# Targeted Information (and Misinformation) in Political Advertising

An STS Research Paper
submitted to the Department of Engineering and Society
Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

David Mehani
Spring, 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
David Mehani

Approved _____ Date _____
Richard Jacques, Department of Engineering and Society

## Information Targeting

As the use of social media and other online communities continues to grow, businesses are collecting more data on their customers than ever before. With this data, behavioral online advertising and other such information targeting technologies continue to improve at connecting the desired users to fitting advertisements. In the 2016 presidential election, the world saw the most notorious use of this technology, which was later leaked in the Cambridge Analytica scandal. The many nefarious uses of information targeting technologies all fall under the framework of "Political Artifacts," which states that some technological artifacts can be inherently political by design. In this case, social media and information targeting technologies can be argued to be inherently political, as they make use of highly targeted advertising through ensuring certain types of users stay on the sites as long as possible, and in turn, receive as many targeted advertisements as possible. As these sites continue to allow political advertising and other types of propaganda to occur, it is becoming more clear that they are designed in ways that take advantage of their users. With all of this in mind, it begs the question: what are the effects of political targeted advertising and social media on elections? This question will be analyzed to look at the effects of these information targeting technologies on election outcomes and to further determine the political nature of social media and other similar websites.

## Social Media and Targeted Campaigning

In a world where everybody is online, advertisement based companies have been able to compile an incredible amount of data on their customers, further improving their information

targeting technologies. While this may not be a huge concern for most advertisements, such as advertisements for products and services, there is a growing concern around the use of these technologies for political advertising/campaigning. As many news outlets have reported in the time immediately following news of the Cambridge Analytica scandal, targeted political advertising and campaigning online may have played a huge role in the previous election, and as this information targeting technology continues to get better, it can continue to become a bigger threat. During the 2016 election campaigning, Cambridge Analytica had "sorted some 220 million Americans into behavioral profiles" with their online data from sites such as Facebook, and delivered messages "tailored to the psychological traits of each individual recipient," a practice known as "behavioral microtargeting" (Ward, 2018). While political propaganda has always had a profound effect on democracies, this effect may be amplified in the age of the internet and behavioral information targeting technologies (Persily, 2017). As these technologies are only becoming better, it becomes increasingly important to study their effects on democracies around the world.

The main artifacts in this study are social networks/websites themselves. Since these websites are where the vast majority of online data is collected, it is important to look at how these sites are so effective at doing this. One way to analyze the behavior of these sites is through the STS theory of "Political Artifacts," as it can be argued that these sites are inherently designed to take advantage of consumers, and possibly even specific demographics. Since these sites work on a business model of the users being a product for advertisers to purchase, there is growing concern that "as free Internet services become increasingly available, poorer consumers will sacrifice their privacy to receive free Internet access, whereas wealthier consumers will pay for

Internet access and realize better privacy protection" (O'Neil, 2001). The stakeholders in this study are the users of social media sites, as they are at the highest risk of receiving targeted political advertisements. These users, even when knowledgeable of the privacy risks, tend to have lax attitudes on the issue, which is a potential side effect of the design of social networking sites.

In the wake of the 2016 election and the Cambridge Analytica scandal, many have called for the abolition of political advertising and social media and other similar sites due to the potentially detrimental effects it may have on the democratic process. While most of the notable companies in this space seem to have ignored or refuted this suggestion, Twitter stands alone in heeding the warning and taking a stand to ban ads of political nature on their platform. Jack Dorsey, Twitter's chief executive, in support of this stance "said political ads, including manipulated videos and the viral spread of misleading information, presented challenges to civic discourse, 'all at increasing velocity, sophistication, and overwhelming scale.'," adding that " he worried the ads had 'significant ramifications that today's democratic infrastructure may not be prepared to handle'" (Konger, 2019). This drastic action taken by Jack Dorsey and Twitter, along with public outcry, demonstrates the growing concern over using online targeted advertising as a campaign tactic. While there is a sizable population of people concerned about this practice, there is still not enough knowledge about the true effects on online targeted advertising to determine whether it is truly a detriment to democracy or it is just a new tool for reaching a broader audience.

