Micro-targeting as a paradox: The Cambridge Analytica Scandal

Veys, Tugche

Tugche Veys (s1949101)

Leiden University

Faculty of Governance and Global Affairs

MSc Public Administration: Economics and Governance

2020-2021 Academic Year

Thesis Capstone: Algorithmic Governance

Supervisor: Dr. Bram Klievink

June 11, 2021

Master Thesis

Micro-targeting as a paradox: The Cambridge Analytica Scandal

19543 words

TABLE OF CONTENTS

Chapter 1- Introduction

Although big data has its advantages to human life (Cian et al., 2018), it also causes issues in terms of privacy, surveillance, and ethics (Zuboff, 2015). The new era created by technological advancement and its borderless character poses dangers to individuality and privacy in many aspects. When people provide personal information in order to make use of certain services on the Internet, their information is being collected and stored each time. This is also called digital footprint, enabling one to observe how often individuals use the Internet. On the one hand, the collected information can be used for advertisement purposes that could be beneficial for users. As such, they could keep up with the latest developments in the world, get discounts, or book holidays. These advantages of data collection are the artifacts of algorithms. From a general perspective, an algorithm is a set of instructions created by computers that help to either solve problems or execute computation (Math Vault, 2019). However, this research takes a more specific and simpler view while defining an algorithm. In social media, algorithms are rules that sustain order, provide relevant results to the user, and direct them to websites that are advertised on the platforms (Digital Marketing Institute, 2019). Algorithms operate in the background of the Internet. They are the masterminds of visualizing social network advertising. As a result, it becomes much easier for users to reach products. Social media users can click on the content and reach their preferences. Algorithms are therefore the first step in social networking and creating the base for user engagement. They build the way up for micro-targeting practices by tracking user movement in social media to come up with more accurate predictions. Micro-targeting entails an exercise that is used to customize collected user information depending on the likings and behavior of the users (Krotzek, 2019). This type of mechanism is a tool for social media companies to increase user engagement and profit.

Micro-targeting allows to assess users' previous and recent preferences to show them individualized content on certain things they are interested in. These advertisements become visible on users' pages for money-making purposes. Once clicked on, the user is directed to a website where there is specific content. It is important to note that randomly clicking on a product on the internet and later on, seeing the same product on social media is not a coincidence. It is the work of algorithms that identify which sites users visit and browse. Consequently, algorithms and micro-targeting are heavily connected to one another. Micro-targeting is essentially a product of algorithms, and this is the main reason why algorithms have an instrumental role in the creation of micro-targeting. The end goal is the same for both: profit-making. In today's 21st century technology-driven world, this is one of the easiest ways for increasing the user base on social media

platforms. What this situation proves is that the presence of social media is the most important element for micro-targeting. In a broad spectrum, this research is based on the idea that there are three stages for user engagement on social media. First, there needs to be a popular social media platform. Second, there is a need for high numbers of users. This would enable micro-targeting to be effective due to the collection of data. Lastly, these algorithms are used to create targeted messages or advertisements for increasing activity, and in turn, increasing profit. The last two stages build the cornerstone of micro-targeting since algorithms are inherent in micro-targeting. In this way, social media companies are aware that such practices are beneficial for business purposes and hence, they use these methods. Generally, users are not even aware that micro-targeting is used as it became very common in recent years. However, they *do* start questioning it when they suffer from its harmful consequences: invasion of individual privacy. On the one hand, micro-targeting allows advertisers to recommend their products to social media users, and users can perceive these ads as helpful for achieving their needs and preferences. On the other hand, there is also the downside of collecting user data for purposes that are not ethical in principle. This situation presents a paradox where micro-targeting is a necessary evil in many aspects.

Micro-targeting as a privacy-invasive and unethical practice is widely known among the privacy and media studies scholarship (Nissembaum, 2016; Papacharissi & Gibson, 2011; Zuboff, 2015). Current literature on micro-targeting is mainly based on the understanding that micro-targeting is a threat to individual privacy and that it goes against democratic norms and values (Bathini, 2021; Ward, 2018). There is an emphasis on how people perceive social media and their behavior on social media platforms. Surveillance, data collection, and privacy aspects of micro-targeting are highly prominent in the already existing literature (Afriat et al. 2020, MacNish, 2020; West, 2019). However, the current literature is not solely enough to explain the relationship between social media users and micro-targeting. Micro-targeting presents a paradox that needs attention in many aspects. For the past couple of years, micro-targeting is used as a two-way tool in determining social media usage and social media companies' profits. First of all, micro-targeting allows social media companies to obtain personal information on their users. Then, advertisers use this information to target individuals to recommend their products. In this way, the advertisers reach a target audience on social media platforms for selling products and services. If users react to these contents, then both the social media companies and the advertisers gain from the user engagement. The more users stay logged in and view products, the more profit the social media platforms make. Similarly, the advertisers can also show their content to more people. What is often ignored is that users, as well, benefit from this model. Although their personal data is used in the creation of such

advertisements, they also gain from it. Micro-targeting helps users to achieve their preferences faster and more accurately. The main problem stemming from this situation is that regardless of the privacy concerns, users do not stop using social media. In fact, particularly users' behavior in such a way makes micro-targeting a paradox since they willingly contribute to micro-targeting practices by being active on social media platforms. It is exactly this paradoxical feature of micro-targeting that has not been addressed thus far. In other words, the *micro-targeting paradox* is absent in the current debate. Hence, this research aims to shed light on micro-targeting from a distinct point of view in a comprehensive manner. In so doing, the research aims to fill the literature gap by offering a theoretical lens based on individual behavior and social media surveillance. This is because micro-targeting relies on social media surveillance. The vicious cycle between micro-targeting, social media, and user behavior sets the stage for a toxic relationship because individuals are exposed to surveillance. Micro-targeting is only possible if the advertisers and the social media companies are able to assess their users' behavior on the platforms. Users actively provide their data on social media, yet, they do not disengage from these platforms. Hence, social media usage does not decline because of the mutually advantaging character of micro-targeting.

The micro-targeting paradox phenomenon emanates from a combination of privacy concepts mentioned in the following sections of the research. Even though these concepts are not directly linked to micro-targeting, they create a base for understanding that micro-targeting is a controversial method that can be abused. What is known about these concepts in the literature is they emerge from privacy breaches and these breaches lead individuals to react in certain ways towards social media. For instance, while privacy fatigue suggests that individuals are used to hearing privacy breaches and therefore do not even feel violated anymore (Choi et al., 2018; Lee et al., 2016), networked privacy indicates that individual privacy is lost once content is shared, and that privacy becomes networked (Boyd, 2014). In the current literature, the most similar concept applying to micro-targeting and its controversiality is the privacy paradox. Barnes (2006) explains that this concept is based on individuals' behavior. Individuals expect to have privacy because they are worried about their personal information being breached. Nevertheless, they willingly provide their information to online services in order to make use of their advantages. This situation indeed creates a paradox as the individual expectations and actions are not in line with one another. These three privacy concepts form the building blocks of the micro-targeting paradox.

Throughout the research, the recent Cambridge Analytica (CA) scandal is taken as a single case and will be examined as the research proceeds. The case represents a bridge between micro-targeting and user behavior as well as users' role in the micro-targeting paradox. Going beyond

privacy, the case offers a new understanding: the reason why micro-targeting is a paradox is due to continuing user engagement on social media. Hence, this research differs from the previous literature as it shows that users are also responsible for the negative consequences of micro-targeting. Data breaches not only occur by the mistakes of social media companies or third parties, but also by social media users because they are the ones who provided their data initially.

Broadly, there has been a lot of criticism over the relationship between Facebook and the data analytics firm Cambridge Analytica (CA) for micro-targeting purposes (Internet Governance Lab, 2020). Therefore, this paper takes the CA scandal as a single case to show how social media data (Facebook in particular) serves as a basis for micro-targeting. The CA scandal suggests a controversial case not only in terms of social media micro-targeting but also in observing the user behavior in the aftermath of the scandal. It is the most recent case related to cybersecurity, social media, and privacy. The scandal's uniqueness comes from its popularity in illustrating the effect of social media micro-targeting on both the governmental and individual levels combined. The case explains this through the discussions between the US government and the relevant actors involved.

Moreover, the case is also popular as of the rumors that Facebook was involved in the election of US President Donald Trump and the Brexit campaign with the collection of Facebook user data. These aspects gained attention in both public and political spheres. They offer a new view of how social media companies use individual data and utilize it in a way that is beneficial for the company and user behavior. Following the revelations of the scandal, the big technology giant Facebook has come under scrutiny regarding user privacy and mass data collection activities. User data is concentrated in the hands of Facebook, giving the company a powerful position in data surveillance. The scandal had such a huge spillover that the US government held Facebook accountable for the illegitimate mass data gathering. The US Senate and Congress questioned Mark Zuckerberg and those who were in charge of Facebook's administration during the time of the scandal. Therefore, it is a complex case due to the biggest data breach in social media history.

This research is trying to answer the following question: Why do individuals continue using social media (Facebook) even though they have privacy concerns over the Cambridge Analytica micro-targeting scandal? It argues that the reason why users still engage on Facebook is because of the micro-targeting paradox. In other words, Facebook usage did not decline drastically because individuals were attracted to micro-targeting. Rather than reducing the user activity, micro-targeting kept the users engaged on the platform. Even though micro-targeting is widely accepted as a practice that fundamentally violates privacy (Korolova, 2010), the users do not perceive it as a huge issue. Continuing user engagement is unusual and the current literature bypasses this aspect. It

mainly discusses that the violations are a threat to individual privacy and democracy, and a well-established privacy regulation is needed (Bennet, 2013; Howard, 2006; Kim et al., 2018; Lavigne, 2020; Munroe & Munroe, 2018). Different from the previous literature, this research assesses social media usage by using micro-targeting as an approach. For this paper, social media usage means citizens' behavior and engagement on Facebook. These behaviors include changing their user status, less frequent usage, or complete disengagement from the platform. Therefore, the research builds upon privacy and surveillance aspects in order to make sense of micro-targeting. Many privacy scholars in the existing literature cover the CA scandal from the citizen perspective in terms of political election manipulation, in other words, micro-targeting as a political tool in winning elections (Baldwin-Philippi, 2017; Bodó et al., 2017; Delacourt, 2016; Jamieson, 2013; Prummer, 2020). This research relies on the current literature, yet, it takes a more citizen-targeted approach with the government's response on the issue. The US is an exemplar case since it is a country where the biggest breach of citizens' privacy was reported, constituting the most populated Facebook user base.

As for the layout, this research is structured in the following way: Chapter 2 first discusses the literature on micro-targeting from the perspectives of various scholars. Then, the chapter mentions the concepts of surveillance and privacy to explain how they are closely linked to micro-targeting. In specific, it shows how these concepts are inherent within the CA case and how they can be interpreted. Chapter 3 then proceeds with the case description, outlining the background of the CA scandal. In so doing, a content analysis is conducted with the inclusion of various academic articles and government reports. The research design is based on a single case study as mentioned previously. Next, Chapter 4 is the analysis section and provides a thorough examination of the relationship between Facebook and micro-targeting in the US from the citizen/individual perspective. Lastly, in Chapter 5 the research finalizes with the main empirical results, conclusions, and implications for further research.

Chapter 2- Literature Review and Theoretical Framework

2.1. Literature Review

While making sense of micro-targeting, its different perspectives and types need to be clear. This section starts with laying out what micro-targeting is and how it has developed differently in the literature. In this subsection, there are various scholars who directly contributed to the discussion on micro-targeting. As well, there are also those who indirectly provide a foundational basis for micro-targeting by using different models and explanations. In the latter, these

contributions might be normative at times, yet, they are essential for two reasons: understanding how social media companies work, and how their workings weaponize micro-targeting that results in contradictory behavior on social media. Hence, it is this research's aim to address the aforementioned reasons and provide evidence for them.

2.1.1. Micro-targeting

Borgesius et al. (2018) argue that micro-targeting is "a type of personalized communication that involves collecting information about people and using that information to show them targeted advertisements" (p. 82). Especially in today's world, it takes place through psycho-geographic segmenting that consists of an algorithm in order to target, differentiate, and categorize individuals according to their traits (Borgesius et al., 2018). It entails calculating individual preferences and their behavior to persuade them into performing the actions that micro-targeting actors seek. Also, it is an appealing strategy as people tend to respond to personally modified messages instead of generic ones. Therefore, micro-targeting is an important tool for shaping behavior. It penetrates the subconscious mind and is related to human psychology. In Gorton's (2016) view, micro-targeting is "creating finely honed messages targeted at narrow categories of voters' based on data analysis 'garnered from individuals' demographic characteristics and consumer and lifestyle habits" (p. 62). He sees micro-targeting as a political tool for influencing voting behavior. However, it can also be seen as a marketing strategy (Borgesius et al., 2018). In this case, manipulation takes place where people are the product, rather than entities with self-determination (Berghel, 2018, p. 88). Moreover, there is no fixed system for micro-targeting as it can take place via email, social media, or face-to-face (Dobber, 2020, p. 9). One of the most prominent trends of micro-targeting involves the analysis of social media data by using phone applications (Bennett, 2015). This also allows the data brokerage firms to create detailed profiling of not only social media users but also those who download the app on their phones. These applications can be used for marketing purposes ranging from shopping to traveling. Hence, micro-targeting has many forms depending on the business model of data analytics firms and digital communication companies. Metcalf et al. (2019) state that micro-targeting yields positive returns. Companies create categories for customers (or users) based on their shared traits and calculate their likelihood to respond to the content created. Even more accurately, if there is more data collected, these contents can be individualized through the customization of user data. This is called nano-targeting, which is aimed at influencing an individual or a specific subgroup (Edsall, 2012). Nano-targeting can be dually beneficial, both a company and an individual can use it for their own gain. Whereas a company could use it to shape

the behavior of an individual, an individual could also use this tactic to get in touch with a company's director for business purposes (Barbu, 2014). In this way, nano-targeting opens a new chapter in the communication strategies realm. It is, however, important that more data means more accurate predictions. Individual privacy becomes fragile and easy to penetrate if there is more data provided. Algorithms and machine learning technologies are therefore key for more precise micro-targeted advertisements as this would in turn increase user engagement.

