measure, 2% included two, 4% included three, and less than 1% included all four measures. In the US, 2% of advertisements included no targeting, 42% of advertisements included one targeting measure, 22% of advertisements included two measures, 28% of advertisements included three, and 6% included all four measures. A more detailed breakdown of these features can be seen in Figure 5. It is interesting to note that even given these limited targeting features to examine, we can see that the United States is much more advanced in its targeting techniques, with 94% of Germany’s targeted advertisements featuring only one targeting measure, the most popular of which is location, the extremes of microtargeting seem less likely.

Figure 5. Percentage of Targeting Factors Used in Advertisements Overall  
 Data Source: (Political Advertising on Google, n.d.)

Number of Targeting Factors Included						
	0	1	2	3	4	Total
Germany	2	40895	1087	1538	70	43592
United States	12552	247067	129623	163629	38055	590926

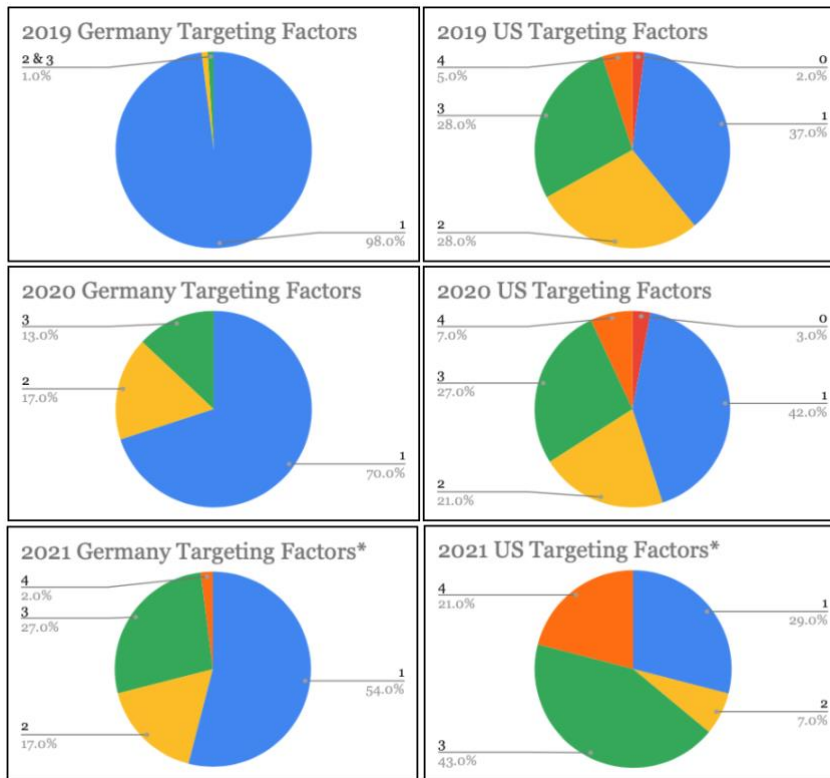


However, we see an increase in the number of targeting factors implemented in Germany and the US year over year. In 2019 we saw only 2% of advertisements in Germany using more than one targeting factor, which increases to 30% in 2020 and 46% in the first half of 2021, suggesting that more advanced targeting practices are becoming more common in Germany. Interestingly, in the US, we also see an overall increase in the

number of advertisements using all four targeting measures year over year, but in the election year 2020, we see a sizable increase in the percentage of advertisements that only use one targeting factor. See Figure 6.

Figure 6. Targeting Factors Used in Advertisements Per Year  
Data Source: (Political Advertising on Google, n.d.)

