

“I don’t like it but that’s how it works”:

Exploring Greek millennials’ perceptions of personalized advertising on Facebook and Instagram.

Student Name: Kelly (Kalliopi) Tsatsarou
Student Number: 572752

Supervisor: Anouk Mols

Master Media Studies - Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master's Thesis
June 2021

“I don’t like it but that’s how it works”:

Exploring Greek millennials’ perceptions of personalized advertising on Facebook and Instagram.

ABSTRACT

In the current digitalized era of social media, numerous companies choose to track and collect people’s data to display personalized advertising on social platforms based on consumers’ lifestyles and preferences. The usefulness of that practice lies in delivering consumers content that is relevant to their interests. Every day, a vast amount of consumers’ personal information (i.e. location, gender, and age) and browsing activity (i.e. websites visited, likes, and shares) are tracked to help companies promote their products and services successfully. Thus, personalized advertising and data tracking constitute forms of consumer surveillance. Of course, this practice directly affects consumers whose personal data is used by companies. Therefore, the aim of this research was to investigate Greek millennials’ perceptions of personalized advertising that they find on their Facebook and Instagram feeds. To obtain in-depth information of consumers’ knowledge, experiences, as well as feelings around personalized advertising and gain an explicit understanding of them, a qualitative method was used. In particular, 14 in-depth interviews were conducted with Greek millennials consumers. The transcripts were analyzed using the constructivist grounded theory approach and five overarching themes emerged from the findings.

All these themes highlighted that consumers experience personalized advertising on social media in three different ways. Pleasant reactions occur when advertisements are close to consumers’ interests and preferences because marketers offer them useful and helpful content. Also, consumers respond positively to personalized advertisements because of their awareness that media creators/developments get paid by advertising. Contrarily, consumer annoyance occurs due to repetitive and misaligned personalized advertising. Besides, fearful reactions are expected because of online risks like hacking, and misuse of personal data. Consumers experience targeted advertising apathetically because they are knowledgeable of the data tracking mechanisms that companies use. As a result, they have compromised with the way the advertising system operates. Interestingly, privacy concerns were only raised due to highly personalized advertisements (i.e. based on private conversations) and it was perceived as invasive in people’s personal lives. Consequently, people have adopted a protective online behavior towards their personal data. They were also motivated to manage their privacy in two ways; by deciding under which circumstances they will self-disclose and by adopting privacy-preserving practices such as deleting cookies, and private navigation.

KEYWORDS: *surveillance, data tracking, personalized advertising, social media, personal data, privacy, privacy-preserving practices*

Table of Contents

| | |
|---|----|
| Abstract and keywords | |
| 1. Introduction | 1 |
| 1.1. Scientific and societal relevance | 1 |
| 1.2. Research question and sub questions | 3 |
| 1.3. Chapter outline | 3 |
| 2. Theoretical framework | 4 |
| 2.1. Data tracking and personalized advertising as forms of consumer surveillance | 4 |
| 2.1.1. Free content justifies the collection of personal data | 5 |
| 2.1.2. Personalized advertising and profiling in digitalized era | 5 |
| 2.2. Privacy: conceptualization, self-disclosure negotiations, and regulation | 6 |
| 2.2.1. Privacy calculus around self-disclosure | 7 |
| 2.2.2. Communication Privacy Management | 8 |
| 2.2.3. General Data Protection Regulation | 9 |
| 2.3. Receptions and experiences of personalized advertising | 9 |
| 2.3.1. Personalized advertising as pleasing for the consumer | 9 |
| 2.3.2. Personalized advertising as irritating for the consumer | 10 |
| 2.3.3. Personalized advertising evokes fearful feelings in consumers | 11 |
| 2.4. Privacy attitudes around personalized advertising | 11 |
| 2.4.1. Privacy apathy | 11 |
| 2.4.2. Privacy concerns | 12 |
| 2.5. Privacy-preserving practices | 13 |
| 2.5.1. Using ad blocking software | 13 |
| 2.5.2. Deleting cookies | 14 |
| 2.5.3. Using private browsing | 15 |
| 2.5.4. Privacy-preserving practices on Facebook | 16 |
| 3. Methodology | 18 |
| 3.1. Sample | 18 |
| 3.1.1. Sampling criteria and data collection | 18 |
| 3.2. Interview procedure | 19 |
| 3.2.1. Online interviews | 20 |
| 3.2.2. Operationalization | 21 |
| 3.2.3. Research ethics: consent forms and pseudonymization | 23 |
| 3.3. Data analysis | 24 |
| 3.4. Credibility: reliability and validity | 26 |
| 4. Results | 28 |
| 4.1. Acknowledging the benefits of personalized advertising | 28 |
| 4.1.1. Useful features of personalized advertisements for consumers | 29 |
| 4.1.2. Useful features of personalized advertisements for businesses | 30 |
| 4.2. Drawbacks of personalized advertising as perceived by consumers | 31 |
| 4.2.1. Personalized advertising is annoying for the consumer | 31 |