Khursheed et al. (2020) share a comparable view with Borgesius et al. (2018) in defining micro-targeting. Yet, their understanding of micro-targeting differs in one key aspect: the similarity between micro-targeting and phishing. Their key argument is that phishing and micro-targeting have the same methods while gathering data and its utilization for various purposes (Khursheed et al., 2020, p. 93). Users hold the decision to respond to the targeted messages in both cases. Even though these activities are generally covert, individuals can choose whether or not to engage with the content that is targeted at them. The authors also argue that the purpose of these two practices is the same: building an extensive dataset based on individual data. They call this process "social engineering" since the collected data is used and utilized for user activity and profit-making (Khursheed et al., 2020, p. 93). Moreover, another view on micro-targeting is suggested by Kerpen (2011). He addresses micro-targeting as hyper-targeting. His words on hyper-targeting are significant in the sense that he provides an explanation that is based on social media in specific. He states that:

> "directing marketing and publicity efforts to a specific group, depending on their profiles, networks and activities on social media platforms. At the time, and even more so now, Facebook, Twitter, and LinkedIn held an unbelievable amount of data on hundreds of millions of people." (Kerpen, 2011, p. 25)

He gives an example where a customer was complaining regarding his stay in one of the hotels in the US. Then, the person received a message on Twitter from the hotel, stating that they were sorry for the customer's bad experience and hoping that he would have a better one in the future (Kerpen, 2011). This example shows how the individual was targeted based on the information he did not even provide in the first place (his social media account). Only knowing the customer's name, the hotel management could find the social media account of the person and sent him an emotionally manipulative message. The management personalized the message and built an emotional link with the customer, adapting their response according to the individual's needs and desires. The broad nature of micro-targeting is hence evident in this example as it does not solely utilize the data that is gathered digitally. It is a normalized and natural practice. Apart from the privacy breaching

perspective of micro-targeting, there are also transparency issues. Users do not know who holds their information and how their data is shared. The user is not aware of the processes that Facebook or Twitter adapt for keeping the users online for a longer time (Pierson & Van Zeeland, 2019). Social media technologies not only exercise micro-targeting within the platforms' users but also among users and other actors. These can be brands, celebrities or ideologies (Pierson & Van Zeeland, 2019, p. 367). Likes, shares, clicks, and views are profitable for social media companies through marketing and targeted advertisements. For instance, on Facebook users' capability to communicate with one another is limited to specific aspects that help Facebook to make a profit (Heyman & Pierson, 2015).

2.1.2. Foundational base for micro-targeting- Privacy and individual control of data

Nissenbaum (2004) advocates for contextual integrity where information and its distribution takes place within the established norms and values, with the principle of non-interference with an individual's privacy. Her work emphasizes the societal understanding of privacy which applies to the individual-level focus of this research. She points out that data and information collection must adhere to ethical boundaries and ensure that it does not harm the individual (Nissenbaum, 2004, p. 147). She explains contextual integrity with four statements (Nissenbaum, 2009). Firstly, she indicates that if there is an appropriate flow of information, there is privacy. Secondly, if the information flow complies with contextual norms and values, then there is contextual integrity. Next, she lays out parameters for understanding contextual norms. These are the type of information, subject, recipient, sender, and transmission (Nissenbaum, 2009). Lastly, while addressing privacy norms, there are three different levels of ethical legitimacy. In the first level, interests and desires are examined; the second level investigates the ethics and politics within the society; and the last level identifies the goals for the society (Nissenbaum, 2009). Nowadays, the four requirements for achieving contextual integrity are diminishing one by one each day. Privacy norms are disrupted by technological advancements in the digital era. The author acknowledges this situation and suggests that this problem must be solved on the societal level as a whole, and not solely on digital life. Moreover, she argues that institutions, regardless of their nature, "wield significant power over the fates of individual citizens and clients. Allowing these institutions free reign in collecting and using information further tips the balance of power in their favor" (Nissenbaum, 2004, p. 147). Her broad explanation for institutions includes governments as well as financial institutions. Yet, they are not the only ones. Her classification can be extended to data firms and tech giants. Their position in holding information has given them the tools to

determine the opinions of many individuals. In the current world order, the positioning of these tech giants produces an oligarchic structure, enabling few of them to hold power over individuals. This notion goes against the logic of self-determination of people and their freedom of thought in making decisions on their own. Hence, Nissenbaum (2004) argues for the idea that individuals are and should be autonomous actors who make decisions critically. In her view, they must be the ones who hold information, because that information is theirs. While she lays the foundational ground for privacy and data collection, in the current world system this does not hold. This aspect especially matters for the research to illustrate the effect of micro-targeting on users, being a highly important instrument for behavior manipulation. It poses dangers to privacy and hints at surveillance practices of technology corporations in creating the content for targeted advertisements on social media. In this case, the relationship between micro-targeting and user privacy becomes controversial and concerning. For this research, the issue is that most individuals do not have relevant knowledge regarding the workings of social media platforms. This favors micro-targeting as a paradox leading the users to get less worried about micro-targeting and more engaged on the platforms.

Similar to Nissenbaum's (2004) view on citizens as independent and self-governing actors, Regan (1995) argues that privacy is not merely crucial for individuals but also for society. Nevertheless, opposing to other privacy scholars who argue that privacy makes individuals better off, Regan (1995) asserts that privacy makes *society* better off. Boyd (2014) illustrates this point and states that "more than anything, I want to see users have the ability to meaningfully influence what's being done with their data and I'd love to see a way for their voices to be represented in these processes" (n. p.). She highlights that collective self-determination over individual data is needed. Therefore, in terms of user engagement on social media, her view indicates that possessing ownership of data determines how likely citizens will be willing to engage in social media platforms. Illegal data gathering and utilization through micro-targeting favor surveillance practices on individuals. This is what Cukier and Mayer-Schoenberger (2013) call datafication which means the creation of things that can be calculated. They argue that datafication is "concrete, individual, and context-bound" (Cukier & Mayer-Schoenberger, 2013). It directly impacts the individual and its effects depend on the context provided. The more context a data firm has on the person, the better, more accurate, and more detailed content it can produce through micro-targeting to influence citizens' behavior. Coupled with social media usage, these targeted features can reach massive audiences around the globe in many ways. This is the case in the CA scandal, as will become clear in the subsequent sections of the paper.

2.1.3. Digital platforms and their workings

Srnicek (2017) offers five categorizations of digital platforms. These are advertising platforms, cloud platforms, industrial platforms, product platforms, and lean platforms. For data-driven micro-targeting, advertising platforms are relevant. These platforms

> "collect data from users (and increasingly from connected objects), and then use different algorithms to process this 'raw material' and fabricate products that are sold to advertisers, namely the possibility to target specific categories of users, sorted according to various criteria (their tastes, interests, income, age- groups, preferred leisure activities, hobbies, etc.)" (Manokha, 2018, p. 899).

In the context of this paper, next to being a social media platform, Facebook can also be identified as an advertising platform given the increased number of advertisements it shows to its users. Srnicek (2017) identifies that all these platforms have one central feature, that is, the fact that their ownership is limited due to the cloud-based nature of these assets. He argues that as there is no physical capital, it is easier to manipulate data (Srnicek, 2017). These explanations suggest that there is a huge threat to privacy (Manokha, 2018, p. 903). Not only does the manipulation of data harm privacy, but it also violates human dignity, freedom of expression, and freedom of thought (Manokha, 2018, p. 903). To sum up, utilizing data has become "the new oil" in the tech industries' marketing strategies (Rosebrough, 2020).

Another aspect of data-driven micro-targeting arises from what Zuboff (2015) calls surveillance capitalism. In essence, surveillance capitalism is "a digital and commercial system that collects, tracks, analyzes, and leverages information about citizens to gain insights into how individuals differ and how these differences can be used to achieve some goal" (Dobber, 2020, p. 8). She argues that data collection is a way to make a profit (Zuboff, 2015, p. 894). In other words, it is a business model. The main actors involved in data collection are corporations such as Facebook. Her explanation asserts that data is monetized and its extraction from advertisers generates surveillance assets (Zuboff, 2015, p. 894). The main threat stemming from her argument is that the extracted data can be used for unexpected and ambiguous purposes that go beyond privacy. This is also depicted by Papacharissi & Gibson's (2011) work, in which they argue that personal data is a currency exchange for accessing more people's data.

This section aimed to provide a literature review on the understanding of micro-targeting on the citizen level and how it threatens individuals. Regarding the wider debate on data-driven micro-targeting, it is evident that micro-targeting has a multidimensional character. Even though authors' views differ, they converge on one dimension that there are dark sides of the digital world and they

pose serious challenges to individual privacy and their social media usage. Yet, social media users do not seem to worry about the possible negative outcomes of these services as they still use them. The micro-targeting paradox, therefore, comes into play as a potential explanation for continuing user engagement.

2.2. Theoretical Framework

In this subsection, the main goal is to unpack the theoretical explanation for continuing user engagement on Facebook. The main concept under examination is the micro-targeting paradox, complemented by the most relevant privacy concept called privacy paradox. Even though these two concepts have shared traits and target the same type of user behavior (continuing engagement), they have different reasonings. The former focuses on the reason *why* people are engaged on social media while the latter sheds light on the *observation* that users engage on these platforms. In essence, the micro-targeting paradox is the more advanced version of the privacy paradox which will be explained throughout the subsection. In order to build up the reasoning for the micro-targeting paradox, the section starts with the concept of surveillance and follows up with the complementing relevant privacy concepts as the section proceeds.

2.2.1. Surveillance

To make sense of privacy, one has to understand the concept of surveillance. Emerging technologies make surveillance a practice that can be both exercised by private and public institutions. Social media companies, cookies, and other third parties that have access to private information pose challenges to individual privacy. As Lyon (2007) argues, surveillance can be summed up as a routine and systematic focus on personal information in order to influence human behavior and maintain control over society. A surveillance society has accurate information on individuals concerning their everyday lives as data collection is a frequent practice. Clarke (1988), also supports this argument and proposes dataveillance, "systematic monitoring of people's actions or communications through the application of information technology" (p. 500). His explanation aligns with the strategies that are employed through social media algorithms. Furthermore, for the purposes of this paper, Hegel's (1812) information model is crucial. He identifies social life's three stages: cognition, communication, and co-operation (Fuchs & Trottier, 2015, p. 114). Information depends on cognitive processes which lead to the emergence of social processes (communication) and eventually form new systems and qualities (co-operation) (Fuchs & Trottier, 2015, p. 114). His model provides a basis for corporations to collect information for various purposes. In the current

digital era, surveillance takes place with data broker firms. The 'communication' level indicates the participation of social media platforms for surveillance practices. Conventionally, surveillance is characterized as information gathering and analysis, or a tool to shape behavior through control (Fuchs, 2011). Yet, these explanations are far too general for the scope of this paper. Hence, the research takes Fuchs and Trottier's (2015) definition of surveillance owing to their focus on the individual level. They suggest

> "surveillance in society involves the collection, storage, processing and assessment of data about humans or groups of humans by an actor in order to advance the latter's goals by violence exerted with the help of the collected information upon the humans under watch" (Fuchs & Trottier, 2015, p. 123).

What is important to highlight here is the similarity of the definitions between micro-targeting and surveillance. They both deal with the collection and processing of individuals' information to favor an actor's goals. The only difference between the two is that micro-targeting usually takes place for commercial purposes while surveillance is rather security-related.

The interlinkage between social media and micro-targeting thus has a threefold explanation. First, social media platforms, and mainly Facebook, can be seen as merchants. "They sell insights and space" to data firms (Dobber, 2020, p. 12). Second, they act as intermediary bodies by linking advertisers and users, advertisers being the data broker firms (Dobber, 2020). Third, they capture the user and provide them with a good experience (Dobber, 2020). Particularly, this classification suggests that social media platforms set the stage for micro-targeting to keep their users engaged and active. The model is based on the principle that both parties gain. Data firms

> "continuously track the citizen, collect data about their behavior, buy and combine additional datasets and clean the data. On the basis of the information, data brokers infer, predict and profile citizens. Individual profiles are continuously updated. Data brokers operate in the background. They provide the fundaments upon which microtargeting efforts rest." (Dobber, 2020, p. 12).

Consequently, looking at the 'tracking' aspect explained above, surveillance is at the heart of data firms' business models. For instance, when an individual searches for specific content on Google and subsequently logs into their Facebook profile, they will see the advertisement of that content related to it. Such instances take place due to the algorithms that data firms create to surveil and track human behavior. In this way, social media platforms and data firms gain from surveillance since they keep individuals engaged. These practices thus give rise to 'Facebook dependency' (Van der Schyff, 2020) and attach people to the platform. To conclude, data collection of individuals take

place with mass surveillance on social media platforms and it is mutually beneficial for social media corporations and data brokers. Their profit comes at the expense of individuals' privacy, which is at the core of their business model.

2.2.2. Privacy fatigue

Citizens' privacy is negatively affected by surveillance practices and this situation causes them to have ambiguous feelings towards social media usage. On the one hand, the capitalist world structure safeguards the privacy of big companies that make profits, in the meantime this very same structure is unable to defend citizens' privacy. Fuchs (2011) calls this socialist privacy. His study links the concept of corporate surveillance to the social media company Facebook. Fuchs (2011) further develops the concept of what Toffler (1980) refers 'prosumer'. Prosumer means consumers and producers are no longer different than each other. They are becoming more and more interlinked each day. Fuchs (2011) goes beyond this view and mentions 'prosumer commodity'. This concept is based on the notion that social media users are a source of capital. Users are commodities and they are being sold to data brokers, advertisers, or private actors. As a result, individual privacy is being breached. Rosenberg (1969) summarizes today's privacy understanding from a more historical perspective where he argued that in the future computers would be used dominantly to obtain complete information on citizens. Similarly, Miller (1971) suggested that with emerging technologies, there would be a "surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers" (p. 1456). Miller's worlds are today's reality where technological devices are the main drivers for a surveillance system. This digital sphere allowed many privacy concerns to emerge, leading to scandals regarding data breaches. In this case, the work of Choi et al. (2018) is central to mention. The authors argue that when there is a scandal arising from privacy issues, despite the generic idea that expects people to take action, they tend to end up not reacting to the issue. Recent research found that people are tired of hearing scandals about data breaches (Keith et al., 2014). Consequently, this situation leads them to think that it is pointless to even try protecting their data after all (Choi et al., 2018). This is called privacy fatigue which stems from the complex nature of data protection and the socio-psychological stress of using social media (Lee et al., 2016). Various reasons for using social media mean that people are exposed to seeing others' activities, including their opinions and discussions. Duggan and Smith (2016) find that these features of social media platforms lead people to feel "worn out", and "stressed and infuriated". People are likely to stop taking action towards protecting their privacy if they feel that they do not

have control over their privacy**.** This aspect has important connotations for micro-targeting. As these targeted advertisements covertly take place, individuals do not even realize if they are in control of their data. Moreover, they do not get surprised if they hear about data breach scandals. Privacy fatigue strengthens micro-targeting because users become unbothered and uninterested to control their behavior on social media. In a way, their lack of knowledge and interest regarding the control of personal data gives the impression that they already lost the battle against protecting their own data. On social media platforms, this behavior leads to getting more exposed to micro-targeting and user engagement. In this case, privacy fatigue helps to explain the micro-targeting paradox by providing a link between user engagement and micro-targeting. This can be depicted by a research that suggests "Everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great ... continuous monitoring will be the norm" (PEW Research, 2014). These breaches have become so common in citizens' daily lives that they normalize micro-targeting and do not mind it.