Number of Targeting Factors Included by Year					
2019					
Targeting Factors	0	1	2	3	4
Germany	0	37598	200	504	10
United States	2961	55945	42513	43444	7728
2020					
Targeting Factors	0	1	2	3	4
Germany	1	1973	474	364	11
United States	9115	134883	69377	86809	24137
2021 (Through June)					
Targeting Factors	0	1	2	3	4
Germany	1	1324	413	670	49
United States	4	4951	1150	7285	3467



\*Through June 30, 2021

The increase in the number of targeting trends used indicates that political advertisers in both countries are becoming more advanced at targeting. In Germany, the number of advertisers using more than one targeting feature increased from just 2% to 28% between 2019 and 2020 and has already jumped to 46% in the first half of 2021. In the US, the most advanced targeted advertisements, which use 3 or 4 of the offered

targeting categories, have increased from 33% of advertisements to 63% of advertisements between 2018 and the first half of 2021. It is important to note that these categories of targeting are the least protected categories of data and are more general targeting trends. However, these trends do indicate that despite increasing data protection policies, advertisers are still advancing their methods of targeting over time.

## 10. Conclusion

Targeting has become an important topic within election advertising regulation and data privacy realms over the past decade. With the introduction of AI and big data, targeting has become more advanced than ever before and creates an expanded risk to the voter. When looking at data protection policies in the digital sphere, it is important to highlight what protections exist and what protections need additional development. Both Germany and the US are on the cusp of more robust data protection. In Germany, the introduction of the MStV is likely to reshape how targeting is monitored, creating stronger protections against manipulative advertising by ensuring additional transparency. The DSA proposal has the ability to help in strengthening these protections if implemented. Additionally, as conversations and proposals around data protections increase in the US, more states are likely to follow in California's footsteps, passing more comprehensive data protection policies. The Honest Ads Act shows some promise in creating more protections for consumers and voters if it is passed. Targeting trends may change as policy continues to develop. That being said, the US has a long way to go to catch up to Germany in terms of data protection. Current regulations put US citizens at a much higher risk of weaponized targeting in election advertising.

The principal vulnerabilities of German data protection policies are unclear definitions and enforcement techniques. Definitions seem to be kept broad to allow for the widest interpretation of their meaning. While this may be an attempt to cover up loopholes, it can have the opposite effect by allowing advertisers to create their interpretations of the defined terms and wait for litigation to prove correct or incorrect. For example, the GDPR leaves gaps in coverage for inferred data which is an essential tool in targeting. Consent requirements differ based on several variables, and there are some gaps in coverage (Crain and Nadler, 2019). Protecting voter's inferred data is vital in restricting microtargeting in Germany as techniques continue to advance. Much of the data that falls into the inferred data category has to do with consumers' actions and reactions, not necessarily their inputs. With the use of psychographic development techniques, this data can give a lot of information on a voter, and therefore it must be protected. Germany's multi-party and multi-vote systems offer them some additional protections from manipulative targeting techniques as dissuading a voter is less powerful in the overall distribution of votes. However, it is important to remember that targeting

can also be used to spread polarizing ideas and create or advance social tensions. Ensuring German citizens are protected from weaponized targeting techniques is still and important issue.

In the US, self-regulation of media sites and advertisers has been the main framework of data protection. When reviewing the self-regulation of advertising platforms on political advertising, we must remember that these changes are not guaranteed. Site rules and regulations will likely change and evolve, and companies have their interest at the forefront instead of the well-being of the people. We also see that regulations set up by social media and search engines are vulnerable to the biases of the regulators (Crain and Nadler, 2019). In the current state, online advertising rules are published as a series of blog posts and press releases by platforms, and they can be challenging to track down and understand. While we can be grateful to these sites for implementing their own rules to protect elections, a legal framework must back up these initiatives to ensure the longevity of internet user protections. A comprehensive data protection policy is a crucial step necessary in protecting US voters from manipulation by targeting. Especially given their high-risk targeting factors such as the two-party system, which incentivizes both persuasion and dissuasion of voters, and the long history and development of targeting practices. Creating an overarching policy will help with enforcement and make a more straightforward implementation process for private enterprises. Models from the GDPR which will be essential to deterring political campaigns from using manipulative targeting techniques will be their data storage and use requirements, their right to be forgotten, and their opt-in model.