| | |
|---|----|
| 4.2.2. Consumers' fearful reactions to personalized advertising | 33 |
| 4.3. Consumers' knowledge of data-tracking practices | 34 |
| 4.3.1. Understanding of consumer surveillance | 34 |
| 4.3.2. Consumers' assumptions of ads' origins..... | 36 |
| 4.4. Consumers' privacy attitudes | 37 |
| 4.4.1. Apathetic responses of personalized advertising | 37 |
| 4.4.2. Privacy Concerns..... | 39 |
| 4.5. Consumers' privacy negotiations | 41 |
| 4.5.1. Privacy-preserving practices | 41 |
| 4.5.2. Self-disclosure strategies on social media..... | 43 |
| 5. Conclusion..... | 46 |
| 5.1. Summary of the findings | 46 |
| 5.2. Societal and scientific relevance | 48 |
| 5.3. Limitations and future research..... | 49 |
| References | 51 |
| Appendix A - Interview guide..... | 60 |
| Appendix B - Coding scheme | 62 |
| Appendix C - Operationalization | 68 |
| Appendix D - Consent form..... | 70 |
| Appendix E - Overview of participants..... | 72 |

1. Introduction

Nowadays, an increasing number of businesses decide to monitor people's online behavior as well as activities and use that information to target them with personalized advertisements. When users sign up for free services such as social media they must provide in return some personal information (Tabora, 2019). For marketers to display targeted content, it is essential to track, collect and analyze this detailed information about the users' online behavior, and interests. Consequently, the consumers become the product because marketers can monitor people through their online activities such as their browsing behavior and click rates on websites, and collect their data by means of sophisticated tracking technologies. Hence, by using data-tracking practices, which can be seen as a form of consumer surveillance, brands use personalized advertisements to successfully promote their products on users' social media feeds (Tabora, 2019). That is why personalization is used as a customer-oriented marketing strategy of "delivering the right content to the right person at the right time to maximize immediate and future business opportunities" (Tam & Ho, 2006, p. 867).

1.1. Scientific and societal relevance

Research into how consumers feel about data tracking and personalized advertising is relevant in both academic and social fields. The societal value of this research lies in investigating important concerns and issues associated with privacy around data tracking practices. Carr and Hayes (2015) define social media as Internet-based platforms that are used for mass-personal communication and interaction. Consequently, these platforms derive most of their value from user-generated content. Social media like Facebook, Instagram, Twitter, and YouTube are considered very important for young people's socialization, education, and employment (Hargittai & Marwick, 2016). In fact, more than 3 billion people use social media today, and 40% of them use social media for communication purposes. Additionally, the number of social media users is expected to reach 4.41 billion in 2025, which highlights that social media networks are incredibly popular, and are projected to become more popular than ever (Chen, 2021). Due to the fact that online platforms and the use of mobile phone applications have both grown in popularity during the digital era, these developments have expanded the flow and accessibility of personal information and privacy issues have become more complicated (Solove, 2004). As a result, this research deals with a highly relevant topic in this rapidly changing field of digital media.

After the General Data Protection Regulation (GDPR) came into force in the European Union on the 25th of May 2018, numerous changes occurred. More specifically, businesses were forced to change their business models in order to protect citizens' privacy and provide them more transparency and control over their personal data (Vranica, 2019). Indeed, before the GDPR, collecting and sharing people's data with third parties without their consent was a usual phenomenon. Excesses like Cambridge Analytica's use of unconsented targeted political advertising via Facebook in 2016 show how targeted advertising can take a harmful turn (Tarran, 2018). Thus, this topic is relevant not only for business but also for citizens (i.e. Internet users) as data tracking has become inextricably linked with online practices in our current society. Furthermore, the scientific value of this study lies in better understanding the feelings and experiences among consumers and between consumers and marketing practices like consumer surveillance. From the point of view of consumers, whose personal data is being collected from companies, it is crucial that companies adjust their data tracking practices to be more user-friendly and less privacy-invasive (Boerman et al., 2017). Moreover, consumers' perspectives can provide valuable feedback and suggestions for future improvements of personalized advertising. On the other side, consumers can learn more insights regarding data tracking and personalized advertising as forms of consumer surveillance and benefit by obtaining a more responsible online behavior.

