

Introduction

The development of the internet led to the advent of social media, which is defined as “the use of technology combined with social interaction to create or co-create value” (Pavlik and McIntosh, 2013, p. 239-240). Social media websites such as Facebook, Twitter, and Tik-Tok allow users to communicate and generate content with others throughout the world. According to the Pew Research Center, as of 2021 more than “72% of the (American) public uses some type of social media”, with 69 percent of Americans favoring Facebook, the most popular platform (*Social Media Fact sheet*, 2023). Considering the large consumer base and demographic information contained on Facebook, protecting users’ privacy and information should be of the highest priority. When a breach does occur though, it is equally important to understand how this data can be used in a nefarious way, such as in the 2016 United States Presidential campaigns.

It was revealed in 2018 by a New York Times report that political consulting firm Cambridge Analytica gathered the personal data of up to 87 million Facebook users through an application called “This Is Your Digital Life”. The application was a paid survey in which 270,000 initial individuals signed up for and participated in. According to former employee Christopher Wylie, the whistleblower about the deceptive practices by Cambridge Analytica, the process was fairly simple: you click on the link, fill out the survey, and at the end you receive a payment code. However, “two very important things happened in those few seconds. First, the app harvested as much data as it could about the user who just logged on” (Hern, 2018) - it was

revealed that over 5,000 data points were gathered by this method. These data points included personal facts such as name, location, and contact information, as well as behavioral information like time spent on certain profiles and pages. Even worse, though, is that “the app did the same thing for all the friends of the user who installed it. Suddenly the hundreds of thousands of people who you’ve paid a couple of dollars to fill out a survey, whose personalities are a mystery, become millions of people whose Facebook profiles are an open book” (Hern, 2018). Millions of people’s information was unknowingly gathered without consent.

The information gathered by Cambridge Analytica was ultimately used by Republicans, notably Ted Cruz and former President Donald Trump to target audiences in an attempt to influence the elections. Christopher Wylie succinctly states how so many data points might be used in an unethical way: “Cambridge Analytica could, Wylie says, craft adverts no one else could: a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one, each designed to suppress their voting intention – even if the same messages, swapped around, would have the opposite effect” (Hern, 2018). Cambridge Analytica built psychographic profiles on each Facebook user and these profiles were utilized to run targeted advertising campaigns addressing controversial issues to influence their vote. Joe Westby states that “Facebook and Google have amassed data vaults with an unprecedented volume of information on human beings. This goes far beyond the data that you choose to share on their platforms to include the vast amounts of data tracked as you engage with the digital world. Mass corporate surveillance on such a scale threatens the very essence of the right to privacy” (Westby, 2021). It is clear that both Facebook and Cambridge Analytica were complicit not only in stealing users’ information, but they attempted to influence the democratic process of elections within the United States.

Methodology

Due to the impact and scale of Cambridge Analytica and Facebook's data break/leak, there are numerous articles online covering the case. Because it directly involved a political process, it garnered the attention from numerous news agencies which have a propensity to be biased. In searching for articles to support this research, it was difficult to stay away from these types of stories, though many were insightful, and data driven. Outside of news agencies, many universities and institutions led research concerning privacy and data-integrity as a direct result of Facebook and Cambridge Analytica's alarming practice. To sort through the numerous articles covering this issue, internet domains ending in ".org" were prioritized, as it was published on behalf of an organization and not by an individual online. Organizational publications tend to have better research; however, it is important to investigate who funds the organization and what their mission and purpose is. Oftentimes, these institutions are funded by individuals with ulterior motives, and therefore this should be considered when reading and analyzing an article they have published. Websites ending in ".edu" were prioritized as well because they require an amount of research before being published on behalf of a university. Students writing academic articles are also not funded by a specific organization or institution and are less likely to be biased outside of their own personal beliefs.

Analysis and Discussion

Targeted advertisements and messages aren't necessarily bad, companies employ these tactics constantly. However, when an entity deceptively collects a person's pattern of behavior and demographic information without their consent, and then uses that to influence a democratic process, the principle behind the data gathering quickly switches from capitalistic to immoral. Surely, had Facebook or Cambridge Analytica provided a disclaimer before the survey which

read “The test results will be used to analyze behavior in an attempt to influence elections”, the fallout would be not as severe because the purpose of the survey was disclosed. Americans have a strong sense of pride in the democratic process, and when that is undermined, especially by a third party, the trust they have may dwindle. The following two advertisements from Cambridge Analytica were distributed to specific individuals based on the psychographic profile built on them:



Rahul Rathi explains the meaning behind the different advertisements covering the same subject of gun rights in America, stating “People high in neuroticism and conscientiousness, tend to worry a lot and prefer order and so the message on the left would resonate more. Closed and agreeable people put other people’s needs before theirs, but don’t enjoy new experiences and so the message on the right would resonate greater” (Rathi, 2019). Both are purposefully manipulative and aim to manipulate one’s beliefs, morals, and psychology to get a message across. Charles Redding, who is often considered the father of organizational communication, outlines five message types which are often observed within an organization: coercive, destructive, deceptive, intrusive, and manipulative-exploitative.