Upon close comparison of the advertisement archive data provided by Facebook and Google, we see that the top US advertisers are political candidates and parties who make a significant investment in developing many variations of advertisements to be run on Facebook. Germany's top advertisers in comparison are primarily government agencies that have many fewer advertisements in the library. The more significant number of advertisements in the US archive indicates that advertisers have more variety and are likely better prepared to target smaller groups of people. The Google Transparency Report indicated that Germany uses far fewer basic targeting features per advertisement than the US. We see that in practice, German political advertisements rely on fewer targeting characteristics even at the most basic level. Based on the limited use

of targeting at this level, it is unlikely that there is a large amount of predatory targeting in Germany. However, a review of this data did indicate that German political advertisers are using more targeting features year over year, indicating growth in political advertisement targeting in Germany. A review of this data following the 2021 elections in Germany would likely give a clearer picture to the advancement in targeted political advertising and is a possible future project to be pursued. Targeting trends indicate that Germany is advancing in their targeting techniques, therefore making data protections especially important to ensure that targeting does not pass over into the use of inferred traits or manipulation. Review of US data indicates that targeting techniques are already implemented frequently. Making the establishment of data protection policies especially important to the voter if targeting is to be restricted.

Germany and the United States offer very different data protection models for comparison. German citizens are well protected by policy that determines the data that can be collected, what it can be used for, and how it can be transferred. These features all have a great impact in restricting targeting as users have a lot more control over how and when their data can be collected. This minimizes the trading and sale of data and does not allow for the development of robust psychographic profiles that may then be used to target voters. Though there is still room for growth in defining exact protections and ensuring transparency in advertising, existing data protections in Germany do restrict the use of more advanced targeting methods. In the United States, voters have much less protection from data collection, use, and sharing. Individual states offer different protections and many of them offer no protections at all. With the exception of a few federal protections against sensitive data collection or the FTC's interpretation of what is unfair or deceptive to consumers, US voters are at the will of the self-regulation of media sites. Putting them at an extremely high risk for targeting. Data is critical to targeting and personal data protection policies are essential in protecting voters from weaponized targeting techniques.

## References

- Facebook.com. n.d. Ads About Social Issues, Elections or Politics. [online] Available at: <[https://www.facebook.com/policies/ads/restricted\\_content/political](https://www.facebook.com/policies/ads/restricted_content/political)> [Accessed 21 July 2021].
- Facebook Ad Library. n.d. Ad Library. [online] Available at: <[https://www.facebook.com/ads/library/?active\\_status=all&ad\\_type=political\\_and\\_issue\\_ads&country=US&media\\_type=all](https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=US&media_type=all)> [Accessed 21 July 2021].
- Ad Observer. 2021. Ad Observer. [online] Available at: <<https://adobserver.org>> [Accessed 21 July 2021].
- Google. n.d. Ad Settings. [online] Available at: <<https://adssettings.google.com/authenticated?hl=en>> [Accessed 21 July 2021].
- Alghizzawi, M., 2019. The role of digital marketing in consumer behavior: A survey. *Int. J. Inf. Technol. Lang. Stud*, 3(1), pp.24-31.
- Angwin, J., Mattu, S. and Parris Jr., T., 2016. Facebook Doesn't Tell Users Everything It Really Knows About Them. [online] ProPublica. Available at: <<https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>> [Accessed 21 July 2021].
- Bakir, V., 2020. Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting. *Frontiers in Communication*, 5, p.67.
- Bipartisan Campaign Reform Act Of 2002*. 2002. Vol. 2356. Washington D.C.
- California Consumer Privacy Act Of 2018*. 2018. Vol. 31427-327316. California.
- Cattaneo, Gabriella, Giorgio Micheletti, Mike Glennon, Carla La Croce, and Chrysoula Mitta. 2020. "The European Data Market Monitoring Tool". Luxembourg: Publications Office of the European Union.
- Chang, A., 2018. The Facebook and Cambridge Analytica scandal, explained with a simple diagram. [online] Vox. Available at: <<https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>> [Accessed 21 July 2021].
- Chester, J. and Montgomery, K.C., 2017. The role of digital marketing in political campaigns. *Internet Policy Review*, 6(4), pp.1-20.
- Christl, W., Kopp, K. and Riechert, P.U., 2017. Corporate surveillance in everyday life. *Cracked Labs*, p.6.
- Clark, K., 2021. The current state of US state data privacy laws. [online] The Drum. Available at: <<https://www.thedrum.com/news/2021/04/26/the-current-state-us-state-data-privacy-laws>> [Accessed 21 July 2021].
- Congresswoman Suzanne DelBene, 2021. DelBene Introduces National Consumer Data Privacy Legislation. [online] Available at: <<https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2740>> [Accessed 21 July 2021].
- Crain, M. and Nadler, A., 2019. Political manipulation and internet advertising infrastructure. *Journal of Information Policy*, 9, pp.370-410.