Therefore, to provide insights into actual consumer practices and perceptions, this research makes use of qualitative data collection through the means of in-depth interviewing and via digital participant observation, which was inspired by Møller and Robards (2019). There has been little academic focus on digital participant observation in the field of advertising studies, since restricted studies have used participant observation (i.e. Scott et al., 1990; Redmond & Griffith, 2006). Hence, taking actual online user behavior as a starting point, the interviews included an activity whereby young consumers were asked to log in to their social media platforms, detect the types of advertisements and explain to the researcher the feelings and the reactions about personalized advertising. This study explores Greek millennials and contributes to a growing body of research mainly focused on Western populations (i.e. Bol et al., 2018; Obar & Oeldorf-Hirsch, 2018), with a qualitative investigation of Greek millennial social media users, a group of people that has not received so far much scholarly attention. In particular, generation Y (i.e. millennials) is nowadays the most active group on Facebook (77%) and Instagram (70%) according to the 2020 Consumer Culture Report (Pickard-Whitehead, 2020).

1.2. Research question and sub questions

In order to provide qualitative insights into how Greek millennials react to targeted ads, a research question and three sub questions were created to guide this research:

RQ: How do Greek millennials experience targeted and personalized advertising on their Facebook and Instagram feeds?

SQ1: How do Greek millennials react to personalized advertising when using Facebook and Instagram?

SQ2: How do Greek millennials perceive targeted and personalized advertising practices?

SQ3: What, if any, measures have Greek millennials taken to protect their privacy, and reduce or prevent data-tracking?

1.3. Chapter outline

This thesis comprises five different sections. After the introduction, the theoretical framework provides insights into current academic literature regarding data tracking, personalized advertising, consumer surveillance, privacy attitudes, and privacy-preserving practices. The methodology section discusses the rationale of the research method, the use of in-depth interviews along with digital participant observation, the sample, and the use of the constructivist grounded approach for interpreting the findings. Subsequently, in the results section, the most relevant findings of the in-depth interviews are analyzed and interpreted with help of existing literature. In the last section, the research concludes by answering the research question as well as the sub questions. Lastly, by contemplating the limitations of this study, suggestions for future research are provided.

2. Theoretical framework

Before investigating how Greek millennials experience targeted and personalized advertising, on their Facebook and Instagram feeds, it is essential to provide a theoretical basis for this study. Therefore, this theoretical framework conceptualizes consumer surveillance in relation to personalized advertising, privacy, the reception of personalized advertising, and privacy attitudes and practices.

2.1. Data tracking and personalized advertising as forms of consumer surveillance

During the 1940s, market research was driven by a need of aligning company production with consumers' inclinations to enhance production efficiency (Pridmore & Zwick, 2011). To accomplish this, it was urgent to monitor consumers by using consumer surveillance techniques. More specifically, the term surveillance refers to "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007, p. 14). Therefore, surveillance can occur in numerous fields (i.e. from health to communication) and for various reasons such as enhancing the safety of the watched (i.e. the lifeguard at the beach).

The history of surveillance is as old as humanity because the activity of gathering information about people is intertwined with human existence (König et al., 2020). In fact, this activity has been increasingly common in the marketing and advertising sectors in the past decades (Pridmore & Zwick, 2011). Hence, the usefulness of people to collect data can be found in their need to learn about other people before attempting to interact with them. The structure of online communications enables marketers to learn information about users through their daily actions, such as online purchases, use of online search engines on the Internet publishers, and ad networks. The importance of consumer surveillance lies in the special economic value as well as the competitive advantage that commercial firms gain (Ruckenstein & Granroth, 2020) because it is less costly to target specific customers that have an interest in specific products or services. For instance, consider a company that sells pointe shoes and advertises those dancing shoes only to people who are interested in ballet. Of course, the latter would be more likely to buy the advertised product than people who are not interested in dancing. For that reason, the act of monitoring consumers can be very advantageous for businesses.