As the use of online targeted advertising for political campaigns continues to increase, the public's concern about these practices increases as well. While there are many concerns about

online targeted political ads, these concerns can typically be broken into three major categories: invasion of privacy, the threat of manipulation, and voter suppression (Borgesius, Möller, Kruikemeier, Fathigh, Irion, Dobber, Vreese, 2018). Of these three concerns, the issue of privacy remains the most pertinent, since successful targeted advertising requires a vast amount of data to be collected from users who may be unaware of this collection. The most recent example of this nefarious style of data collection is tied to the Cambridge Analytica scandal of 2016, where Cambridge Analytica sent out a personality test to some 350,000 volunteers on Facebook. While this population of users agreed to giving up personal information, "Cambridge Analytica realized they could integrate this information with a range of data from social media platforms, browsers, online purchases, voting results, and more to build '5,000+ data points on 230 million US adults.'" (Isaak, Hanna, 2018). Herein lies the root of the data privacy issue, as what started as 350,000 volunteers giving data points to Cambridge Analytica turned into the mass data collection of almost every United States citizen of voting age, most of whom unaware that this was happening.

While this collection of data from unconsenting users is alarming, even the targeting of consenting users may be inherently iniquitous due to the attitude users of social media develop as they use the sites. Research suggests that this attitude may be the result of "a combination of high gratification, usage patterns, and a psychological mechanism similar to third-person effect" (Debatin, Lovejoy, Horn, Hughes, 2009). In the paper "Do Artifacts Have Politics?", Winner describes the most important examples of technologies as those "that have political consequences are those that transcend the simple categories of 'intended' and 'unintended' altogether" (Winner, 2017). Social media is a prime example of this kind of artifact. With this in mind, it is

also important to take a look into social media's role in voter manipulation/suppression through targeted advertising. Since social media sites serve as convenient platforms for sharing information, it is no surprise that information can spread virally in certain populations. Put into the context of politics, this poses a clear threat for the mass manipulation of public opinion and the potential for manipulating and suppressing voters. In a study investigating Russian meddling in the 2016 election through Twitter bots, researchers "found that Conservatives retweeted Russian trolls over 30 times more than Liberals and produced 36 times more tweets. More recently, Stella et al. high-lighted how bots can play significant roles in targeting influential humans to manipulate online discussion thus increasing in-fighting. Especially for the spread of fake news, various studies showed how political leaning, age, and education can greatly affect fake news spread, alongside with other mechanisms that leverage emotions and cognitive limits." (Deb, Luceri, Badawy, Ferrara, 2019). This mode of information spread is especially concerning in the frame of politics and elections, as it is shown to be the driving force of voter manipulation and suppression online. More specifically, in the 2016 presidential election, these bots and advertisements "were intended to influence the election either by supporting Trump, maligning Clinton, or by suppressing the vote. The suppression efforts, directly or indirectly, attempted to convince various groups, such as Black voters and Bernie Sanders supporters, even after Sanders endorsed Clinton, to not vote at all or to vote for a different candidate." (Ravel, 2019). Ravel, a former commissioner of the Federal Election Commission, argues that because of the highly target nature of these advertisements and bots, the equal participation of all citizens and groups in the democratic process, the crux of democracy, may become compromised, representing a major problem for the future of democratic systems.

**Targeted Political Advertisements: By the Numbers**

The rise of social media and its continued growth has undoubtedly had a sizable effect on campaigning tactics, opening up a completely new and vast outlet for reaching out to potential voters. In 2007, not long after Facebook expanded beyond college students and into the general public, Facebook unveiled a technology that had changed the course of advertising forever, calling it "Facebook Ads." This platform was broken up into three parts, the most important one being "an interface to gather insights into people's activity on Facebook that marketers care about" (Facebook, 2019). While this technology has some obvious merit to both marketers and consumers alike, "Facebook Ads" and other similar technologies have had and continue to have a profound effect on the campaigning process in the United States.