- Data.worldbank.org. 2021. Population, total | Data. [online] Available at: <<https://data.worldbank.org/indicator/SP.POP.TOTL>> [Accessed 21 July 2021].
- Digital Strategy EC. 2021. Digital privacy. [online] Available at: <<https://digital-strategy.ec.europa.eu/en/policies/digital-privacy>> [Accessed 21 July 2021].
- European Commission. n.d. The Digital Services Act: ensuring a safe and accountable online environment. [online] Available at: <[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment\\_en#what-are-the-next-steps](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#what-are-the-next-steps)> [Accessed 21 July 2021].
- Digital Strategy EC. 2021. The Digital Services Act Package. [online] Available at: <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>> [Accessed 21 July 2021].
- Dobber, T., Ó Fathaigh, R. and Zuiderveen Borgesius, F., 2019. The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4).
- Edelson, L., Sakhuja, S., Dey, R. and McCoy, D., 2019. An analysis of united states online political advertising transparency. arXiv preprint arXiv:1902.04385.
- Google Support. n.d. Election Advertising Verification. [online] Available at: <<https://support.google.com/adspolicy/troubleshooter/9973345#ts=9974014%2C10424610&zip%2Cverification-for-individuals%2Cverification-for-organizations>> [Accessed 21 July 2021].
- Eskens, S., 2019. A right to reset your user profile and more: GDPR-rights for personalized news consumers. *International Data Privacy Law*.
- EU Directive 2002/58*: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 p.37
- EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L119/1
- Facebook for Business. n.d. Facebook Advertising Targeting Options. [online] Available at: <[https://www.facebook.com/business/ads/ad-targeting?content\\_id=7ko93HYgrMsIy4k&ref=sem\\_smb&utm\\_source=GOOGLE&utm\\_medium=fbsmbsem&utm\\_campaign=PFX\\_SEM\\_G\\_BusinessAds\\_US\\_EN\\_Brand\\_Exact\\_Desktop&utm\\_content=Audience\\_Evaluating&kenid=\\_k\\_CjwKCAjw-qeFBhAsEiwA2G7NlwSu6WIe75trOzzd3zYAaK6Zhk4-05rAXY1091DRgTQfQrbJTRmSGBocmMEQAvD\\_BwE\\_k\\_&utm\\_term=facebook%20ad%20audiences&utm\\_ct=EVG&gclid=CjwKCAjw-qeFBhAsEiwA2G7NlwSu6WIe75trOzzd3zYAaK6Zhk4-05rAXY1091DRgTQfQrbJTRmSGBocmMEQAvD\\_BwE.](https://www.facebook.com/business/ads/ad-targeting?content_id=7ko93HYgrMsIy4k&ref=sem_smb&utm_source=GOOGLE&utm_medium=fbsmbsem&utm_campaign=PFX_SEM_G_BusinessAds_US_EN_Brand_Exact_Desktop&utm_content=Audience_Evaluating&kenid=_k_CjwKCAjw-qeFBhAsEiwA2G7NlwSu6WIe75trOzzd3zYAaK6Zhk4-05rAXY1091DRgTQfQrbJTRmSGBocmMEQAvD_BwE_k_&utm_term=facebook%20ad%20audiences&utm_ct=EVG&gclid=CjwKCAjw-qeFBhAsEiwA2G7NlwSu6WIe75trOzzd3zYAaK6Zhk4-05rAXY1091DRgTQfQrbJTRmSGBocmMEQAvD_BwE.)> [Accessed 21 July 2021].
- FCC, n.d. Political Programming. [online] FCC.gov. Available at: <<https://www.fcc.gov/media/policy/political-programming>> [Accessed 21 July 2021].