Coercive messages are considered “intimidating, repressive, threatening” and accounts for an abuse of power which influences an individual’s autonomy (Johannesen et. al., 2008, p. 162). Cambridge Analytica capitalized on and abused Facebook’s lax privacy laws to gather

information on millions of individuals. This data was then used to tailor intimidating and threatening messages viewed by individuals. Though they did not outright threaten the viewer, the advertisements implied the negative consequences if, as in the example above, someone did not own a firearm.

Destructive messages are defined as communication which “attacks others’ self-esteem, reputation, or deeply held feelings; reflects unconcern or contempt for others’ basic values” (Johannesen et. al., 2008, p. 162). These include but are not limited to insults or negative remarks about a group of people, which were perpetuated by the toxic environment of social media, especially surrounding the 2016 Presidential elections. Cambridge Analytica capitalized on the deeply held beliefs about others within the American society to further incite division in the United States. Deceptive messages “intentionally distort[s] the truth in order to deceive or cheat” which include “evasive and deliberately misleading messages, intentional ambiguity to mislead” (Johannesen et. al., 2008, p. 162). Misinformation was at the heart of many Cambridge Analytica campaigns, and it was certain that they “planted fake news” to try and persuade or dissuade their target audience (*'Cambridge Analytica planted fake news'* 2018).

Intrusive and manipulative-exploitative messages account for the majority of Cambridge Analytica’s targeted advertisements. Intrusive communication “violates ‘privacy’ rights” and includes the “use of computer technologies to monitor employee behavior” (Johannesen et. al., 2008, p. 163). Despite addressing employee behavior, the intrusive message is applicable across society. It is well documented that Cambridge Analytica used data based on Facebook viewers’ history and trends to tailor political messages towards their beliefs. It is the monitoring and tracking of behavior to intentionally influence elections that is a major ethical issue. Finally, manipulative-exploitative messages “satisfy personal gain or shows unconcern for others by

exploiting their fears, prejudices, or lack of knowledge” and is personified as a “patronizing or condescending attitude towards others” (Johannesen et. al., 2008, p. 163). Considering the fact that two Republican candidates employed Cambridge Analytica to target voters, it is easy to understand how their messages would be shaped. Republicans, who are notably pro-life, pro-gun, and jingoistic are more likely to be persuaded by messages addressing these issues, especially the controversial aspects of such subjects.

Conclusion and Recommendations

The Facebook and Cambridge Analytica scandal highlights the ethical implications of data collection in our excessively digital and interconnected world. Their manipulation of personal data for political purposes raised ethical concerns around privacy and consent, and more notably, social media’s influence on democracy. Facebook’s inaction to protect over 87 million users’ data enabled Cambridge Analytica to utilize this personal data to influence the outcome of the 2016 United States Presidential election. Facebook has acknowledged their role in this scandal, and owner and creator Mark Zuckerberg has even testified before the United States Congress advocating for stricter privacy measures.

Works Cited

- Pavlik, J. V., & McIntosh, S. (2013). *Converging media: A new introduction to mass communication*. Oxford University Press.
- Social Media Fact sheet. (2023, April 05). Retrieved April 23, 2023, from <https://www.pewresearch.org/internet/fact-sheet/social-media/>
- Hern, A. (2018, May 06). Cambridge Analytica: How did it turn clicks into votes? Retrieved April 23, 2023, from <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>
- Westby, J. (2021, October 11). 'The great hack': Cambridge Analytica is just the tip of the iceberg. Retrieved April 24, 2023, from <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>
- Arora, N., & Zinolabedini, D. (2019, December 01). The ethical implications of the 2018 Facebook-Cambridge Analytica Data scandal. Retrieved April 24, 2023, from <https://repositories.lib.utexas.edu/handle/2152/80574>
- Johannesen, R. L., Valde, K. S., & Whedbee, K. E. (2008). *Ethics In Human Communication* (Sixth). Waveland Press, Inc.
- Rathi, R. (2019, January 13). Effect of cambridge analytica's facebook ads on the 2016 US presidential election. Retrieved April 24, 2023, from <https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d>
- 'Cambridge Analytica planted fake news'. (2018, March 20). Retrieved April 24, 2023, from <https://www.bbc.com/news/av/world-43472347>