2.2.3. Privacy paradox

Barnes (2006) introduces a concept called the privacy paradox. This is related to privacy fatigue, however, argues that the association between people's actual behavior and concerns over their privacy does not align. People frequently state that they have worries about privacy, yet, they provide their personal information on websites to make use of shopping discounts or other services (Beresford et al., 2012). Several scholars tried to grasp why the privacy paradox occurs. They focused on causal explanations, for instance, the insufficient understanding of risks of such behavior, people not encountering data breaches, or other peoples' influence (Hinds et al., 2020). Yet, they fail to acknowledge that micro-targeting itself is the reason why people *are* engaged with these platforms. They are aware of the fact that they are surveilled and their privacy is being breached, however, they make use of those services (Metcalf et al., 2019). They keep up with the advantages of providing personal information to fulfill their needs. The two-way relationship between the users and the algorithms is mutually reinforcing. Van Dijk (2014) supports this claim by going against the wide-known literature that social media platforms are the facilitators of data breaches. On the contrary, both realms are intertwined. As stated before, micro-targeting's role in social media is to draw an audience to a particular content for increased returns (Metcalf et al., 2019). Therefore, the partnership between social media platforms and data firms mutually benefit from micro-targeting. For instance, while Facebook would keep individuals online for a long period, CA would make a profit by selling them the specific content that individuals are interested

in. Once individuals find the content they desire, this will create a chain reaction for the future and they will subconsciously perceive micro-targeting as a useful tool (Dobber, 2020). This explains user engagement in these platforms because micro-targeting ensures that individuals receive specifically targeted advertisements according to their likings. In this case, even though individuals become subject to a privacy breach, this paradoxical relationship feeds the users and causes dependency on social media platforms (Van der Schyff, 2020).

2.2.4. Networked privacy

According to Petronio (2010), the Communication Privacy Management (CPM) theory addresses privacy as publicness, such that both of them having the same meaning. In her view, privacy is someone's feeling of rightfully holding private information regardless of it being personal or collective (Petronio, 2002). In this case, since individuals own their information, they can control their information. Even though individuals may create boundaries regarding their data, if they want to connect with other people they need to form their boundaries accordingly. If users decide to engage with others on social media, they need to bear the consequences of taking such action. However, another explanation indicates that users are not always aware of how social media services work. On the individual level, people lack knowledge of how the digital sphere and algorithms operate, and how these can potentially cause harm to privacy. These algorithms are "opaque", meaning that even the creators of these programs do not know how they work after a certain time (Pasquale, 2015). This stems from the borderless nature of privacy and data which is known as networked privacy (Boyd, 2012). For instance, once a post is shared on social media, the individual loses control over the usage of the content. Even if the individual has a private account, the content can be easily shared and reposted by others and spill over to a bigger audience (Jia & Xu, 2016). Even if individuals prefer to set private profiles and share their information with a limited amount of people, this is an illusion (Jia & Xu, 2016). Individuals might feel that they have ownership over their data and can therefore control the flow of information. However, this is challenged "when the shared information concerns several other parties or stakeholders". (Jia & Xu, 2016, p. 5). One contribution to the networked privacy framework comes from Marwick and Boyd (2014). The authors start by introducing "networked publics", a product of the networked technologies and communities where people, technology, and practice intersects (Marwick & Boyd, 2014, p. 1052). Their work then examines how teenagers struggle to manage their privacy due to other people's privacy violations. These violations take place by what they call "invisible audiences", such as friend suggestions or companies (Marwick & Boyd, 2014). Invisible audiences

can obtain information on users that essentially should not be available to them. If users have public profiles or have information on their page, social media algorithms identify the information and show it to relevant actors that have links to the information the user provides. For instance, a user profile that has a university education section filled can easily appear in another user's friend suggestions who is at the same university. Hence, networked privacy creates ambiguous boundaries on social media privacy. For instance on Facebook, there is the presence of collective information control. When the individual shares personal data two actors become the co-owners of data: information recipients (Facebook) and information stakeholders (third-party individuals that are related to the content that is shared) (Jia & Xu, 2016, p. 5). In this way, these actors can collectively decide on what to do with the information (Fong, Anwar, & Zhao, 2009).

Starting from the beginning of the theoretical framework, the mentioned concepts deliver a detailed insight to grasp the micro-targeting paradox in the following ways. First, the surveillance aspect suggests that users are being surveilled on social media, being the most important feature for micro-targeting to take place. Second, privacy fatigue argues that users do not mind data breaches anymore since they are used to them by now. This is also another way of saying that users do not mind micro-targeting. If they are using the services of social media, it means that they are pleased with micro-targeting. Third, the privacy paradox puts together the controversy of users' claim for privacy while at the same time them being still online. Lastly, networked privacy explains how users are unaware of what privacy actually entails. In most cases, users do not even realize that their data has been breached, due to networked privacy explained above. Putting all these insights together, the reasoning behind the continuing social media engagement of users become clear. That being, users benefit from micro-targeting as well. Why this situation is a 'paradox' is particularly because of users' appreciation of micro-targeting. The more users are online, the more they are exposed to micro-targeting, and the more they view ads. Conversely, the paradox also works backward as well: when there are more ads, there are more online users, and they become more exposed to micro-targeting. In either case, there is a clear mutually beneficial relationship between the users and the social media companies. Chapter 4 (the analysis section) will present the application of this conceptual model on the CA scandal and show the influence of micro-targeting on American citizens' Facebook usage.

Chapter 3- Research Design and Data Collection

3.1. Justification for the Research

In the analysis, the CA scandal constitutes a single case study for a thorough examination. Focusing on a single case offers a unique opportunity to research the scandal in detail and gain more insights into the world of privacy. The case has been the most popular data breach in the history of Facebook. Not only in terms of individual privacy but also politically, the CA scandal is has a huge impact on society as a whole. One of the main reasons why the case is very controversial was because of its political repercussions in the US and the world. It is no doubt that American elections are of great importance to international relations and that democratic values are the building blocks for Western liberal world order. Therefore, a data breach of such great nature can be also considered as a breach of the US democracy and its democratic foundations. In the case of CA, there is a partnership between Facebook and CA in obtaining user information for political ends. It is therefore a distinct case for many disciplines such as political science and cybersecurity. In terms of the privacy viewpoint, the case is also relevant to public administration as individual behavior is the unit of analysis in this research.

According to Lijphart (1917), there are six categories of case studies. These are atheoretical, interpretative, hypothesis-generating, theory-confirming, theory-infirming, and deviant case studies (Lijphart, 1917, p. 691). The CA scandal falls into the fourth category. A theory-confirming case study implies that the case either confirms or enhances the existing theory, aiming to show what is further developed (Lijphart, 1917, p. 692). It provides additional explanations or insights which have not been considered before. Theory-confirming cases do not tend to produce new hypotheses but they "strengthen the proposition in question" (Lijphart, 1917, p. 692). In this way, a detailed description and comprehensive investigation of the case are guaranteed. The CA scandal is a theory-confirming case due to two reasons. First, the case goes beyond only explaining how the scandal emerged. The case puts together the relevant concepts and produces the micro-targeting paradox, a new concept arguing that micro-targeting is not only exercised by companies but it is also a practice that users appreciate. Although micro-targeting has deceptive and manipulative characteristics, users are also responsible for their own actions. Users react positively to micro-targeting on Facebook as it is easier for them to reach their preferred item. They click on the advertisements that are offered to them without thinking too much about how such advertisements appeared on their main page. They also tend to give out their personal information to online websites to make use of the benefits provided. In the case of Facebook, users can decide to have a public or private profile. Even though this selection limits the information that is visible to other users, Facebook still has the

personal information of the user. What is important to understand is the following: the problem with data breaches is not that users who have public profiles are more exposed to the breach than those who have private profiles. A profile status does not matter when a data breach occurs. The issue is that Facebook already collects and stores data if the users provide their information. Then, when a data breach such as the CA occurs, the exposed user information does not matter in terms of public or private user profiles. Therefore, it does not make a difference to have public or private profiles in the context of data breaches. Profile status only determines the information that other users can see. In this case, the only way for users to not suffer from data breaches is to not have a profile at all. This aspect is usually ignored in the existing literature as there is a focus on the understanding that limiting the visibility of information to others can help avoid data breaches. The conventional perspective focuses on privacy from a more superficial way. However, the CA scandal shows a new dimension of privacy, one that is paradoxical. People seek privacy, yet, they create social media accounts by willingly providing their personal information.

The second reason why the CA scandal is a deviant case is concerning the powerful position of Facebook over the globe. Even though it is a social media company, its role in the 2016 US presidential elections flared up ideas about Facebook's political engagement which is essentially not what the company is entitled to do. Facebook is one of the most popular social networks in the world and has the largest user base thus far (Tankovska, 2021). Its users are increasing day by day and this, in turn, gives Facebook a very powerful position and responsibility in controlling user-generated data. Conventionally, information gathering is a practice that is done by intelligence agencies. Nowadays, Facebook also collects data and people are aware that they provide their personal data. Users are the actors who start the process of online data gathering. Although CA was the data company that utilized Facebook user information, the source was Facebook, and the root source was Facebook user engagement and activity. It is especially this paradoxical nature of privacy and micro-targeting that makes the CA scandal interesting to examine.

3.2. Methodology, Data Collection, and Operationalization

While conducting the research, Facebook users in the US are the center of attention. As the case description section will mention, American users constitute the largest user base of Facebook. In addition, more than the users of any other country, American users suffered the most from the scandal. Facebook announced that CA held the data of over 87 million users, around 70 million of users being in the US (Horwitz, 2018). These statistics show that American users have been the most manipulated population by micro-targeting practices compared to other countries' users. The

scandal questioned the US privacy laws and how such a massive breach went undetected by the government for five years. Given the governmental processes on the scandal, conducting a textual content analysis fits the best for this research. Official court hearings on the issue by the US Federal Trade Commission, government reports, and the testimony of Mark Zuckerberg, Aleksandr Kogan, and Christopher Wiley who were responsible during the time of the breach are valuable to take into consideration. Moreover, since the hearings were recorded by the government, the research also includes the videos of these court sessions. The research furthermore makes use of relevant academic articles. Looking at these data is necessary since they offer a deep understanding of the scandal and the relationship between Facebook, CA and individual privacy, and user behavior. In light of the data collection, there are two indicators in the research. First, depending on the testimonies, privacy-related statements will be blended into the research. The main reason for this is to show how the scandal impacts American Facebook users and how they react to it. In this way, identifying the user behavior will be possible. Second, the change in user behavior has four categories: complete disengagement from Facebook by deleting accounts, deactivating accounts, adjusting privacy settings, and continuance of usage (Brown, 2020). If users disengage themselves from Facebook, it leads to a decrease in Facebook usage. Conversely, if users continue using Facebook, the usage remains as it is or can increase if more individuals join. With regard to the privacy settings adjustment, this category also acts in the same way as in the previous category. Changing privacy settings and transforming the account into a private profile does not make any difference in terms of Facebook usage. It only limits the visibility of the profile's content to other users. Facebook still holds user data regardless of the profile being public or private.

The CA scandal is an event based on micro-targeting. A single case is examined to observe the practice of micro-targeting and its effects on Facebook user engagement in the US. During the research, the micro-targeting scandal of CA is the independent variable. The dependent variable is Facebook user behavior in the US. American users are the baseline as first, Facebook is a powerful American company and second, the most impact was seen in the US. Moreover, while the unit of analysis is the individual behavior, the unit of observation is the customer base. In the former, there is a focus on individuals' engagement on Facebook. This is measured through the changes in the customer base with regard to the scandal. The unit of analysis and observation differ from one another due to the availability of the data and the method that is used in the research. To assess this case, there are two points worth noting. First, the research does not aim to assess Facebook user engagement based on individual responses, but takes a holistic view on the continuing of user engagement; the reason being the micro-targeting paradox. Therefore, the official court trials

become important sources to acquire knowledge on the behavior of American users through the statements during the hearings. Second, as an essential procedure of textual content analysis, the research includes the relevant discussions of the analysis section in the appendix, outlining the actors' statements. There will be direct quotations from the hearings collected in a table, making it easier and clearer for the reader to follow. Even though individual responses through interviews would generate more accurate results on observing user behavior, it is difficult to identify those who were directly affected by the scandal in the US. It is also problematic to conduct interviews given Facebook's large user base in the US. As a compensation for this weakness, the research instead uses various scholars who have conducted in-person interviews with Facebook users as secondary sources. The researcher acknowledges that the inability to receive personal responses from the users is the limitation of this thesis and can be risky in terms of validity and reliability. Yet, the current research is valuable for identifying a phenomenon that has been neglected thus far. The micro-targeting paradox is not a concept that has been explicitly stated in the previous literature but was rather mentioned under the privacy scholarship (Barnes, 2006; Boyd, 2012; Choi et al., 2018; Duggan & Smith, 2016). The main strength of this thesis is to make clear and visible that the micro-targeting paradox emerges as a combination of many privacy concepts discussed above. It is also another strength that the research recognizes the micro-targeting paradox in explaining the mutually beneficial relationship between micro-targeting and user engagement. This relationship becomes clear in the following section, proceeding with the case description.

3.3. Case Description- Cambridge Analytica scandal

CA is a data broker firm in the UK that also operates in the US. It is a branch of a parent firm called SCL Group which consists of different sections from SCL Elections to SCL Defense (Medium, 2017). Concerning the scandal that the company was involved in micro-targeting practices in political elections, it is important to note that the research is interested in its impact on individuals from the privacy viewpoint, rather than its political aspects.

The Psychometrics Center of the University of Cambridge conducted a personality test in 2013 on Facebook. It was developed by data scientist Alexandr Kogan under a third-party app called "thisisyourdigitallife" (Wired, n. d.). 350.000 people participated in the US. This test evaluated the respondents' so-called OCEAN psychological profile. OCEAN stood for openness, conscientiousness, extraversion, agreeableness, and neuroticism (Isaak & Hanna, 2018, p. 57). Respondents' answers were correlated with their Facebook activity. Looking at these responses, "this work demonstrated that the OCEAN profile for any individual could be deduced reasonably

accurately by looking at these metrics and without using a formal psychographic instrument" (Isaak & Hanna, 2018, p. 57). In this test, there was no evidence that it reached data of respondents' families or friends. The University of Cambridge claimed that they refused to share their results with CA. After this survey, there was another research project initiated by the Global Science Research (GSR) with CA's cooperation (Manokha, 2018, p. 891). The aim was to "identify the parameters needed to develop the OCEAN profiles using a personality quiz on Amazon's Mechanical Turk platform and Qualtrics, a survey platform" (Isaak & Hanna, 2018, p. 57). What was different than the first research was the requirement that the users had to access Facebook first which would eventually authorize the GSR to have access to the personal data of the respondents and their friends. Consequently, CA suddenly held data coming from millions of Facebook users, without their legitimate consent. Through the survey, CA was able to reach people's data who did not even participate in the survey. Aleksandr Kogan sold the data to CA in order for them to utilize it for US elections. Importantly, the OCEAN analysis had links to Ted Cruz's and Donald Trump's campaigns because the app had connections with the targeted messages that were used in their campaign projects (Isaak & Hanna, 2018, p. 57). In the end, the "thisisyourdigitallife" app gathered the personal data of 87 million Facebook users, even though only 350.000 people participated in the personality survey while 270.000 people downloaded the app (Horwitz, 2018). Personal data included locations of the users, liked pages, profile contents, current cities, and even in some cases their news feeds (Rosenberg, Confessore & Cadwalladr, 2018).