- FEC, n.d. Advertising and disclaimers. [online] FEC.gov. Available at: <<https://www.fec.gov/help-candidates-and-committees/advertising-and-disclaimers/>> [Accessed 21 July 2021].
- FEC, n.d. Understanding Ways to Support Federal Candidates. [online] FEC.gov. Available at: <<https://www.fec.gov/introduction-campaign-finance/understanding-ways-support-federal-candidates/>> [Accessed 21 July 2021].
- Federal Trade Commission, 2020. Privacy & Data Security Update: 2019. Washington D.C.: FTC, pp.1-18.
- FTC, 2021. A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority. [online] ftc.gov. Available at: <<https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>> [Accessed 21 July 2021].
- German Bundestag. n.d. Funding of Political Parties. [online] Available at: <<https://www.bmi.bund.de/EN/topics/constitution/funding-of-political-parties/funding-of-political-parties-node.html>> [Accessed 21 July 2021].
- Ghosh, A., Venkatadri, G. and Mislove, A., 2019. Analyzing political advertisers' use of Facebook's targeting features. In IEEE workshop on technology and consumer protection (ConPro'19).
- Google Support. n.d. Helping Advertisers Comply with the GDPR. [online] Available at: <<https://support.google.com/google-ads/answer/9028179?hl=en>> [Accessed 21 July 2021].
- Facebook. n.d. How Updates to Our Cookies Consent Prompt and Privacy Controls in Europe May Affect Your Ads and Reporting. [online] Available at: <<https://www.facebook.com/business/help/171174698192658>> [Accessed 21 July 2021].
- Hu, M., 2020. Cambridge Analytica's black box. *Big Data & Society*, 7(2), no. 2 (2020): 2053951720938091.
- IDC & Open Evidence. 2017. European Data Market. SMART 2013/0063. European Commission.
- International IDEA, 2018. Digital Microtargeting: Political Party Innovation Primer 1. International Institute for Democracy and Electoral Assistance, pp.1-28.
- Johnson, E.J. and Goldstein, D., 2003. Do defaults save lives?.
- Jungherr, A., 2016. Four functions of digital tools in election campaigns: The German case. *The International Journal of Press/Politics*, 21(3), pp.358-377.
- Kozyreva, A., Lorenz-Spreen, P., Hertwig, R., Lewandowsky, S. and Herzog, S.M., 2021. Public attitudes towards algorithmic personalization and use of personal data online: evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, 8(1), pp.1-11.
- Kreiss, D. and Barrett, B., 2020. Democratic Tradeoffs: Platforms and Political Advertising. *Ohio St. Tech. LJ*, 16, p.493.
- Kruschinski, S. and Haller, A., 2017. Restrictions on data-driven political micro-targeting in Germany. *Internet Policy Review*, 6(4), pp.1-23.
- Lapowsky, I., 2016. This Is How Facebook Actually Won Trump The Presidency. [online] *Wired*. Available at:<<https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/>>