2.1.1. Free content justifies the collection of personal data

In particular, on social networks like Facebook and Instagram, where various interactions take place (i.e. ‘likes’, ‘shares’ and ‘comments’), there is no monetary refund. Thus, people must provide some personal data (i.e. hours of usage or user engagement) in return for the free content (Tabora, 2019). McFarlane (2020) also admits that the primary way that social media like Facebook and Instagram make money is by selling advertising to other companies. As a consequence, watching online advertisements constitutes the key reason for free content on the Internet. Additionally, König et al. (2020) argue that precise details of people’s lives are collected, stored, and processed on a daily basis within vast computer databases that are owned by large corporations. Organizations take advantage of living in this ‘tracked society’ as it enables them to use this consumer data to develop as well orient future business practices. Accordingly, by collecting customers’ information companies manage to increase their marketing efficiency and effectiveness because consumer behavior can be predicted (Pridmore & Lyon, 2011).

2.1.2. Personalized advertising and profiling in digitalized era

Since the introduction of new media and communication technologies and the spread of broadband and mobile devices, personalized advertising and marketing campaigns have become part of consumers’ daily interaction with brands. In order for the companies to send personalized content that is relevant to consumers’ lifestyles and reduce the number of unwanted advertisements, it is essential to know consumers’ interests and demographics (i.e. age, gender, and nationality). In marketing, the act of knowing and understanding the customer is crucial because it enables companies to determine the applicability of an advertisement, with the aim to deliver it to the audience that is the most interested in (Eldering, 2001). For this reason, “a consumer profiling system which can profile the consumer, provide access to the consumer profile securely, and return a measurement of the potential applicability of an advertisement” is needed (Eldering, 2001, p. 1). Consumer surveillance practices like consumer profiling systems enable companies to show personalized advertisements and work with targeted marketing campaigns with the ultimate aim to intensify the ad’s click-through rates and increase business profit (Ur et al., 2012).

For marketers, relevance is both important and critical as they need to understand consumers to interact with them at a highly intimate and personalized level. Indeed, to control the communication and consumption environment, marketers have to become “intimate experts” (Darmody & Zwick, 2020, p. 7). By using current and emerging technologies of

consumer surveillance marketers are able to predict consumers' behaviors, beliefs as well as choices, and address them at a highly personalized level. Also, the structure of online communications that promotes self-disclosure, enables marketers to learn more information about users than in the past with traditional media (i.e. television and radio) (Evans, 2009). Consequently, every user profile gets a unique choice context adapted specifically to users, based on their preferences, habits, and other identifiers (Damody & Zwick, 2020).

In the words of Aguirre et al. (2015, p. 2), personalization is about “a customer-oriented marketing strategy that aims to deliver the right content to the right person at the right time”. One way to display personalized advertising is to use Online Behavioral Advertising (OBA), which nowadays constitutes a common practice for businesses. This marketing practice would be impossible without cookies because these small pieces of data that are placed on websites can track and store users' online activities and preferences (Johnson, 2021). More specifically, with the use of cookies marketers can receive and store consumers' information and utilize it to target people grounded on their interests. In this case, advertisers monitor consumers' online behavior and use this collected data to show them individually targeted advertisements to promote their campaigns (Boerman et al., 2017). OBA enables more precise advertising by creating pertinent and effective ads and therefore it is considered to be one of the most prevalent advertising techniques in the future (Kumar & Gupta, 2016). As a result, OBA can be understood as a practice of tracking users across websites to deduce the interests and preferences of consumers.

2.2. Privacy: conceptualization, self-disclosure negotiations, and regulation

Data collection through personalization practices and profiling has a direct impact on consumer privacy. More precisely, privacy has been recognized as one of the fundamental human rights in the 1948 Universal Declaration of Human Rights. Accordingly, the majority of people consider privacy in the everyday life as an important value. This is verified from the findings of two surveys that Pew Research Center conducted. In particular, the vast majority of the respondents (93%) feel that it is important to control who can get information about them as well as what kind of personal information can be collected about them (Madden & Rainie, 2015).