These two projects had the same goals. As indicated by CEO of CA Alexander Nix, "the key was to identify those who might be enticed to vote for their client or be discouraged to vote for their opponent" (Isaak & Hanna, 2018, p. 57). The first incident arose in 2015 where a journalist reported that CA was illegally harvesting personal data from Facebook and using them for the Ted Cruz campaign (Svitek & Samsel, 2018). Many journalists continued reporting CA and argued that collected data was also used in the Brexit campaign (Cadwalladr & Graham-Harrison, 2018). In 2018, Christopher Wylie, a former CA employee, exposed the firm and came out as a whistleblower (Cadwalladr & Graham-Harrison, 2018). The Guardian reporter Carole Cadwalladr's news report has gained huge attention and led to strong public debate. Facebook was highly criticized by the public and the company's reputation suffered. Mark Zuckerberg, the CEO of Facebook came before the US Congress and had a trial regarding the data breach. The Federal Trade Commission (FTC) fined the company with 5 billion dollars, which was the largest fine for a violation of any kind in the US government thus far (Snider & Baig, 2019). Yet, according to FTC Commissioner Rohit Chopra, the fine was less than it was supposed to be (Hu, 2020, p. 3). After the allegations

and the scandal, CA announced bankruptcy after the resignation of the CEO Alexander Nix. After the newspaper articles on the scandal, Facebook's market value decreased tremendously and 3 million users in Europe left Facebook (Neate, 2018). Zuckerberg then asserted that the company was aiming to hire 20.000 new personnel for security and privacy-related issues (Neate, 2018).

Considering these events, the CA scandal is relevant for this research as it is based on the relationship between micro-targeting and social media usage by drawing attention to individual behavior. The popularity and seriousness of the case come from the fact that it is identified as the biggest data leak so far in Facebook's history. Not only in terms of Facebook's financial loss but also the loss of user trust gave the company a big hit. Its involvement in micro-targeting activities portrayed Facebook as an unreliable social media platform among the public. This can also be illustrated by the #deletefacebook movement which received popular support (González-Bailón & Gorham, 2018). Therefore, what makes the case unique in this paper's context is that it explains individuals' Facebook usage when privacy breaches such as the CA scandal occur.

Chapter 4- Analysis

Throughout the chapter, the research is interested in the US court hearings regarding the CA scandal. Mark Zuckerberg has given two testimonies regarding the scandal. These were in the US Senate Commerce and Judiciary Committees, and US House Energy and Commerce Committee respectively. These court hearings lasted for over nine hours and during the sessions, all the members of the committees had the opportunity to ask questions to Mark Zuckerberg. Moreover, the research also includes the testimonies of Aleksandr Kogan, the app developer, and Christopher Wiley, the whistleblower and former employee of CA. Their testimonies are relatively shorter, lasting for just over one and two hours respectively. Including these testimonies in the analysis is crucial since the issue also gains a legal perspective. All the actors responsible for the scandal and them appearing before the court with their official statements are first-hand sources. They offer a more detailed understanding of the issue depending on the positions of the actors. Importantly, all the court sessions have official transcripts. The Washington Post published both of the Zuckerberg trial transcripts on the scandal. Similarly, the transcripts of the Kogan and Wiley trials are also visible on C-Span. Due to the importance and large volume of the Zuckerberg testimonies, the analysis starts with the Senate and House hearings on April 11th and 12th in 2018. First, the analysis section will unpack the official statements made by the responsible actors after the breach and then analyze the change in Facebook usage of American citizens in the aftermath of the scandal with secondary data.

4.1. The Zuckerberg Senate Hearing

At the beginning of the trial, Senator John Thune states that Facebook is an extraordinary discovery.[1] He draws attention to its user base, yet, indicates that he has concerns over how Facebook users can shape its decisions without being manipulated by micro-targeting activities. He further goes on to ask what Facebook will do in order to protect user data. His remarks matter in the sense that it shows the user perspective and the importance of individual privacy. In this way, Senator Thune also means that Facebook bears a huge responsibility to make adjustments in their regulations regarding data privacy. Senator Grassley continues with his opening comments by indicating that Facebook has data points on individuals as they click on advertisements, provide their locations and the like.[2] He asserts that this is how Facebook makes revenue, which 98% of its 40 billion dollars revenue in 2017 coming from online advertisements on Facebook and Instagram.[3] Senator Grassley acknowledges that growth and innovation will become the reality if there is more data collection, however, the abuse of such data remains alarming.[4] Following his statement, Zuckerberg starts with his official testimony about Facebook's vision of connecting people as well as its ability to make positive changes for society overall.[5] He then apologizes for the CA data breach and indicates his commitment to solving the issue.[6] His statement follows with the explanation of how Facebook approached the data breach issue, saying that when Facebook first contacted CA about the scandal, CA answered that they deleted all the data they had.[7] However, this was not the case. Moreover, Zuckerberg argued that Facebook is running investigations over the app developers who have access to a huge amount of user data, and banning them if they are misusing individuals' data.[8] His testimony, therefore, hints cooperative steps towards protecting individual data.

---

[1] *see Appendix 1, the section on Senator Thune.*

[2] *see Appendix 1, the section on Senator Grassley.*

[3] *see Appendix 1, the section on Senator Grassley.*

[4] *see Appendix 1, the section on Senator Grassley.*

[5] *see Appendix 1, the section after Senator Grassley, under the section of Zuckerberg's response.*

[6] *see Appendix 1, the section after Senator Grassley, under the section of Zuckerberg's response.*

[7] *see Appendix 1, the section after Senator Grassley, under the section of Zuckerberg's response.*

[8] *see Appendix 1, the section after Senator Grassley, under the section of Zuckerberg's response.*

After Zuckerberg's official testimony, Senator Grassley starts questioning the CEO on why Facebook does not block the third parties who want to achieve user information.[9] He also asks what the company's responsibility is regarding its terms and conditions. Zuckerberg answers that users have control over their data and content before they share specific content, and they can do this by choosing whom they can share it with.[10] In this regard, the users can either share their content publicly, with their friends or with people they select. This remark is important since it shows that people are responsible for their data. If they choose to share content, they can simply share it in any way they want. Concerning Facebook's terms and conditions, Zuckerberg mentions that creating very long terms and conditions is not useful for users as they tend to get confused while reading them and/or that most of them do not even read that section.[11] It is essential for users to know what they agree to before they share their data. In this respect, users also bear the responsibility of controlling their data. If they choose to agree, then they are also accountable for the data breach since they willingly provided their data and agreed to the terms of using Facebook. This gives birth to the micro-targeting paradox, providing evidence for the mutually reinforcing link between user engagement and micro-targeting. Subsequently, the hearing moves on with Senator Nelson's question where he gives an example from his own experience. While he was discussing a type of chocolate with his friends on Facebook, he says that he starts seeing chocolate advertisements on his main page.[12] From this example, he asks if there will be an option for Facebook to offer another version of itself where people can pay to not receive advertisements.[13] Zuckerberg responds that users can "turn off third-party information" if they do not want to receive advertisements.[14] Moreover, he discusses the overall feedback that Facebook gets from its users suggest that people like to see relevant ads rather than irrelevant ones.[15] Even though users might have doubts over the use of their information for showing them relevant ads, they still prefer Facebook to show ads that are relevant to them. This is important first-hand evidence for the research because it supports the micro-targeting paradox.

---

[9]*see Appendix 1, the second section on Senator Grassley.*

[10]*see Appendix 1, the section on Zuckerberg's response to Senator Grassley.*

[11]*see Appendix 1, the section on Zuckerberg's response to Senator Grassley.*

[12]*see Appendix 1, the section on Senator Nelson.*

[13]*see Appendix 1, the section on Senator Nelson.*

[14]*see Appendix 1, the section on Zuckerberg's response to Senator Nelson.*

[15]*see Appendix 1, the section on Zuckerberg's response to Senator Nelson.*

Continuing with Senator Hatch's question, there is the question of data monetization. He argues that if a service is free of charge, then there is another way of making profit.[16] He asks what the business model of Facebook is.[17] Zuckerberg replies "Senator, we run ads" and once again, asserts that Facebook does not control user data. Instead, he highlights, users are the ones who have complete control over their data.[18] They can adjust their settings according to how they want to share their content. However, there is an important distinction to make. Senator Wicker asks an interesting question regarding Facebook's data collection. That is, whether or not Facebook collects users' chat history or calls who have Android phones.[19] Zuckerberg mentions that Facebook has an app called Messenger and that before users join, they can synchronize their text messages in order to make their communication easier with other people.[20] In this case, if users opt-in to the service, they do provide their personal information such as the accounts of their friends or pictures. On the other hand, if users do not agree to the synchronization, then they have to specifically mention that in the beginning. This feature gives users control of information as Zuckerberg argues. It is depending on the user how they want to control their information. Similar to Senator Wicker's point, Senator Graham discusses the terms and conditions document of Facebook. He reads one of the terms out loud and says "I'm a lawyer. I have no idea what that means. But, when you look at terms of service, this is what you get. Do you think the average consumer understands what they're signing up for?".[21] Zuckerberg responds by saying that people do not even read the entire document when they sign up. Hence, this situation leads to inaccurate information revolving around privacy concerns. Even though people want privacy, meanwhile they do not inform themselves on these services and they still engage in these platforms, leading to the micro-targeting paradox. Such mistakes also apply to micro-targeting practices since most people do not even realize that their thoughts are being influenced through targeted advertisements. Zuckerberg argues that there are controls that people can use in order to direct their activity on Facebook. They help to see how the individual content and information is being used. Yet, many people do not make use of those tools because they benefit from the engagement and being one click away from the services Facebook

---

[16]*see Appendix 1, the section on Senator Hatch.*

[17]*see Appendix 1, the section on Senator Hatch.*

[18]*see Appendix 1, the section on Zuckerberg's response to Senator Hatch.*

[19]*see Appendix 1, the section on Senator Wicker.*

[20]*see Appendix 1, the section on Zuckerberg's response to Senator Hatch.*

[21]*see Appendix 1, the section on Senator Graham.*

provides. In sum, as much as Facebook is responsible for safeguarding individuals' data, individuals are also in control of their own information.

The hearing moves on with Senator Cornyn's turn to ask questions. He asks what happens if individuals decide to delete their Facebook accounts, and that whether or not third parties would have individuals' data.[22] Zuckerberg replies that Facebook sells data neither to third parties nor anyone else.[23] What Facebook allows, he explains, is matching advertisers with individuals based on their shared relevant content.[24] This ensures people getting targeted advertisements and keeps them more engaged on the platform. Given from one of Zuckerberg's previous answers that users would like to see targeted advertisements, rather than irrelevant ones, individuals benefit from micro-targeting. Likewise, Senator Whitehouse also mentions what the status is of the third parties when Facebook bans them.[25] Zuckerberg clarifies that when Facebook found out that CA was obtaining user data, Facebook did not immediately ban CA from the platform.[26] Instead, Facebook asked CA to delete all the data they had over users. It was only when Facebook discovered that they were an advertiser did Facebook ban CA and its parent company. This means that CA was banned from doing business with Facebook, however, not banning personal accounts specifically. Since these technicalities are not clear to users, Senator Whitehouse states

> "…all I wanted to establish with you is that that document that Senator Graham held up, that is not a negotiable thing with individual customers; that is a take it or leave it proposition for your customers to sign up to, or not use the service".[27]

His proposal is crucial for building clear lines of communication between Facebook and its users. Putting weight on users' shoulders with Facebook's overly complicated terms and conditions further enhances the micro-targeting paradox as it leads users to sign up for services that they do not have information on. If Facebook has the responsibility of protecting individual data, it also should clearly indicate how their information will be used. Senator Lee's question also supports this

---

[22] *see Appendix 1, the section on Senator Cornyn.*

[23] *see Appendix 1, the section on Zuckerberg's response to Senator Cornyn.*

[24] *see Appendix 1, the section on Zuckerberg's response to Senator Cornyn.*

[25] *see Appendix 1, the section on Senator Whitehouse.*

[26] *see Appendix 1, the section on Zuckerberg's response to Senator*

[27] *see Appendix 1, the section on Senator Whitehouse*

argument. He suggests that Facebook's free-of-charge feature comes with its alternatives, that is, monetizing data.[28]

Following Senator Hatch's question, Senator Lee asks for a couple of examples of what kinds of data Facebook collects and how these data are utilized.[29] Zuckerberg responds is that Facebook collects two types of data.[30] The first one consists of what users share, for instance, their pictures, likes, or posts. Individuals have full control over their data in the first category. Additionally, they can delete any of their data at any time. The second category includes, as Zuckerberg states, "specific data that we collect (Facebook) in order to make the advertising experiences better, and more relevant, and work for businesses".[31] In this case, if users click on the specific advertisement that Facebook offers and they get directed to a new page, this means that micro-targeting achieved its purpose. In turn, the second category data is being collected to make the services more useful and engaging to the user.[32] Altogether, users and businesses benefit from targeted advertisements since first, users get more relevant ads and engage on the platform, and second, advertisers perform better and can assist the users more accurately in what they would like to see. Zuckerberg explains that users also have full control over the second category.[33] Individuals can adjust their settings that would limit Facebook's collection of their data. However, the advertisements they see will be irrelevant and even random in most cases. This is the reason why most people do not want to limit Facebook's data collection. Overall, from Zuckerberg's statements, in both categories, users have complete control over their information and its status. If users willingly make their information available to Facebook in order to use its services, then they will see targeted advertisements based on their activity on Facebook. Most individuals prefer this option because it is valuable to them.

An important question on whether or not Facebook is safe has been proposed by Senator Fischer.[34] According to Zuckerberg, given all the controls that Facebook has, Facebook is safe.[35]

---

[28]*see Appendix 1, the section on Senator Lee.*

[29]*see Appendix 1, the section on Senator Lee.*

[30]*see Appendix 1, the section on Zuckerberg's response to Senator Lee.*

[31]*see Appendix 1, the section on Zuckerberg's response to Senator Lee.*

[32]*see Appendix 1, the section on Zuckerberg's response to Senator Lee.*

[33]*see Appendix 1, the section on Zuckerberg's response to Senator Lee.*

[34]*see Appendix 1, the section on Senator Fischer.*

[35]*see Appendix 1, the section on Senator Fischer.*

They not only make people feel secure but people also want to have those options. Having controls help individuals to achieve their desires which people expect from using the service. Once individuals sign up for Facebook, they have access to these controls in order to make their information visible to people that they want, and they have full control of their shares. Moreover, according to Senator Moran, Facebook is in a debatable position in complying with the FTC consent order that has been in place since 2011. He poses a question to Zuckerberg directly on the data breach of 87 million Facebook users. He asks "how does the case of approximately 87 million Facebook friends having their data shared with a third party due to the consent of only 300,000 consenting users not violate that agreement?".[36] Zuckerberg suggests that the platform worked in the following way: people could join an app and provide their information as well as the information of their friends.[37] Those individuals who joined the app once more had specific settings for the feature. Facebook explained how the platform was functioning, and people decided to consent. Senator Moran continues by asking if it is appropriate for Facebook to gather information on those who did not consent. This is involving individuals that did not particularly consent, but eventually had their data breached just because their friends consented. In order words, through the individuals who consented, Facebook was able to reach information on the friends of those users. Zuckerberg replies that

> "…you might want to have a calendar that can have your friends' birthdays on it, or you might want your address book to have your friends' pictures in it, or you might want a map that can show your friends' addresses on it. In order to do that, we needed to build a tool that allowed people to sign in to an app and bring some of their information, and some of their friends' information, to those apps. We made it very clear that this is how it worked, and — and when people signed up for Facebook, they signed up for that as well."[38]

From his answer, the problem is not that there is an illegitimate collection of personal data. Instead, what drives such thoughts come from users' lack of knowledge of the services that Facebook provides. As mentioned earlier, most individuals do not even read the terms and conditions when they sign up for Facebook. If people (unknowingly and/or unawarely) consented to provide their information to the app developed by Aleksandr Kogan, they are as responsible as Facebook on the CA scandal. Even though they did not consent for their information to be sold to CA, they did

---

[36]*see Appendix 1, the section on Senator Moran.*

[37]*see Appendix 1, the section on Zuckerberg's response to Senator Moran.*

[38]*see Appendix 1, the section on Zuckerberg's response to Senator Moran.*

consent to the terms of the app. In essence, the first and foremost responsibility of users is to read the terms of the services they sign up for, and then decide whether they want to join. In this way, the misinformation could be heavily reduced on data-related issues.