- Leathern, R., 2020. Expanded Transparency and More Controls for Political Ads. [online] About.fb.com. Available at: <<https://about.fb.com/news/2020/01/political-ads/>> [Accessed 20 July 2021].
- Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N. and de Vreese, C.H., 2018. Platform ad archives: Promises and pitfalls. *Internet Policy Review*, 8(4).
- Lindsay, J., 2020. The 2020 Election by the Numbers. [Blog] Water's Edge, Available at: <<https://www.cfr.org/blog/2020-election-numbers>> [Accessed 20 July 2021].
- McMinn, S., Hurt, A. and Talbot, R., 2020. Money Tracker: How Much Trump And Biden Have Raised In The 2020 Election. [online] Npr.org. Available at: <<https://www.npr.org/2020/05/20/858347477/money-tracker-how-much-trump-and-biden-have-raised-in-the-2020-election>> [Accessed 21 July 2021].
- Merriam-Webster.com Dictionary, s.v. Black Box. accessed July 20, 2021, <https://www.merriam-webster.com/dictionary/black%20box>.
- National Conference of State Legislatures. 2021. 2020 Consumer Data Privacy Legislation. [online] Available at: <<https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx>> [Accessed 21 July 2021].
- Nelson, M. and Jaurisch, J., 2020. Germany's new media treaty demands that platforms explain algorithms and stop discriminating. Can it deliver? - AlgorithmWatch. [online] AlgorithmWatch. Available at: <<https://algorithmwatch.org/en/new-media-treaty-germany/>> [Accessed 21 July 2021].
- Bloomberg News, 2020. The Nine Types of Voters Who Will Decide 2020. [online] Bloomberg.com. Available at: <<https://www.bloomberg.com/features/2020-election-voter-profiles>> [Accessed 21 July 2021].
- Nix, Alexander. 2016. Cambridge Analytica - The Power Of Big Data And Psychographics. Video. New York: Youtube.
- OECD, 2013. Exploring the economics of personal data: a survey of methodologies for measuring monetary value. OECD Publishing.
- Palese, M., 2018. How does proportional representation work in Germany?. [online] Electoral-reform.org.uk. Available at: <<https://www.electoral-reform.org.uk/how-does-proportional-representation-work-in-germany/>> [Accessed 21 July 2021].
- German Bundestag. n.d. Parliamentary Groups. [online] Available at: <<https://www.bundestag.de/en/parliament/groups?url=L2VuL3BhcmxpYW11bnQvZ3JvdXBzL2dyb3Vwcy1kaXN0cmliidXRpb24tMTk3NjQ0&mod=mod487054>> [Accessed 21 July 2021].
- German Bundestag. n.d. Party Funding. [online] Available at: <[https://www.bundestag.de/en/parliament/function/party\\_funding](https://www.bundestag.de/en/parliament/function/party_funding)> [Accessed 21 July 2021].
- Transparencyreport.google.com. 2021. Political advertising on Google. [online] Available at: <<https://transparencyreport.google.com/political-ads/home>> [Accessed 20 July 2021].
- Google Support. n.d. Political advertising on Google FAQs - Transparency Report Help Center. [online]

Available at:

<<https://support.google.com/transparencyreport/answer/9575640?hl=en#zippy=%2Cwhich-advertisers-are-included-in-the-political-advertising-transparency-report%2Cwhy-are-you-publishing-a-report-about-political-advertising%2Cwhich-products-are-represented-in-the-political-advertising-transparency-report%2Cwhy-are-some-advertisers-mentioned-multiple-times-in-the-top-advertiser-table%2Cwhy-am-i-seeing-ads-paid-for-by-multiple-advertisers-in-the-transparency-report%2Cin-the-eu-report-why-do-some-advertisers-appear-on-multiple-country-pages%2Cwhere-can-i-see-additional-disclosures-for-california-political-ads%2Cwhere-did-ads-in-the-report-appear%2Cwhy-cant-i-see-the-content-of-some-ads-in-the-report%2Cchow-was-the-report-modified-after-the-united-kingdom-left-the-european-union%2Cwhat-targeting-criteria-can-be-used-for-election-ads>> [Accessed 20 July 2021].

Facebook. n.d. Preparing for Elections. [online] Available at:

<<https://about.facebook.com/actions/preparing-for-elections-on-facebook/#increasing-transparency>> [Accessed 21 July 2021].

Privacyrights.org. 2021. Data Brokers | Privacy Rights Clearinghouse. [online] Available at:

<<https://privacyrights.org/data-brokers>> [Accessed 21 July 2021].