However, privacy constitutes a broad as well as diverse concept, and there are various definitions rather than one universal-agreed notion (Boyd & Marwick, 2011). According to Westin (1967), informational privacy refers to the right of choosing what kind of personal information about an individual is known to other people. Similarly, Van der Velden and El

Emam (2013) define informational privacy as the ability to control who collects and reveals one's information and under which circumstances. The focus of this research is on informational privacy on the Internet and most specifically on social media. This is due to the fact that informational privacy has become one of the most predominant issues of today's digital era because young people disclose a vast amount of personal data on social media networks (Boyd & Marwick, 2011). As a result, people tend to be careful about privacy issues because of the risks that are intertwined with information disclosure (Aquisti & Gross, 2006).

2.2.1. Privacy calculus around self-disclosure

Through online activities, like online shopping, consumers provide organizations with vast amounts of personal information, which enables companies to tailor their products and services to people's interests and preferences. But it is common for consumers to think about whether or not they will trade personal data to receive advantages in return. To be more precise, the privacy calculus theory as described by Bol et al. (2018) reveals that in some cases online self-disclosure practices are based on a cost-benefit trade-off because consumers have to weigh the hypothesized benefits and privacy risks to decide whether or not they will provide their personal data to the retailer. Interestingly, even though several studies show that users consider privacy as a highly ranked value (Dinev & Hart, 2006; Obar & Oeldorf-Hirsch, 2018) and they are aware of the possible risks of online disclosure (Xie et al., 2019), consumers are still willing to provide personal information online in exchange for advantages such as coupons, discount codes, and bonuses. Nonetheless, the potential risks are not insignificant to be overtaken. Online self-disclosure can be risky since personal information provides instant access to financial accounts, credit card records, and other financial assets. Consequently, the potential misuse of consumers' information can lead to identity theft, fraud, stalking, and harassment. Lastly, as Brake (2014) discusses, people might reveal sensitive data not only about themselves but also about others (i.e. friends, relatives, colleagues), and as a result, more people would be put at risk. Hence, these users can be seen as privacy pragmatists, who are constantly engaging in decision-making progresses where they have to assess the costs and benefits and eventually determine if the self-disclosure practice is worthwhile (Dinev & Hart, 2006). It must be noted that privacy legislation attempts to set limits "to the ever more data-hungry business models of many Internet enterprises like advertising companies and e-commerce sites" (Ziegeldorf et al., 2014, p. 2730). In particular, there have been established numerous regulations by public policymakers against

technological developments with the goal to protect people's data on the Internet. The most recent regulation is the EU's aforementioned GDPR.

2.2.2. Communication Privacy Management

Negotiations of online self-disclosure are also discussed in Communication Privacy Management theory (CPM). CPM has been applied to online social media in the last years whereby its central focus has been on privacy regulation that takes place via communicative interactions (Petronio, 2013). In particular, CPM theory refers to the way that people manage private information and reflect their attitudes towards privacy, and describes the reasons that people are willing or not to disclose personal information (Petronio & Durham, 2015).

As Petronio (2010) argues, the system of CPM consists of three main elements; a) privacy ownership, b) privacy control, and c) privacy turbulence. Regarding privacy ownership, it focuses on individuals' belief that they are the owners of private information. As a consequence, they are responsible for not only protecting private information but also managing this information in order to reach the desired goals. Hence, ownership can be restricted to the individual or can be shared with other people (Petronio, 2010). Subsequently, privacy control focuses on the conditions that people consider when they give or deny access to private information. Ownership signifies that people have the right to control the flow of private information and make use of specific privacy rules. These privacy rules are established with the aim for the people to determine how, with whom, and for how long other individuals can have access to someone's private information. Moreover, privacy rules are rooted in decision criteria such as motivations and cultural values (Petronio, 2010). For instance, there are different cultural values regarding privacy, and for that reason, English people have higher privacy needs than the Israelis (Durham, 2008). The last element of the CPM theory which is privacy turbulence has received significant focus during the last decade. This is because privacy regulation can have unforeseeable impacts and as a result, it is possible for privacy management systems to fail. Therefore, privacy turbulence constitutes the sign for "the needed change in the privacy management system regarding privacy rules and expectations for appropriate privacy regulation" (Petronio, 2013, p. 11).

The CPM theory addresses the level of individual control over privacy because it provides an understanding of how people decide to handle their personal information and manage their privacy. Individual control over privacy also occurs on a different level along with the establishment of privacy regulations by public policymakers.