One important instance concerning surveillance practices has been brought up by Senator Heller. She makes remarks to Zuckerberg's words where once he said that users would not count on Facebook if they thought that Facebook was giving up their information to intelligence agencies.[39] Zuckerberg claims that Facebook does not sell data to anyone. He emphasizes the distinction between government surveillance and Facebook. Unlike the former, on Facebook, for any content that is shared, users have control over it.[40] Individuals have access to view what Facebook might know about them and they can delete all that information. Essentially, Facebook has a tool for people to download the data that Facebook has over them.[41] Throughout the hearing, Zuckerberg mentions this tool twice, which is interesting to add since even the senators are not aware that such control exists. Furthermore, another crucial statement comes from Senator Tillis in a way that supports the 'control' argument. He expresses that he has spent the majority of his life in the data analytics realm and is aware of how data-related issues might be confusing to individuals. During his remarks, he makes important notes on individuals' responsibility of controlling their information on Facebook. He suggests

> "But go to the privacy tab. If you don't want to share something, don't share it. This is a free service. Go on there and say I don't want to allow third party search engines to get in my Facebook page. Go on there and say only my friends can look at it. Go on there and understand what you're signing up for. It's a free app. Now you need to do more."[42]

In that regard, what is clear from Senator Tillis' remarks is that users have all the necessary tools and information before they sign up for services. They can choose not to receive targeted advertisements if they do not want to. They can also adjust their accounts according to their preferences. Making use of social media is appealing to individuals, yet, in general, they do not even know what they sign up for. Due to this exact lack of knowledge, users demonize Facebook or other social media companies although they are the ones who first-handedly provide information to those services after all. This issue is critical when it comes to public debate and how the media

---

[39] *see Appendix 1, the section on Senator Heller.*

[40] *see Appendix 1, the section on Zuckerberg's response to Senator Heller.*

[41] *see Appendix 1, the section on Zuckerberg's response to Senator Heller.*

[42] *see Appendix 1, the section on Senator Tillis.*

portrays Facebook and CA as the only ones to blame. It is also the individuals who sign up for the service, provide valuable data, and keep their engagement on Facebook. In this case, making sure that individual data is secure becomes possible if individuals do not sign up at all which goes beyond the scope of this thesis.

In terms of Facebook usage, during his turn in the hearing, Senator Johnson starts questioning how many people actually read the terms and conditions. He then asks critically, "With all this publicity, have you documented any kind of backlash from Facebook users? I mean, has there been a dramatic falloff in the number of people who utilize Facebook because of these concerns?".[43] This question is essential to understand user engagement after the scandal to make an assessment of the effect of targeted advertisements on the users. Surprisingly, Zuckerberg responds that there has not been a decline in Facebook usage.[44] The CEO claims that there have been instances where some users were motivating others to delete their accounts, yet there has not been a huge decline overall. Further, Senator Johnson claims that users seem to be not worried about the scandal and about Facebook as they are not disengaging from the platform.[45] Zuckerberg responds that people do get worried about their data, and Facebook should put more effort into providing its user the best service.[46] During the conversation, Senator Johnson states that "But it seems like Facebook users still want to use the platform because they enjoy sharing photos and they share the connectivity with family members, that type of thing. And that overrides their concerns about privacy".[47] This is an important insight of the hearing regarding Facebook usage and why it did not decline. In fact, Senator Johnson's and Zuckerberg's conversation gets even more interesting when the Senator asks if Zuckerberg has thought of creating a new version of Facebook if Facebook cannot stop the data flow to advertisers.[48] This version would require users to pay a certain amount of money to not receive targeted advertisements. The question has been proposed before during the hearing, however, what differs this time is Zuckerberg's remarks. He states that even if Facebook creates that version, the free version would be the best because in general people do not want to pay

---

[43] *see Appendix 1, the section on Senator Johnson.*

[44] *see Appendix 1, the section on Zuckerberg's response to Senator Johnson.*

[45] *see Appendix 1, the section on Senator Johnson.*

[46] *see Appendix 1, the section on Zuckerberg's response to Senator Johnson.*

[47] *see Appendix 1, the section on Senator Johnson.*

[48] *see Appendix 1, the section on Senator Johnson.*

for a service.[49] Meaning that there are two conclusions to make. First, Facebook is built in a way to maximize user engagement. This is ensured if people stay logged into Facebook for a long time. Micro-targeted advertisements, therefore, serve well to Facebook's goal of increasing user engagement and make a profit. Second, as Zuckerberg suggests, people appreciate seeing relevant advertisements targeted to their specific needs. In that case, both Facebook and its users benefit from the service, and this mutually reinforcing relationship ends up with increasing user engagement. Users do not leave the platform despite the scandal. Facebook's previous incidents regarding data privacy can also support this argument. That being, although Facebook has been through many legal challenges, its user base is growing day by day reaching over 2 million users over the world (Tankovska, 2021). In sum, if people did not appreciate it or benefit from it in the first place, they would not sign up for the service. The fact that they are still engaged on Facebook is the paradoxical effect of micro-targeting on its users.

Regarding the specifics of how Facebook works, Zuckerberg comments that Facebook offers two options to its users. These are deactivating or deleting an account. His answer is related to Senator Capito's question on if Facebook could recreate an account that has been deleted.[50] The first option (deactivation) permits people to "shut down or suspend" an account.[51] If users decide to deactivate their account, their information does not get deleted and whenever they decide to log into their accounts their data stays the way it is. The second option, on the other hand, (deletion) will completely erase all the data of the user, and in this case, it is irreversible.[52] To put it differently, if users want to go back to Facebook, they will have to create a new account since their old account will be non-existing anymore. Following from the early remarks that users do not leave Facebook despite the CA scandal, leaving corresponds to deleting the account. People might deactivate their accounts or use Facebook less frequently. However, this does not mean that they are disconnected from the platform for good. According to numerous statistics reports after the scandal broke out, most American people either started using Facebook less often or deactivated their accounts for a while. In general, users stayed on Facebook despite the scandal due to its various benefits.

In conclusion, remarks in Mark Zuckerberg's Senate hearing support the claim that users keep engaged on Facebook because they find targeted advertisements relevant and useful features.

---

[49]*see Appendix 1, the section on Zuckerberg's response to Senator Johnson.*

[50]*see Appendix 1, the section on Senator Capito.*

[51]*see Appendix 1, the section on Zuckerberg's response to Senator Capito.*

[52]*see Appendix 1, the section on Zuckerberg's response to Senator Capito.*

User engagement on Facebook did not decline specifically because of the CA scandal. Instead, despite all the privacy concerns raised by the US government, users still keep their accounts on Facebook. Many senators asserted that there is a breach of Facebook user trust in the aftermath of the scandal. However, lack of trust is not equivalent to less Facebook usage. It could be possible for users to feel skeptical and suspicious about providing their data to Facebook and still keeping their accounts active. In that case, the bottom line which has been highlighted during the whole hearing is that people have the option to adjust their data on Facebook according to their preferences. If users feel concerned that the third parties use their information for micro-targeting purposes, they have the option to not join the platform. Contrarily, when users decide to join the platform, they also make use of micro-targeting with the targeted advertisements tailored specifically for them. As a consequence, these aspects give rise to the micro-targeting paradox which the research also refers to as the necessary evil.

4.2. The Zuckerberg House Hearing

On the next day, Mark Zuckerberg testified once more before the US House Energy and Commerce Committee. This hearing had very similar traits to the Senate hearing with comparable questions posed by the congressmen and congresswomen. In that regard, the research focuses on the data that help to get a deeper knowledge of Facebook and how it operates for user engagement purposes. The hearing starts with Congressman Walden's opening statement and he focuses on the disturbance of CA's activities. Subsequently, Congressman Pallone raises a question regarding Facebook's willingness to provide more privacy to its users.[53] Zuckerberg answers that his team made changes that allow users to have more privacy and meanwhile limit third parties' access to user data.[54] Congressman Pallone follows up with another question, asking "How can consumers have control over their data when Facebook doesn't have control over the data itself?".[55] Zuckerberg replies that Facebook allows its users to move their data from other apps to Facebook because most users want to have the ability to do such adjustments.[56] He acknowledges that this feature might be abused as well, therefore Facebook limited the data that advertisers can obtain. Furthermore, even though users can choose to adjust their profiles to a more private one, Congressman Barton argues

---

[53]*see Appendix 2, the section on Congressman Pallone.*

[54]*see Appendix 2, the section on Zuckerberg's response to Congressman Pallone.*

[55]*see Appendix 2, the section on Congressman Pallone.*

[56]*see Appendix 2, the section on Zuckerberg's response to Congressman Pallone.*

that it is difficult to do it.[57] Users in his view have to spend a lot of time to make it happen. This difficulty might cause users to not change their settings. It can also be that users do not want to adjust their profiles not only because it is difficult to change everything but also because they enjoy the perks of having a public profile for more interaction. When the latter is the case, they contribute more to the micro-targeting paradox because they will receive more ads. In the following minutes, Congressman Shimkus asks a clarification question on how Facebook tracks information even when the user is not logged in.[58] Zuckerberg explains that Facebook tracks certain information for security purposes to make sure an individual does not download publicly shared information from users' pages.[59] These individuals might not have Facebook accounts but can have access to publicly shared information. Therefore, Facebook, as Zuckerberg suggests, has an off-line tracking feature for security measures.[60] On the other hand, Facebook also provides

> "an ad network that third-party websites and apps can run in order to help them make money. And those ads — you know, similar to what Google does and what the rest of the industry does — it's not limited to people who are just on Facebook. So, for the purposes of that, we may also collect information to make it so that those ads are more relevant and work better on those websites. There's a control that — for that second class of information around ad targeting — anyone can turn off, has complete control over it."[61]

Zuckerberg's explanation supports the previous claims he made in the Senate hearing that users can change the settings if they do not want to receive ads. However, as suggested earlier, most users choose not to do it because they make use of the ad service. Congressman Burgess also raises the same issue that he does not look at the terms and conditions himself when he signs up for an app.[62] Zuckerberg approves that most of the time it is indeed the case that users do not read what they are agreeing to.[63] Hence, it is crucial that users have knowledge of the terms and conditions of an application to make sure it is in line with their expectations from the app.

---

[57]*see Appendix 2, the section on Congressman Barton.*

[58]*see Appendix 2, the section on Congressman Shimkus.*

[59]*see Appendix 2, the section on Zuckerberg's response to Congressman Skimkus.*

[60]*see Appendix 2, the section on Zuckerberg's response to Congressman Shimkus.*

[61]*see Appendix 2, the section on Zuckerberg's response to Congressman Shimkus.*

[62]*see Appendix 2, the section on Congressman Burgess.*

[63]*see Appendix 2, the section on Zuckerberg's response to Congressman Burgess.*

A striking discussion regarding Facebook usage has been addressed by Congresswoman Degette during the hearing. She asks "Now, since the revelations surrounding Cambridge Analytica, Facebook has not noticed a significant increase in users deactivating their accounts. Is that correct?".[64] Zuckerberg states that it is correct.[65] She further asks "Now, since the revelations surrounding Cambridge Analytica, Facebook has also not noticed a decrease in user interaction on Facebook. Correct?".[66] The answer is yes once more.[67] Considering these last two questions, there is direct evidence that Facebook usage did not decline in the US after the CA scandal. This finding is core for the research to explain why users do not leave Facebook. The answer is users' appreciation of Facebook and how it operates. According to Zuckerberg, Facebook's advertising platform provides the best experience for its users as users value seeing targeted advertisements. Even though users can limit the advertisements they receive, mounting evidence shows that they prefer not to. In that regard, this situation gives rise to the micro-targeting paradox, supporting the research's hypothesis. Similarly, later on in the hearing, Congressman Guthrie mentions the advantages of targeted ads and how they make life easier.[68] He explains his own experience where he was planning to book a hotel in Florida and then receiving ads that showed the same hotel with the same price. He states

> "So I thought it was actually convenient. Instead of getting just an ad to someplace I'll never go, I got an ad specifically to a place I was — I was looking to go, so I thought that was convenient…We get to do that for free, because your business model relies on consumer-driven data."[69]

Moreover, he states that this did not happen on Facebook specifically, however, Facebook also uses the same strategies with targeted advertisements. These tools are not only applicable for Facebook but almost all of the companies in Silicon Valley, suggesting that Facebook is not unique in terms of the ads experiences. Zuckerberg agrees with this statement and indicates that their business model

---

[64]*see Appendix 2, the section on Congresswoman Degette.*

[65]*see Appendix 2, the section on Zuckerberg's response to Congresswoman Degette.*

[66]*see Appendix 2, the section on Congresswoman Degette.*

[67] *see Appendix 2, the section on Zuckerberg's response to Congresswoman Degette.*

[68]*see Appendix 2, the section on Congressman Guthrie.*

[69]*see Appendix 2, the section on Congressman Guthrie.*

based on ads yield the best service because of Facebook's mission of connecting people free of charge.[70] He clarifies a couple of general points one being

> "we already give people a control to not use that data and ads, if they want. Most people don't do that. I think part of the reason for that is that people get that if they are going to see ads, that they want them to be relevant. But the other thing is that our — a lot of what our business — what makes the ads work, or what makes the business good is just that people are very engaged with Facebook. We have more than a billion people who spend almost an hour a day across all our services."[71]

These claims are particularly relevant for understanding how the micro-targeting paradox works. Facebook provides users to adapt their settings to their preferences, and yet, a majority of users still do not use them. In turn, users become exposed to targeted advertisements and are active on Facebook for long periods of time. The chain reaction created by users' lack of using the necessary controls feeds the micro-targeting paradox and makes it important to take into consideration in explaining why Facebook usage did not decline even after the scandal. Nevertheless, such a cycle can only break if users do not join Facebook.