Revella, A., n.d. Psychographics and personas: how to get to the truth about why people buy. [Blog]

Hotjar, Available at: <<https://www.hotjar.com/blog/psychographics-in-marketing>> [Accessed 21 July 2021].

Rieke, A., Yu, H., Robinson, D. and Van Hoboken, J., 2016. Data brokers in an open society.

Ruohonen, J., 2020, October. A Dip Into a Deep Well: Online Political Advertisements, Valence, and European Electoral Campaigning. In *Multidisciplinary International Symposium on Disinformation in Open Online Media* (pp. 37-51). Springer, Cham.

Schultheis, E., 2013. In Germany, one TV ad per candidate. [online] POLITICO. Available at:

<<https://www.politico.com/story/2013/09/germany-elections-one-tv-ad-per-candidate-096770>> [Accessed 20 July 2021].

Simmons-simmons.com. 2020. The new German State Media Treaty - legal requirements on telemedia.

[online] Available at: <<https://www.simmons-simmons.com/en/publications/ckdhmlhufqy9g09265hhz6tw1/the-new-german-state-media-treaty---legal-requirements-on-telemedia>> [Accessed 20 July 2021].

Spencer, S., 2019. An Update On Our Political Ads Policy. [online] Available at:

<<https://blog.google/technology/ads/update-our-political-ads-policy/>> [Accessed 21 July 2021].

Statista. 2021. Breakdown of CDU expenditures Germany 2019. [online] Available at:

<<https://www.statista.com/statistics/957344/expenditures-political-party-cdu-germany>> [Accessed 21 July 2021].

Thaler, R. and Sunstein, C., 2008. *Nudge*. New Haven: Yale University Press.

Turow, J., Delli Carpini, M.X., Draper, N.A. and Howard-Williams, R., 2012. Americans roundly reject tailored political advertising.

Twitter., n.d. Business Twitter. n.d. Political Content. [online] Available at:

<<https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html>>  
[Accessed 20 July 2021].

Warner, M., 2019. The Honest Ads Act. [online] U.S. Senator Mark R. Warner. Available at:

<<https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act>> [Accessed 20 July 2021].

Facebook. n.d. What is the Facebook Ad Library and How Do I Search It?. [online] Available at:

<<https://www.facebook.com/help/259468828226154>> [Accessed 21 July 2021].

Wolford, B., n.d. What are the GDPR consent requirements? - GDPR.eu. [online] GDPR.eu. Available at:

<<https://gdpr.eu/gdpr-consent-requirements/>> [Accessed 21 July 2021].

Google Support. n.d. Why you're seeing an ad. [online] Available at:

<[https://support.google.com/ads/answer/1634057?p=privpol\\_whyad&hl=en&visit\\_id=637577350377416582-3132555781&rd=1](https://support.google.com/ads/answer/1634057?p=privpol_whyad&hl=en&visit_id=637577350377416582-3132555781&rd=1)> [Accessed 21 July 2021].

Zuboff, S., 2019. The Age of Surveillance Capitalism. London: Profile Books.

## **Glossary of Acronyms**

AfD – Alternative for Deutschland  
AI – Artificial Intelligence  
API – Application Programming Interface  
CCPA – California Consumer Privacy Act  
CCPR – California Privacy Rights Act  
CDU – Christian Democratic Union of Germany  
CSU – Christian Social Union  
DMA – Digital Market’s Act  
DSA – Digital Services Act  
EU – European Union  
EC – European Commission  
FCC – Federal Communications Commission  
FEC – Federal Election Commission  
FDP – Free Democratic Party  
FTC – Federal Trade Commission  
GDPR – General Data Protection Regulation  
MStV – Interstate Media Treaty (Medienstaatsvertrag)  
NPR – National Public Radio  
NYU – New York University  
OECD – Organization for Co-Operation and Development  
PII – Protected Identifiable Information  
SPD – Social Democratic Party of Germany