Facebook Ads and other online targeted advertising services have become some of the most powerful tools in the arsenal of campaign managers. The effects of the launch of these services were seen almost immediately in the 2008 presidential election: total campaign spending very nearly doubled from the previous election in 2004 (from $891,514,450 to $1,769,982,008) (FEC, 2020). While not all of this massive increase was due to online advertising, over $40,000,000 were spent on online targeted ads, with Obama, the eventual victor, coming in as the top spender on these advertisements (FEC, 2020). Another large factor in this increase in spending was the drastic increase in so-called "individual expenditures," or outside spending, made mostly by ideological groups to finance ads advocating for or against certain candidates. These contributions were largely spent on online advertising, as Facebook Ads and other services began to offer their targeted advertising services to the public (Albert, 2017). The 2008 election

serves as the beginning of a trend that is here to stay, as evidenced by sustained growth most recently capped off by 2020 presidential candidate Michael Bloomberg alone surpassing $40,000,000 in just Facebook advertising (Kraus, 2020). Because of this trend, it is important to further analyze the effects and ethics of the use of behavioral online advertising for political campaigns.

Looking deeper into FEC data for the past three elections (the only ones making use of online targeted advertising), each of the victors was also the candidate who spent the most on targeted ads on sites such as Facebook. While it is impossible to draw causal conclusions from such limited data, one important data point from the spending numbers is that in the 2016 election, the Clinton campaign outspent the Trump campaign in general by approximately a quarter of a billion dollars, however the Trump campaign spent significantly more on Facebook Ads, with Trump emerging victorious in the election. While conclusions cannot be drawn from just on election outcome, this demonstrates a situation that should be monitored in future elections in order to more accurately judge the power of online targeted advertisements for political campaigns.

**Are Targeted Political Advertisements on Social Media Ethical?**

With the campaign spending data, although limited to a short past, seemingly supporting the power of targeted social media advertisements for political campaigns and the growing popularity of this tactic, it is important to look at ethical concerns regarding this form of campaigning. In order to analyze this complex situation, online targeted political advertisements

can be broken into two parts for ethical analysis: the operation of social media sites themselves and the practice of targeting political advertisements toward specific demographics.

While online targeted advertising is a relatively new practice, simple targeted advertising certainly is not. Prior to the development of this technology, getting a message out to specific demographics was still a cornerstone of campaigning for office. Before Facebook Ads and other similar services, campaigns were still able to reach specific demographics, albeit broader than what is possible now, through careful selection of traditional television, radio, and printed advertisements. It is no surprise that these tactics have been commonplace, as showing advertisements to the wrong groups of people can be equated to a waste of money, and is mostly useless to a political campaign. Even when applying the most stringent ethical frameworks to this situation, the practice of showing political advertisements to certain demographics is not inherently unethical; it is merely a maximization of the use of campaign funds in an attempt to win an election.

Since there is nothing inherently unethical about campaigning to specific demographics, the real ethical concerns over online targeted political advertising lie in the operation of the social media sites themselves, both in the unprecedented power they have to quickly and accurately spread information and the behaviors they cause users to subconsciously exhibit. The ability for these platforms to be able to accurately identify specific demographics is supported almost exclusively by their extensive collection of user data. While many of these sites have privacy settings and the legally required privacy policy and terms of service documents available to their users, there are still ethical concerns over these practices. Although privacy controls and information are available to users, these items can be confusing and misleading, leading many

users to a false sense of privacy. Even users who are not misled by the privacy information on social media sites are at risk, as research suggests these users tend to develop lax attitudes toward the privacy concerns due to the high gratification designs of these sites.

The two aforementioned practices of social media sites are ethically questionable, but when combining these with the practice of maintaining "Shadow Profiles" and finally the use of all of these tactics for political purposes, the behavior of these sites becomes concretely unethical. "Shadow Profiles", most notoriously used by Facebook, are essentially profiles of people that are created with data compiled from other users, and most importantly, without the consent of any of the involved parties (Brandom, 2018). Not only can these profiles be used to fill in missing data from a more private "real" profile, but they can also be created for people who are not even users of the site. While this may not be a huge perturbation in the realm of marketing products to consumers, concern over this practice expands when it is used in micro-targeting potential voters for political advertisements. This nonconsensual use of data, both of people who are convinced of the privacy of their profile and of people who are wholly unaware that these sites have built profiles on them, for the purpose of manipulating and suppressing voters is where the unethical behavior lies and is what poses the biggest threat to the democratic process.