4.3. The Wiley Senate Hearing

During Christopher Wiley's hearing in the US Senate, the content of the questions is centered upon the political aspects of the scandal, especially regarding the US presidential campaign in 2016. The witnesses' testimonies are shaped around accusing Facebook of manipulating and persuading the voters to vote for a certain candidate. Dr. Mark Jamison draws attention to the transparency issue by arguing that users' information is being gathered without them even knowing how such action takes place (C-Span, 2018, 34:32- 34:36). Further, Dr. Eitan Hersh states that influencing elections should not be the job of Facebook. He claims that micro-targeting practices are ineffective in political campaigns (C-Span, 2018, 39:45- 40:01). Most importantly, there is no claim that this is the case for non-political content. The distinction Dr. Hersh makes is in line with the previous claims that users stay on Facebook because of the targeted advertisements that involve all kinds of content, and not necessarily political. In other words, Dr. Hersh only addresses the ineffectiveness of political ads and not other kinds of ads, supporting the previous findings on continuing user engagement. Senator Kennedy disagrees with Dr. Hersh's claim, saying that if companies such as CA and Facebook spend as well as make billions of dollars from online

---

[70] *see Appendix 2, the section on Zuckerberg's response to Congressman Guthrie.*

[71] *see Appendix 2, the section on Zuckerberg's response to Congressman Guthrie.*

advertising, then they must have trustworthy evidence (C-Span, 2018, 46:48- 47:15). In Zuckerberg's earlier statements in both the Senate and House hearings, he asserted that the entire business model of Facebook was based on running ads that are relevant to users' preferences. In this case, Senator Kennedy's point is confirmed.

As the hearing moves on, Senator Cornyn asks Wiley a question regarding the Zuckerberg Senate hearing. In that hearing, he indicated that Facebook may not sell data, but it "clearly rent(s) it". Regarding this conversation, Senator Cornyn asks Wiley how he views Facebook (C-Span, 2018, 01:11:35- 01:12:02). Wiley replies that Facebook is a platform that supports data usage (C-Span, 2018, 1:12:02- 1:12:08). He states, even though an actor cannot buy data by going on Facebook, "the layouts of people's profiles on Facebook make it very conducive to scraping data" (C-Span, 2018, 01:12:23- 01:12:30). In this case, third parties can utilize user data to show targeted advertisements to users, and this situation, in turn, leads users to spend more time on the platform because of the relevance of the content. Therefore, if all a platform needs is (utilizing) data to make a profit, the micro-targeting paradox becomes inevitable. From the societal perspective of social media use, Wiley suggests that people do not have the option to not use social media anymore. He gives the example of job hirings where employers see LinkedIn as a necessity to hire the candidates (C-Span, 2018, 01:13:26- 01:13:48). Concerning Senator Cornyn's follow-up question on the terms and conditions of Facebook, Wiley reiterates the previous point. He answers that users should have informed consent before they sign up (C-Span, 2018, 01:14:08- 01:15:04). Yet, the issue of social media developed into a situation where people are obliged to opt-in regardless to have jobs. Wiley states that

> "this narrative of consent is problematic in the sense that when people have to use these platforms, it does not matter whether or not they understand. If they have to use it to get a job, they will still use it. We are coercing people to hand over a lot of information…" (C-Span, 2018, 01:16:15- 01:16:48).

His statement suggests that users use platforms such as Facebook for the sake of using it, and not because they choose to. This leads to two problems: first, users become unaware of the terms and conditions of the services. As a consequence, they are not informed about the way the platform operates. Second, users develop an inaccurate understanding of social media and its usage. They become active users to fit in the digital environment. Both of these issues ultimately result in the micro-targeting paradox because once individuals are on the platform they are exposed to content that is created through their activity on Facebook. They become more engaged as they view more ads and content, and the usage, therefore, does not decline. Lastly, Dr. Hersh comments on Facebook by saying that he would not encourage people to use Facebook because of their business model, and he states he is surprised "by people's continuing interest in the company" (C-Span,

2018, 01:29:40- 01:29:45). His words have direct support for the micro-targeting paradox. He criticizes Facebook for collecting user data and utilizing it for micro-targeting. However, users remain engaged on Facebook, showing that users do not see such practices as problematic.

4.4. The Kogan Senate Hearing

Throughout the Kogan hearing, there has not been a lot of discussion on the user perspective of social media, however, there have been important remarks and views reported from the witnesses and Dr. Aleksandr Kogan. Predominantly, there has been great focus on data privacy issues and how to regulate companies such as Facebook to ensure user privacy in the US. Dr. Kogan starts his testimony at the beginning of the hearing by saying that he and his research team perceived collecting people's data was normal, and "people whose data was being collected knew it was regularly happening" (C-Span, 2018a, 17:00- 17:05). This statement provides a link to what previous literature calls privacy fatigue. People get used to and tired of hearing about privacy issues and therefore they develop immunity where they do not view data breaches as big issues anymore. He states that it is normal for tech companies to base their business models on utilizing data, however, users need to be well-informed about the terms of using platforms such as Facebook. The app he developed required Facebook users to have Facebook accounts, and users received terms and conditions before they agreed to use it. Zuckerberg claims that Dr. Kogan sold the data to CA, yet, there is a bigger issue regarding the scandal. This issue is related to users having proper information on the services that require data collection. If users are well-informed on what they sign up for, the micro-targeting paradox will be tackled. If users find it disturbing to share their data with third parties, then there will be less user engagement due to a lower number of users. Yet, this is not the case. Facebook usage did not decline even after the scandal. It is precisely because of the steady Facebook usage that the company is not keen to offer a new version of Facebook to its users, a platform where people can pay a subscription to not receive ads. In the current situation, it is not optimal for Facebook to create such a version because there is no loss in user engagement. Micro-targeting benefits the users, advertisers, and Facebook, giving rise to the micro-targeting paradox. Similar to Kogan's views, Dr. Ashkan Soltani's opening remarks sum up Facebook's corporate strategies. He discusses that the CA scandal should not come as a surprise and that its consequences are expectable. He suggests that Facebook has a business model that "pays developers for access to information to maintain a dominant position in the market" (C-Span, 2018a, 22:28- 22:39). Dr. Soltani cites an article which uncovered that third parties could still access user information even if they used Facebook's controls to block the data flow (C-Span, 2018a, 23:13- 23:24). This statement suggesting the opposite of Zuckerberg's claim that users have specific controls which block third parties' acquiring of individual data. Supporting Dr. Soltani's remarks, Dr. Kogan views Facebook

as a company that bases its strategy on keeping its user active on the platform (C-Span, 2018a, 29:58-30:16). The more the users stay online, the more ads will appear in users' feeds and the endless cycle of micro-targeting paradox is fulfilled. In another statement, Dr. Kogan comments that Facebook is aiming for "an addictive pattern of behavior" (C-Span, 2018a, 01:21:42- 01:22:00). Facebook's primary source of revenue is based on keeping its users engaged and online on the platform so that they can view more ads. More specifically, Facebook's entire business strategy depends on the micro-targeting paradox. Rather than bringing people and communities together, Dr. Kogan argues that Facebook is causing people to get addicted to the platform, and therefore needs to be regulated (C-Span, 2018a, 01:22:18- 01:22:21).

The hearings overall highlight huge evidence that users choose to stay engaged on the platform because micro-targeting attracts them. The more they provide data, the more advertisements they receive, and the longer they stay online resulting in increased user engagement on Facebook. Even though there are controls to tackle privacy issues, users do not adjust them because the ads will show less, and users will not be able to make use of the micro-targeted ads as much as they can. Moreover, it is also the case that users do not have knowledge that they exist. As a result, they contribute to the micro-targeting paradox without even knowing. These hearings make clear that micro-targeting becomes are paradox due to individual users' behavior, being their continuing engagement on Facebook.

4.5. Other documents

The 2014 US Federal Commission's report, which examined nine data companies in the country, showed that CA was not properly regulated, lacking transparency, and gathering individual data without their real interaction (Mueller, 2019). This stemmed both from the workings of cyberspace and the borderless nature of data. The report finds that six of those companies including CA access data from government entities as well as provide them with services such as marketing strategies (U.S. FTC, 2014). The Mueller (2019) report, therefore, suggests that CA is beyond a simple data broker and that it is a much bigger player in the data industry. Considering that the company harnessed the data of over 87 million American Facebook users without consent, CA brings Facebook under suspicion in many ways. One aspect of this is evident when looking at the US hearing where Senator Kamala Harris was questioning the COO of Facebook Sheryl Sandberg. Harris states:

> "Your company's business model is, it's obviously complex, but benefits from increased user engagement. And that results, of course, in increased revenue. So, simply put the more

people that use your platform, the more they are exposed to third party ads, the more revenue you generate. Would you agree with that?…" (C-Span, 2018d, 01:32:07).

Senator Harris frames the micro-targeting issue through a business lens, however, her words also confirm the micro-targeting paradox. When there are more users on the platform, they view more ads, and Facebook gains from this interaction. Facebook users also benefit from this situation as they choose to be on the platform. One study regarding the CA scandal also illustrates how micro-targeting is a paradox. After the scandal, there was not only a market value decrease of 134 billion dollars but also a huge drop in Facebook user confidence (Meredith, 2018). A survey study done by The Manifest in the US indicates that only 27% of users trusted Facebook, with a decline of 66% compared to the previous year (Herhold, 2019). Moreover, 44% of the users have negative attitudes towards Facebook and 37% of the users use Facebook less (Herhold, 2019). It is striking that even though almost half of the users view Facebook negatively, most of them are still using it. The fact that people who complain about Facebook and the scandal *on Facebook* is also equally striking (Herhold, 2019). Yet, loss of trust does not mean user disengagement from Facebook. It is important to distinguish that the survey study only deals with user trust, and not the actual usage. This irony shows users are almost dependent on Facebook, backing the claim of privacy paradox as well as the micro-targeting paradox. Despite the scandal, micro-targeting still benefited Facebook in the long run and kept its users committed to the platform. Equally, Facebook users continued holding their Facebook accounts due to its perks.

Van der Schyff et al.'s (2020) study touches upon the privacy paradox by arguing that individuals have a Facebook dependency and continue to use the app with a growing user base notwithstanding the scandal. This research examines the relationship between individuals' OCEAN profiles and their intensity of Facebook usage. The authors conduct their analysis with a sample of US citizens, which makes the research relevant for this paper (Van Der Schyff et al., 2020, p. 1). Their main finding is that only two of the personality traits (agreeableness and extraversion) were positively correlated with the intensity of Facebook usage (Van der Schyff et al., 2020, p. 9). This implies that the more agreeable and extrovert the individuals are, the more intensive they use Facebook. The authors reported that users saw Facebook as a tool that gives them psychological and social benefits, rather than an app that risks their data (Van Der Schyff et al., 2020). This finding is logical in the context of micro-targeting on social media platforms as the relationship between the two is mutually reinforcing each other for increased user engagement. Even though Van Der Schyff et al. (2020) argue that Facebook dependency is a behavioral problem, its useful features created through micro-targeting were the reason why people continued using Facebook. In other words,

micro-targeting was the main reason for the continuous user engagement on Facebook. Thereby, their findings directly support the micro-targeting paradox by suggesting that users, Facebook, and data firms such as CA overall benefit from micro-targeting.

Another survey conducted in the US by the Pew Research Center looks at user activity on Facebook and indicates that 54% of the users changed their privacy settings when the scandal broke out. While 42% of the individuals state that they took a break from the app for a while, only 26% deleted their accounts completely (Perrin, 2018). Given only a little more than half of the users' change in their privacy settings and the relatively small number of people deleting their accounts also supports privacy paradox. Even though individuals were concerned about their data, a majority of users did not stop using Facebook. The two surveys show that despite the biggest data breach scandal in recent history, US citizens remained engaged on Facebook. Chris Hoofnagle summarises this issue by saying that

> "In most situations, where a company does something that's unpopular, they have blowback, they lose the ability to do something. But in Facebook's case, we have something I call blow-forward, where they take two steps forward, there's some type of public reaction, and they just take a little step back. So, over time, they have been able to open up profiles more and more" (Yue et al., 2020, p. 14).

His comment is still relevant today as Facebook was able to survive a major privacy scandal and continued growing up to date.

To dig deeper into the privacy concerns of individuals, the qualitative research of Hinds et al. (2020) is important to mention. The authors conducted semi-structured interviews with several participants in the aftermath of the scandal. They touched upon individuals' understanding of privacy and analyzed their behavior towards Facebook. Their research produced surprising results as the majority of participants neither deleted their accounts nor changed their privacy settings (Hinds et al., 2020, p. 1). They were not concerned about privacy breaches and did not feel surprised after the CA scandal because they knew that these types of activities were already plausible. One respondent comments

> "With stuff like the recent Facebook scandal, it's like you don't realize how open your data is. I feel like a lot of companies probably do have my data now and I've just kind of got to the point where I've accepted, the basic data, I don't care about sharing that with third parties anymore because I know most of them probably have it by this point." (Hinds et al., 2020, p. 7).

As argued above, this hints at the concept of privacy fatigue where individuals think it is worthless to try protecting their data. Similarly, another participant mentions

> "I think Facebook's made it very difficult for you to remain very private. Like, maybe I don't know, maybe they've changed it now, but I remember like maybe two years ago when I was trying to... push down my privacy, I found it really difficult to be able to tick all the boxes that meant I was completely private because it just felt like I was just getting through some hoops... Friends of friends, they were still finding my profile... Because it almost seems like they don't want you to be private... Well, obviously they don't because I don't think that's come up, they want your profile to be as private but also as public as it possibly can, so I think they make it very difficult for you to just like really limit yourself to just your friends." (Hinds et al., 2020, p. 8).

The respondent makes clear that Facebook has a controversial strategy. While it provides various controls to its users, Zuckerberg's previous claim that users get the most satisfaction from Facebook through targeted advertisements indicates that there is a blurred line between privacy and user behavior. Users would like to have privacy, but in the meantime, they benefit from targeted advertisements. These advertisements come at the expense of having fewer controls for limiting data, making their accounts more vulnerable to data breaches. As a result, the micro-targeting paradox emerges out of ambiguous user behavior, leading to more engagement.

Networked privacy was also present in the respondents' answers. A respondent argued that whenever he searches for a product on eBay, he sees the same product appearing in Facebook advertisements (Hinds et al., 2020, p. 6). He stated that he was concerned because he could not find the connection between these two platforms. Likewise, another respondent asserted that she kept on receiving new friend suggestions even though she did not know any of them (Hinds et al., 2020, p. 6). As mentioned previously, networked privacy entails that once an individual engages with such platforms, be it Facebook or any other one, the product or information that is searched does not only stay in one domain. Instead, multiple stakeholders receive the same information. Their structure is collective in the sense that there is more than one information holder. The main purpose of networked privacy is to keep the users more networked since it makes data collection easier for micro-targeting. Networked privacy was also present in the scandal since the "thisisyourdigitallife" app had access to the personal data of those who did not even use the app. It was enough for one person to download and use it, and the company had data of the users' families and friends (Wired, n. d.). CA held the data of more than 87 million American Facebook users without their knowledge, leveraging multiple stakeholders to hold personal data. Users did not know that CA had their data

for micro-targeting purposes until the scandal was revealed. However, even after the scandal, there was no drastic decline in Facebook engagement as most of the individuals kept their accounts.