2.2.3. General Data Protection Regulation

The GDPR (2016/679) was established on the 27th of April 2016, with the aim to protect users' privacy and provide them with more transparency about, and control over their personal information (Vranica, 2019). This is accomplished by obliging organizations that have an online presence to inform users in clear and specific language about the data collection strategies used and by asking users' freely given consent. Therefore, terms of policy constitute the way for online advertisers to legitimize their engagement with Internet users. Nonetheless, the consent request for users' data collection is written in vague and unclear language along with confusing and verbose terminology (Kshetri & DeFranco, 2020). Furthermore, Tabora (2019, para. 1) argues that these documents are vague for Internet users because the documents are "too long to read and even harder to understand". Numerous previous empirical researches (Obar & Oeldorf-Hirsch, 2018; Steinfeld, 2016) have displayed that these policies are usually ignored by users. In fact, McDonald and Cranor (2008) explored the average time that a regular Internet user should devote to read the terms and conditions document, and surprisingly it was 40 minutes per day. Consequently, Obar and Oeldorf-Hirsch (2018, p. 5) argue that the phrase "I agree to the terms and conditions" that Internet users just click on the accept bottom without actually reading them, is believed to be "the biggest lie on the Internet". Thus, regardless of the actual effect that terms of service have on consumer behavior, regulations like the GDRR constitute important tools that create awareness of data collection practices.

2.3. Receptions and experiences of personalized advertising

One of the goals of this study is to investigate consumer reactions towards personalized advertising. Ruckenstein and Granroth (2020) claim that even though consumers' reactions to targeted marketing vary, there are three prevalent and divergent emotional reactions to personalized advertising that will be discussed next; fear, irritation, and pleasure.

2.3.1. Personalized advertising as pleasing for the consumer

To begin with pleasure, as De Keyzer et al. (2015) argue, consumers are inclined to respond positively to online advertising when the personalized message is detected as personally relevant (i.e. when there is a match between the message and the consumers). In particular, customers are pleased when the algorithm really understands them and operates the way they want, by displaying advertisements with desirable content. In this case, when there

is an increased personal relevance in advertisements, they can be perceived as helpful or even useful for consumers (Ur et al., 2012). Additionally, if the content of an advertisement is more connected to people's interests, when a skier receives an ad about ski equipment for example, then the advertisement seems more appealing for the consumer (Tucker, 2014). The reason is simple; people are able to find new products that are fitted to their interests. Thus, it is clear that a higher depth of personalization is closer to consumers' interests and preferences, and consequently, such advertisements are not only believed to be helpful, but also obtain greater click-through rates (Bleier & Eisenbeiss, 2015).

2.3.2. Personalized advertising as irritating for the consumer

On the other hand, social networks are mainly used by people as a means of entertainment, contact, and connection. Especially for young people, social media are considered the most prevalent communication channels due to the digitalized era they have been embedded in from an early age (Chu, 2011 as cited in De Keyzer et al., 2015). For this reason, consumers feel distracted when they receive advertisements in a medium that is designed for personal amusement and connection with friends and relatives. Similarly, consumer irritation can be evoked due to pop-up ads and banners that appear constantly on the Internet. Research conducted by Ur et al. (2012) revealed a close relationship between online advertising and annoying pop-ups since the latter can be perceived by consumers as an aggressive way of advertising. Accordingly, people feel like advertisers 'bombard' them with commercial messages, and as a result, consumers have no trust in pop-up ads. Furthermore, even though people find helpful online advertising that is relevant to their interests or their behaviors, the same does not apply when the algorithm shows targeted advertisements based on personal criteria like demographics (i.e. gender, age, nationality). More precisely, as Ruckenstein and Granroth (2020) illustrate, users feel that marketers see them only as caricatures that are categorized based on their gender. As a consequence, consumers are disturbed by this tactic due to the fact that both advertising and marketing fields tend to promote and replicate gender stereotypes (for example when a young woman gets an advertisement about pregnancy tests). One last case that user annoyance occurs is when the market fails to understand the needs of the consumer. This is caused by misaligned personalized advertising or failed automated targeted advertising (Ruckenstein and Granroth, 2020). Also, it is very common for people to have already bought a product or a service but the same banner keeps being displayed to them over and over. As a result, consumers feel that they are being profiled inaccurately (Ur et al., 2012).