**Conclusion**

As the use of targeted online advertising as a campaign strategy continues to gain popularity, concerns about the practice are arising at a similar pace. While politicians and campaign managers have been trying to target advertisements to specific demographics

throughout history, social media and other online platforms have made this task far easier, albeit with questionable tactics. By using "Shadow Profiles" and other intricacies of target advertising technologies, sites that use targeted advertising have been able to collect data on the majority of voters, providing campaigns with a far broader reach than ever before. This reach, which is nonconsensual in nature, when combined with the potential for voter manipulation and voter suppression, shows a trend of alarming campaign tactics which have the potential to undermine the democratic process. As campaign spending on online targeted advertising only continues to increase, legislation against this practice (or sub-practices) must be put in place in order to limit the possibly detrimental effects it can have on democracies. The EU has already passed the General Data Protection Regulation in order to combat situations such as the Cambridge Analytica scandal and to provide legal recourse for similar cases in the future (Tieu, 2018), and other countries should follow suit in order to both protect the online privacy of their citizens and protect the integrity of their democracies.

**References**


Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. Journal of Media Ethics, 33(3), 133–148. doi: 10.1080/23736992.2018.1477047

Persily, N. (2017). Can Democracy Survive the Internet? Journal of Democracy, 28(2), 63–76. doi: 10.1353/jod.2017.0025

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. Social Science Computer Review, 19(1), 17–31. doi: 10.1177/089443930101900103

Conger, K. (2019, October 30). Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says. New York Times. Retrieved from https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html?auth=login-google

Borgesius, F. J. Z., Möller, J., Kruikemeier, S., Fathaigh, R. Ó., Irion, K., Dobber, T., … Vreese, C. D. (2018). Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, 14(1), 82. doi: 10.18352/ulr.420

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 51(8), 56–59. doi: 10.1109/mc.2018.3191268

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication, 15(1), 83–108. doi: 10.1111/j.1083-6101.2009.01494.x

Winner, L. (2017). Do Artifacts Have Politics? Computer Ethics, 177–192.

doi: 10.4324/9781315259697-21

Stella, M., Ferrara, E., & Domenico, M. D. (2018). Bots increase exposure to negative and inflammatory content in online social systems. Proceedings of the National Academy of Sciences, 115(49), 12435–12440. doi: 10.1073/pnas.1803470115

Deb, A., Luceri, L., Badawy, A., & Ferrara, E. (2019). Perils and Challenges of Social Media and

Election Manipulation Analysis: The 2018 US Midterms. Companion Proceedings of The 2019 World Wide Web Conference on - WWW 19. doi: 10.1145/3308560.3316486

Ravel, A. (2019). A New Kind of Voter Suppression in Modern Elections. The University of Memphis Law Review.

Facebook Unveils Facebook Ads. (2019, November 7). Retrieved April 24, 2020, from https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

FEC reports on financial activity U.S. Senate and House campaigns : final report. Washington, D.C. :Federal Election Commission.

Albert, Z. (2017). Trends in Campaign Financing, 1980-2016.

Kraus, R. (2020, March 4). Bloomberg is out. Here's how much he spent on Facebook ads. Retrieved April 24, 2020, from https://mashable.com/article/bloomberg-ends-campaign-facebook-advertising-spend/

Brandom, R. (2018, April 11). Shadow profiles are the biggest flaw in Facebook's privacy defense. Retrieved April 24, 2020, from https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

Tieu, K. (2018, April 5). International Data Privacy in a Post-Cambridge Analytica World. Retrieved from https://www.jtl.columbia.edu/international-data-privacy-in-a-post-cambridge-analytica-world/