Similarly, Brown's (2020) work also implicated more or less the same characteristics regarding Facebook usage. She interviewed ten undergraduate students in terms of their decisions on Facebook (leaving or staying) after the scandal. None of the respondents permanently left Facebook (Brown, 2020, p. 1). Respondents frequently argued that Facebook provided useful services such as networking and complete disengagement from the platform would disclose their relationships with others (Brown, 2020, p. 2). Seven out of ten respondents replied that they were not surprised about the affair which supports privacy fatigue (Brown, 2020, p. 4). Further, there was only one respondent who temporarily deactivated his account for a long time, yet, decided to reactivate it again due to its helpful aspects such as college applications and networking (Brown, 2020, p. 4). Others who decided to stay showed similar connotations to Hinds et al.'s (2020) evidence such as that they have nothing to hide or that these activities do not bother them (Brown, 2020, p. 5). One respondent argues that he was not shocked at all when the scandal came to light as he knew that micro-targeting is how Facebook makes a profit (Brown, 2020, p. 5). This claim aligns with the fact that micro-targeting is a business model and its utilization on Facebook for various purposes is a known issue. Another respondent backs up this aspect by saying that

> "the only harm that can come to me that I was aware of [would be] from it posting and using, like, my data to target specific ads from Cambridge Analytica or whatever they were doing with the data to try to sway the election. I guess in that way it would be bad. But I never considered closing my account because of it" (Brown, 2020, p. 5).

Combining these responses, there is evidence for the micro-targeting paradox. Users do not perceive micro-targeting as a harmful tool to the extent that it leads them to delete their accounts. They instead make use of what micro-targeting offers them on Facebook. In turn, both Facebook and its users gain from such interaction because it favors both parties. The evidence shows that users are still engaged on Facebook despite privacy concerns and a major micro-targeting scandal. There has not been a considerable decline in Facebook usage and it is alarming that users are a part of how micro-targeting is a paradox. The analyzed hearings highlight many issues inherent in the realm of social media. It is a necessity that users inform themselves about how social media platforms work. In that way, users become more aware of what they sign up for. This can halt misinformation and change people's perception of social media. If they are better informed about how social media platforms work, they can make clear judgements on whether or not they want to join the platforms. For this to take place, both the social media companies and users have the

responsibility of protecting personal data. In the case they disagree with the terms of service, they have the freedom to not join. Signing up for services without even reading the terms only leads to more confusion regarding how these platforms work. Micro-targeting feeds from user data, and when it is successful, users become more susceptible to stay on the platforms.

Chapter 5- Conclusions and Implications

This thesis tried to answer why users kept their engagement on Facebook in the aftermath of the CA scandal. Throughout the research, the aim was to provide an explanation for the mutually beneficial relationship between micro-targeting and increased user engagement. The thesis analyzed this relationship by providing the micro-targeting paradox as a potential explanation. User engagement did not decline on Facebook because of the micro-targeting paradox. Examining the CA case on the relationship between micro-targeting and user engagement has been the focus of this paper because the case illustrated that despite such a major scandal, there was not a backlash from Facebook users in terms of usage. The previous literature lacked regarding the logic behind the ongoing user engagement on Facebook even after the scandal. This paper, therefore, aimed to fulfill the 'why' question. The micro-targeting paradox as a concept has not been explicit in the literature, but rather, mentioned implicitly under the privacy scholarship through a couple of privacy concepts. Each privacy concept mentioned in this research highlighted a different aspect of the micro-targeting paradox. In this case, bringing these concepts together entails what the micro-targeting paradox is. As a strength, the paper identified explicitly what the micro-targeting paradox is in detail. Although there has been a lot of research done concerning the CA scandal, this research addressed the research gap on the reason why users kept their Facebook accounts after the scandal. In terms of the weaknesses of this paper, there are three important points to make. First, the research aimed to explain the change in user behavior through observing the customer base, and not through conducting in-person interviews. This was a major challenge for the paper in terms of validity and reliability. A large amount of data on the scandal and the court hearings were appealing for content analysis. Additionally, identifying millions of American Facebook users who were affected by the scandal would require resources and be time-consuming for the thesis. Second, measuring the change in user behavior on the individual level would be equally problematic due to location and time constraints. Further research could advance on this matter to reach more accurate results on the individual level. Lastly, the thesis used secondary sources regarding individual responses (interviews) towards the scandal. Even though these sources were helpful for identifying the micro-targeting paradox, they are not directly a product of this thesis. Therefore, there is a risk in terms of reliability and whether or not the secondary sources reflect the truth of the interviews. A possible

solution to this issue would be to conduct interviews and a content analysis together. Moreover, the scope of this research could be enlarged to other regions in the world, for instance, Europe. This would allow scholars to compare and contrast how the usage in the US and Europe would differ and what the implications of this comparison would be. Moreover, the comparison could be relevant for US policy-makers to formulate well-rounded privacy protection laws in the future.

Appendixes

Note: All the quotations mentioned below are taken from the official transcripts The Washington Post published on the Zuckerberg hearings.

Appendix 1- The Zuckerberg Senate Hearing

US Senators	**Quotations from the transcript**	**Zuckerberg's response (if applicable)**
Senator Thune	"…Facebook is pretty extraordinary. More than 2 billion people use Facebook every month. 1.4 billion people use it every day; more than the population of any country on Earth except China, and more than four times the population of the United States." (para. 12) "And the fact that those 87 million people may have technically consented to making their data available doesn't make those people feel any better… Right now I am not convinced that Facebook's users have the information that they need to make meaningful choices… How will you protect users data?" (para. 19)	—

Senator Grassley	“Today, Facebook has access of data points, ranging from ads that you've clicked on, events you've attended and your location, based upon your mobile device.” (para. 51) “Facebook generates — generated $40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.” (para. 52) “The potential for further growth and innovation based on collection of data is unlimitedless.” (para. 54)	–

		Zuckerberg starts with his testimony after Senator Grassley's opening statements: "When we first contacted Cambridge Analytica, they told us that they had deleted the data. About a month ago, we heard new reports that suggested that wasn't true. And, now, we're working with governments in the U.S., the U.K. and around the world to do a full audit of what they've done and to make sure they get rid of any data they may still have." (para. 94). "Third, to prevent this from ever happening again, going forward, we're making sure that developers can't access as much information now." (para. 96).

Senator Grassley	“My question: Why doesn't Facebook disclose to its users all the ways that data might be used by Facebook and other third parties? And what is Facebook's responsibility to inform users about that information?” (para. 123).	“Mr. Chairman, I believe it's important to tell people exactly how the information that they share on Facebook is going to be used. That's why, every single time you go to share something on Facebook, whether it's a photo in Facebook, or a message — in Messenger or What's App, every single time, there's a control right there about who you're going to be sharing it with…” (para. 124) “To your broader point about the privacy policy, this gets into an — an issue that I — I think we and others in the tech industry have found challenging, which is that long privacy policies are very confusing. And if you make it long and spell out all the detail, then you're probably going to reduce the percent of people who read it and make it accessible to them. (para. 125).

Senator Nelson	"Yesterday when we talked, I gave the relatively harmless example that I'm communicating with my friends on Facebook and indicate that I love a certain kind of chocolate. And all of a sudden I start receiving advertisements for chocolate. What if I don't want to receive those commercial advertisements?…Are you actually considering having Facebook users pay for you not to use the information?" (para. 129)	"Senator, people have a control over how their information is used in ads in the product today. So if you want to have an experience where your ads aren't — aren't targeted using all the information that we have available, you can turn off third-party information. What we found is that even though some people don't like ads, people really don't like ads that aren't relevant. And while there is some discomfort for sure with using information in making ads more relevant, the overwhelming feedback that we get from our community is that people would rather have us show relevant content there than not. So we offer this control that — that you're referencing. Some people use it. It's not the majority of people on Facebook. And — and I think that that's — that's a good level of control to offer." (para. 132- 134).

Senator Hatch	"…If you want something without having to pay money for it, you're going to have to pay for it in some other way, it seems to me. And that's where — what we're seeing here… And these great websites that don't charge for access — they extract value in some other way. And there's nothing wrong with that, as long as they're upfront about what they're doing." (para. 218- 219). "…how do you sustain a business model in which users don't pay for your service?" (para. 226).	"Senator, we run ads." (para. 227) "Every piece of content that you share on Facebook, you own and you have complete control over who sees it and — and how you share it, and you can remove it at any time." (p. 232).
Senator Wicker	"Is it true that — as was recently publicized, that Facebook collects the call and text histories of its users that use Android phones?" (para. 294).	"Senator, we have an app called Messenger for sending messages to your Facebook friends. And that app offers people an option to sync their — their text messages into the messenging app, and to make it so that — so basically so you can have one app where it has both your texts and — and your Facebook messages in one place." (para. 295). "…you have to affirmatively say that you want to sync that information before we get

Senator Graham	“It says, “The terms govern your use of Facebook and the products, features, apps, services, technologies, software we offer — Facebook's products or products — except where we expressly state that separate terms, and not these, apply.” I'm a lawyer. I have no idea what that means. But, when you look at terms of service, this is what you get. Do you think the average consumer understands what they're signing up for?” (para. 419-420).	“I don't think that the average person likely reads that whole document.” (para. 421). “because we have the controls in line every time…” (para. 426).
Senator Cornyn	“How about third parties that you have contracted with to use some of that underlying information, perhaps to target advertising for themselves? You can't — do you — do you call back that information, as well? Or does that remain in their custody?” (para. 540). “Well, you clearly rent it (data).” (para. 542).	“…And we do not sell data to advertisers. We don't sell data to anyone.” (para. 541). “What we allow is for advertisers to tell us who they want to reach, and then we do the placement.” (para. 543).

Senator Whitehouse	“And all I wanted to establish with you is that that document that Senator Graham held up, that is not a negotiable thing with individual customers; that is a take it or leave it proposition for your customers to sign up to, or not use the service.” (para. 666).	“Cambridge Analytica actually has a parent company and we banned the parent company. And recently we also banned a firm called AIQ, which I think is also associated with them. And if we find other firms that are associated with them, we will block them from the platform as well.” (para. 661). “Senator, my understanding is we're blocking them from doing business on the platform, but I do not believe that we're blocking people's personal accounts.” (para. 663).

Senator Lee	“From what you've said today, and from previous statements made by you and other officials at your company, data is at the center of your business model. It's how you make money. Your ability to run your business effectively, given that you don't charge your users, is based on monetizing data. And so the real issue, it seems to me, really comes down to what you tell the public, what you tell users of Facebook, about what you're going to do with the data. About how you're going to use it.” (para. 693-694).	“The vast majority — and then the first category, is content that people chose to share on the service themselves. So that's all the photos that you share, the posts that you make, what you think of as the Facebook service, right? That's — everyone has control every single time that they go to share that. They can delete that data any time they want; full control, the majority of the data. The second category is around specific data that we collect in order to make the advertising experiences better, and more relevant, and work for businesses. And those often revolve around measuring, okay, if you — if we showed you an ad, then you click through and you go somewhere else, we can measure that you actually — that the — that the ad worked. That helps make the experience more relevant and better for — for people, who are getting more relevant ads, and better for the businesses because they perform better. You also have control completely of that second type of data. You can turn off the ability for Facebook to collect that — your ads will get worse, so a lot of people don't want to do that. But you have complete control over what you do there as well.” (para. 699- 701).

Senator Fischer	“So is this — is then a question of Facebook is about feeling safe, or are users actually safe? Is Facebook — is Facebook being safe?” (para. 830).	“Senator, I think Facebook is safe. I use it, my family uses it, and all the people I love and care about use it all the time. These controls are not just to make people feel safe; it's actually what people want in the product. The reality is, is that when you — just think about how you use this yourself. You don't want to share it — if you take a photo, you're not always going to send that to the same people. Sometimes you're going to want to text it to one person. Sometimes you might send it group. I bet you have a page. You'll probably want to put some stuff out there publicly so you can communicate with your constituents.” (para. 831- 832).

Senator Moran	"…how does the case of approximately 87 million Facebook friends having their data shared with a third party due to the consent of only 300,000 consenting users not violate that agreement?" (para. 1054).	"…the way that the platform worked, that you could sign into an app and bring some of your information and some of your friends' information is how we explained it would work. People had settings to that effect. We explained and — and they consented to — to it working that way. And the — the system basically worked as it was designed." (para. 1055). "…you might want to have a calendar that can have your friends' birthdays on it, or you might want your address book to have your friends' pictures in it, or you might want a map that can show your friends' addresses on it. In order to do that, we needed to build a tool that allowed people to sign in to an app and bring some of their information, and some of their friends' information, to those apps. We made it very clear that this is how it worked, and — and when people signed up for Facebook, they signed up for that as well. (para. 1060).

Senator Heller	“Do you believe you're more responsible with millions of American's personal data than the Federal government would be?” (para. 1120).	“Yes. But, senator, the — your point about surveillance, I think that there's a very important distinction to draw here, which is that when — when organizations do surveillance people don't have control over that. But on Facebook, everything that you share there you have control over. You can — you can say I don't want this information to be there. You have full access to understand all, every piece of information that Facebook might know about you, and you can get rid of all of it. And I — I don't know of any other — any surveillance organization in the world that operates that way, which is why I think that that comparison isn't really apt here.” (para. 1121).
Senator Tillis	“But go to the privacy tab. If you don't want to share something, don't share it. This is a free service. Go on there and say I don't want to allow third party search engines to get in my Facebook page. Go on there and say only my friends can look at it. Go on there and understand what you're signing up for. It's a free app.” (para. 1174).	—

Senator Johnson	"With all this publicity, have you documented any kind of backlash from Facebook users? I mean, has there been a dramatic falloff in the number of people who utilize Facebook because of these concerns?" (para. 1296).	"Senator, there has not." (para. 1297).
	"So it's kind of safe to say that Facebook users don't seem to be overly concerned about all these revelations, although obviously Congress apparently is." (para. 1300).	"Well, senator, I think people are concerned about it. And I think these are incredibly important issues that people want us to address. And I think people have told us that very clearly." (para. 1301).
	"But it seems like Facebook users still want to use the platform because they enjoy sharing photos and they share the connectivity with family members, that type of thing. And that overrides their concerns about privacy." (para. 1302).	"…But overall, the — I think that the ads experience is going to be the best one. I think in general, people like not having to pay for a service." (para. 1307).

Senator Capito	“Okay. So if somebody leaves Facebook and then rejoins and asks Facebook, can you recreate my past, your answer would be?” (para. 1347).	“We offer deactivation, which allows you to shut down or suspend your account…” (para. 1348). “So they deactivate their account temporarily, but then want the ability to turn it back on when they're ready. You can also delete your account, which is wiping everything. If you do that, then you can't get it back.” (para. 1348).

Appendix 2- The Zuckerberg House Hearing

US Congressmen and congresswomen	Quotations from the transcript	Zuckerberg's response (if applicable)
Congressman Pallone	"Yes or no: Is Facebook changing any user default settings to be more privacy-protective?" (para. 110). "How can consumers have control over their data when Facebook doesn't have control over the data itself? That's my concern." (para. 123).	"Congressman, yes. In — in response to these issues, we've changed a lot of the way that our platform works, so, that way, developers can't get access to as much information." (para. 111). "Congressman, what we allowed — what we allow with our developer platform is for people to choose to sign into other apps and bring their data with them. That's something a lot of people want to be able to do… In order to do that, you need to be able to sign into an app, bring some of your data and some of your friends' data. And that's what we built." (para. 124-126).
Congressman Barton	"You can pretty well set up your Facebook account to — to be almost totally private. But you have to really work at it." (para. 156).	–

Congressman Shimkus	“And how does tracking work across different devices?” (para. 270).	“…what information do we track, and why, about people who are not signed into Facebook. We track certain information for security reasons and for ads reasons.” (para. 272). “The second thing that we do is we provide an ad network that third-party websites and apps can run in order to help them make money. And those ads — you know, similar to what Google does and what the rest of the industry does — it's not limited to people who are just on Facebook. So, for the purposes of that, we may also collect information to make it so that those ads are more relevant and work better on those websites. There's a control that — for that second class of information around ad targeting — anyone can turn off, has complete control over it.” (para. 275-276).
Congressman Burgess	“Look, I'm as bad as anyone else. I see an app, I want it, I download it, I breeze through the stuff. Just take me to the — to the good stuff in the app. But, if a consumer wanted to know, could they know?” (para. 325).	“Congressman, I think you're raising an important point, which is that I think, if someone wanted to know, they could. But I think that a lot of people probably just accept terms of service without taking the time to read through it.” (para. 326).

Congresswoman Degette	“Now, since the revelations surrounding Cambridge Analytica, Facebook has not noticed a significant increase in users deactivating their accounts. Is that correct?” (para. 412). “Now, since the revelations surrounding Cambridge Analytica, Facebook has also not noticed a decrease in user interaction on Facebook. Correct?” (para. 414).	“Yes.” (para. 413). “Yes, that's correct.” (para. 415).
Congressman Guthrie	“My — my friend and I was planning a family trip to Florida, and I searched a town in Florida, and all of a sudden, I started getting ads for a brand of hotel that I typically stay in, and a great hotel at the price available to the public, because it was on the Internet, that I was willing to pay and stay there. So I thought it was actually convenient. Instead of getting just an ad to someplace I'll never go, I got an ad specifically to a place I was — I was looking to go, so I thought that was convenient. And it wasn't Facebook, although my wife used Facebook to message my mother-in-law this weekend for where we're meeting up, so it's very valuable. We get to do that for free, because your business model relies on consumer-driven data.” (para. 776).	“And that's why the ads business model is in service of the social mission that we have, and you know, I think sometimes that gets lost, but I think that's a really important point.” (para. 778) “…we already give people a control to not use that data and ads, if they want. Most people don't do that. I think part of the reason for that is that people get that if they are going to see ads, that they want them to be relevant. But the other thing is that our — a lot of what our business — what makes the ads work, or what makes the business good is just that people are very engaged with Facebook. We have more than a billion people who spend almost an hour a day across all our services.” (para. 784-785).

References

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2020). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society, 37*(2), 115-127.

Baldwin-Philippi, J. (2017). The Myths of Data-Driven Campaigning. *Political Communication, 34*(4), 627-633.

Barbu, O. (2014). Advertising, microtargeting and social media. *Procedia-Social and Behavioral Sciences*, *163*, 44-49.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bathini, D. R. (2021). Microtargeting control: Explicating algorithmic control and nudges in platform−mediated cab driving in India. *New Technology, Work, and Employment, 36*(1), 74-93.

Bennett, C. (2013). The politics of privacy and the privacy of pol- itics: parties, elections and voter surveillance in Western democracies. First Monday 18(8). DOI: 10.5210/fm.v18i8. 4789

Bennett, C. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society*, *13(3/4)*, 370-389.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters, 117*(1), 25-27.

Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer, 51*(5), 84-89.

Bodó, B, Helberger, N, & De Vreese, C.H. (2017). Political micro-targeting: A Manchurian candidate or just a dark horse? *Internet Policy Review, 6*(4), 1-14.

Borgesius F. J. F., Möller, J., Kruikemeier, S., Faathnaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review, 14*(1): 82-96.

Boyd, D. (2012). Networked Privacy. *Surveillance & Society, 10*(3/4), 348-350.

Boyd, D. (2014, July 2). *What does the Facebook experiment teach us? Growing anxiety about data manipulation.* Medium. https://medium.com/message/what-does-the-facebook-experiment-teach-us-c858c08e287f.

Brown, A. J. (2020). "Should I Stay or Should I Leave?": Exploring (Dis)continued Facebook Use After the Cambridge Analytica Scandal. *Social Media Society, 6*(1), 205630512091388.

Cadwalladr, C. & Graham-Harrison, E. (2018, March 17). Cambridge Analytica: links to Moscow oil firm and St Petersburg university. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university**.**

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42-51.

Cian, F., Marconcini, M., & Ceccato, P. (2018). Normalized Difference Flood Index for rapid flood mapping: Taking advantage of EO big data. *Remote Sensing of Environment, 209*, 712-730.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498-512.

CNN (2018, March 21). Mark Zuckerberg in his own words: The CNN interview. *CNN.* https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html.

C-Span (2018, May 16). *Cambridge Analytica and Data Privacy*. [Video]. C-Span. https://www.c-span.org/video/?445621-1/cambridge-analytica-whistleblower-christopher-wylie-testifies-data-privacy.

C-Span (2018a, June 19). *Cambridge Analytica and Facebook Data Partners.* [Video]. C-Span. https://www.c-span.org/video/?447132-1/senate-committee-examines-cambridge-analytica-partnership-facebook.

C-Span (2018b, April 10). *Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection.* [Video]. C-Span. https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection.

C-Span (2018c, April 11). *Facebook CEO Mark Zuckerberg Hearing on Data Protection.* [Video]. C-Span. https://www.c-span.org/video/?443490-1/facebook-ceo-mark-zuckerberg-testifies-data-protection.

C-Span (2018d, September 5). *Foreign Influence and Social Media.* [Video]. C-Span. https://www.c-span.org/video/?450990-1/foreign-influence-social-media.

Cukier, K. & Mayer-Schoenberger, V. (2013). The Rise of Big Data: How It's Changing the Way We Think About the World. *Foreign Affairs 92*(3): 28-40.

Delacourt, S. (2016). *Shopping for Votes: How Politicians Choose Us and We Choose Them.* Madeira Park: D & M Publishers.

Digital Marketing Institute. (2019, May 3). *How do algorithms work?* https://digitalmarketinginstitute.com/blog/how-do-social-media-algorithms-work.

Dobber, T. (2020). Data & Democracy: Political microtargeting: A threat to electoral integrity?. *University of Amsterdam.*

Duggan M. & Smith, A. (2016, October, 25). The Political Environment on Social Media. *Pew Research Center (Internet & Technology)* https://www.pewresearch.org/internet/2016/10/25/the-political-environment-on-social-media/.

Edsall, T.B. (2012, April 15). Let the nanotargeting begin. *The New York Times*, https://campaignstops.blogs.nytimes.com/2012/04/15/let-the-nanotargeting-begin/ (accessed 18 April 2021).

Fong, P. W., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for Facebook-style social network systems. *Computer Security–ESORICS 2009*, 303-320. Springer Berlin Heidelberg.

Fuchs, C. (2011). How to define surveillance? *MATRIZes*, 5(1), 109–133.

Fuchs, C. & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications, 40*(1), 113-135.

González-Bailón, S. & Gorham, A. (2018, April 4). Want to change Facebook? Don't delete your account—use it for good. *Quartz.* https://qz.com/1244750/the-delete-facebook-movement-is-ultimately-self-defeating/#:~:text=The%20%23DeleteFacebook%20campaign%20gives%20voice,the%20%23DeleteFacebook%20movement%20is%20obvious.

Gorton, W. A. (2016). Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy. *New Political Science, 38*(1), 61-80.

Hegel, G. W. F. (1812). *Science of logic.* London: Routledge.

Herhold, K. (2019, March 27). How People View Facebook After the Cambridge Analytica Data Breach. *The Manifest.* https://themanifest.com/social-media/how-people-view-facebook-after-cambridge-analytica-data-breach.

Heyman, R. & Pierson, J. (2015). Social Media, Delinguistification and Colonization of

Lifeworld: Changing Faces of Facebook. *Social Media + Society*, 1(2), 1-11.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-computer Studies, 143*, 1-14.

Horwitz, J. (2018, April 5). Outside the US, the Philippines saw the most Facebook user data go to Cambridge Analytica. *Quartz*. https://qz.com/1245355/outside-us-philippines-saw-most-facebook-user-data-go-to-cambridge-analytica/.

Howard P. N. (2006). New Media Campaigns and the Managed Citizen. New York: Cambridge University Press.

Hu, M. (2020). Cambridge Analytica's black box. *Big Data & Society, 7*(2), 1-6.

Internet Governance Lab (2020, June 17). *Beyond Cambridge Analytica: Microtargeting and Online Campaigns in 2020.* https://internetgovernancelab.org/events/2020/9/2/beyond-cambridge-analytica-microtargeting-and-online-campaigns-in-2020.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), 56-59.

Jamieson, K. H. (2013). Messages, Micro-targeting, and New Media Technologies. *The Forum : A Journal of Applied Research in Contemporary Politics, 11*(3), 429-435.

Jia, H. & Xu, H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology, 10*(1), 1-19. https://doi.org/10.5817/CP2016-1-4.

Keith, M. J., Maynes, C., Lowry, P. B., & Babb, J. (2014). Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. *International Conference on Information Systems.* 1-18. https://doi.org/10.13140/2.1.3164.6403.

Kerpen, D. (2011). Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Generally Amazing on Facebook. *McGraw-Hill. Kindle Edition.*

Khursheed, B., Pitropakis, N., McKeown, S., & Lambrinoudakis, C. (2020). Microtargeting or Microphishing? Phishing Unveiled. In *International Conference on Trust and Privacy in Digital Business* (pp. 89-105). Springer, Cham.

Kim Y. M., Hsu J., Neiman D., Kou, C., Bankston, L., Kim, S. Y., Heinrich, R., Baragwanath, R. & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. *Political Communication, 35*(4), 515–541.

Korolova, A. (2010). Privacy Violations Using Microtargeted Ads: A Case Study. *2010 IEEE International Conference on Data Mining Workshops,* 474-482, doi: 10.1109/ICDMW.2010.137.

Krotzek, L. J. (2019). Inside the Voter's Mind: The Effect of Psychometric Microtargeting on Feelings Toward and Propensity to Vote for a Candidate. *International Journal of Communication 13(2019),* 3609-3629.

Lavigne, M. (2020). Strengthening ties: The influence of micro-targeting on partisan attitudes and the vote. *Party Politics, 20*(10) , 1-12. DOI: 10.1177/1354068820918387.

Lee, A. R., Son, S., & Kim, K. K. (2016). Information and communication technology overload and social networking service fatigue: A stress perspective. *Computers in Human Behavior, 55*, 51-61.

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *The American Political Science Review, 65*(3), 682-693.

Lyon, D. (2007). *Surveillance studies : An overview*. Cambridge, UK ; Malden, MA: Polity.

MacNish, K. (2020). Mass Surveillance: A Private Affair? *Moral Philosophy and Politics, 7*(1), 9-27.

Manokha, I. (2018). Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective. *Theory & Event, 21*(4), 891-913.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051-1067.

Math Vault, The Definitive Glossary of Higher Mathematical Jargon. (2019, August 1) *Algorithm.* https://mathvault.ca/math-glossary/#algo.

Medium. (2017, March 19). SCL Group joins the US State Dept. https://medium.com/textifire/scl-group-joins-the-us-state-dept-ad5cac8155ff.

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. *CNBC*. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

Metcalf, A. L., Angle, J. W., Phelan, C. N., Muth, B. A., & Finley, J. C. (2019). More "Bank" for the Buck: Microtargeting and Normative Appeals to Increase Social Marketing Efficiency. *Social Marketing Quarterly, 25*(1), 26-39.

Miller, A. R. (1971). *The Assault on Privacy.* Ann Arbor, Michigan: The University of Michigan Press.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. US Department of Justice.

Munroe K.B. & Munroe H.D. (2018). Constituency campaigning in the age of data. *Canadian Journal of Political Science/Revue Canadienne de Science Politique, 51*(1): 135–154.

Neate, R. (2018, July 26). Over $119bn wiped off Facebook's market cap after growth shock. *The Guardian.* https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119-158.

Nissenbaum, H. (2009). *Privacy in Context*. Redwood City: Stanford University Press.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. London: Viking.

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social networking sites.". In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–90). New York: Springer.

Pasquale, F. (2015). *The Black Box Society*. Cambridge: Harvard University Press.

Perrin, A. (2018). Americans are changing their relationship with Facebook. *Pew Research Center.* https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

Peruzzi, A., Zollo, F., Quattrociocchi, W. & Scala, A. (2018). How News May Affect Markets' Complex Structure: The Case of Cambridge Analytica. *Entropy, 20*(10), 1-12.

Petronio, S. (2002). *Boundaries of privacy dialectics of disclosure* (SUNY series in communication studies). Albany: State University of New York Press.

Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review, 2*(3), 175-196.

Pew Research Center (2014). Digital life in 2015. (Research Report). [WWW document] http://www.pewinternet.org/2014/03/11/digital-life-in-2025/.

Pierson, J., & Van Zeeland, I. (2019). Privacy from a Media Studies Perspective. In *The Handbook of Privacy Studies* (pp. 355-382). Amsterdam: Amsterdam University Press.

Prummer, A. (2020). Micro-targeting and polarization. *Journal of Public Economics, 188*, 104210. 1-21.

Regan, P. (1995). *Legislating Privacy Technology, Social Values, and Public Policy.* Chapel Hill: The University of North Carolina Press.

Rosebrough M. (2010, April 27). Is data really "the new oil"? *Kenway Consulting.* https://www.kenwayconsulting.com/blog/data-is-the-new-oil/#:~:text=The%20concept%20behind%20%E2%80%9Cdata%20is,so%20in%20a%20timely%20manner.

Rosenberg, M. (1969). *Death of Privacy.* Random House.

Snider, M. & Baig, E. C. (2019, July 24). Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures, *USA Today.* https://eu.usatoday.com/story/tech/news/2019/07/24/facebook-pay-record-5-billion-fine-u-s-privacy-violations/1812499001/.

Srnicek, N. (2017). *Platform capitalism.* Cambridge: Polity Press.

Svitek, P. & Samsel, H. (2018, March 20). *Ted Cruz says Cambridge Analytica told his presidential campaign its data use was legal.* The Texas Tribune. https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/.

Tankovska, H. (2021, February 9). Global social networks ranked by number of users 2021. *Statista.* https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

Toffler, A. (1980). *The third wave*. New York: Morrow.

Transcript of Mark Zuckerberg's Senate hearing. (2018, April 11). The Washington Post. Retrieved April 20, 2021 from https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

Transcript of Zuckerberg's appearance before House committee (2018, April 12). The Washington Post. Retrieved April 20, 2021 from https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

U.S. Government. U.S. Federal Trade Commission (U.S. FTC). (2014). *Data Brokers: A Call for Transparency and Accountability.* U.S. Federal Trade Commission.

Van Der Schyff, K., Flowerday, S., Kruger, H., & Patel, N. (2020). Intensity of Facebook Use: A Personality-based Perspective on Dependency Formation. *Behaviour & Information Technology*, 1-17. https://doi.org/10.1080/0144929X.2020.1800095.

Van Dijck, J. (2013). *The Culture of Connectivity: a Critical History of Social Media.* Oxford: Oxford University Press.

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.

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society, 58*(1), 20-41.

Wired (n. d.). *The Cambridge Analytica Story, Explained*. https://www.wired.com/amp-stories/cambridge-analytica-explainer/.

Yue, T, Beraite, R., & Chaudhri, V. (2020). *Reputation Crisis? Facebook Meets Cambridge Analytica. RSM Case Development Centre.* http://hdl.handle.net/1765/131568.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.