2.3.3. Personalized advertising evokes fearful feelings in consumers

Regarding fearful reactions, these are related to concerns about the misuse of personal information by the advertisers and the fear of hacking users' data. More specifically, consumers are frightened when they are not aware of what kind of data will be collected and how will be used by organizations (Ruckenstein & Granroth, 2020). Studies have shown that people are prone to experience the feeling of vulnerability if they realize that firms collect secretly their data (Aguirre et al., 2015). This is due to the fact that companies can gather personal information without users' knowledge and consent via covert as well as misleading strategies (i.e. lack of explicit cookie notification).

On the contrary, consumers seem to appreciate overt data collection techniques due to the fact that companies choose not only to inform users about the collection of personal information but also to ask users to give their consent for the data collection. Thus, with the use of cookie transparency, users are likely to feel that they maintain control over their personal data. Concerning again users' feelings of fear, in the research of O'Donnell and Cramer (2015), participants hesitated to click on targeted advertising because of facing past negative incidents with online fraud and scams by clicking unknown targeted ads. It is necessary to mention at this point that consumers are more positively inclined to click on trustworthy retailers' advertisements and websites than on unreliable ones (Aguirre et al., 2015). Hence, unknown as well as trustless retailers and websites are likely to cause negative and worrying feelings to online customers. Lastly, consumers experience fearful reactions when the online targeted advertising mimics their past behavior (Bleier & Eisenbeiss, 2015) and there is a high possibility to feel like losing control over their privacy. This is justified since people feel like being followed and monitored, which makes targeted advertising being perceived as privacy-invasive.

2.4. Privacy attitudes around personalized advertising

Besides emotional reactions to online targeted advertising, people are also prone to react to privacy implications of Internet use in general and targeted advertising in particular, and display privacy apathy, fatalism, or concerns.

2.4.1. Privacy apathy

According to Sharma and Crossler (2014), privacy apathy can be described as the indifference towards privacy risks because of users' perception that privacy is nonexistent on

the Internet. Privacy apathy can be explained by consumers' past privacy invasion experiences because their personal information has already been shared with third parties, and consequently, it is inevitable to protect this data for the future. As a result, many people adopt unconcerned behavior based on the belief that sooner or later companies will get users' information anyway and they are willing to provide personal information online if this has a benefit (i.e. discounts, or free software) (Yoo et al., 2012). This passivity can also be caused by consumers' ignorance of the Internet's risks such as hacking, identity theft, and stalking. A cynical and unconcerned attitude towards privacy can be dangerous because it often goes hand in hand with a lack of privacy-preserving practices as well as limited awareness of the value of personal information (Yoo et al., 2012).

Such behavior can be explained by the rational fatalism theory. More precisely, according to Xie et al. (2019), rational people are willing to take the risk and share a vast amount of personal data if the risk becomes unavoidable. Additionally, numerous empirical studies have shown that people are prone to disclose more personal information on the Internet including social media, than in face-to-face communication (Tidwell and Walther, 2002). It is essential to state that nowadays, people are likely to disclose personal information due to the lack of awareness of the dangers that lurk, as disclosing constitutes an important part of online activities (i.e. online purchase), or in maintaining social interactions and relationships (Hargittai & Marwick, 2016). Consequently, social networks have created a feeling among people that they must disclose every detail of their lives (i.e. from what they are eating to what they have ordered).

2.4.2. Privacy concerns

Previous research has revealed that the collection of personal information can pose profound challenges for consumers' privacy (Awad & Krishnan, 2006). More specifically, when people do not trust online companies and experience targeted advertising negatively they are likely to raise concerns about their personal information and not provide their data. Also, when companies decide to covertly collect users' data by not informing consumers about what kind of data will be collected, how retailers will use this information, and for how long will be stored, people can exhibit privacy concerns due to the lack of awareness and consent (Eldering, 2001). It is worth mentioning that regular Internet users lack basic knowledge of how tracking mechanisms collect, store and use their data (Kshetri & DeFranco, 2020). This absence of understanding of how tracking practices operate is without a doubt the key factor that marketers take advantage of, to collect personal data (Tabora, 2019). As a

result, consumers cannot comprehend the various ways that tracking systems collect personal data and for what purposes this data will be used. According to Evans (2009), online advertising businesses can be transparent about the tracking mechanisms they use and with whom this data is shared. However, they hesitate to do that, firstly because of the cost and secondly due to the fear that consumers may not want to disclose their personal information (Evans, 2009).

2.5. Privacy-preserving practices

Since people are deeply concerned regarding their privacy on the Internet, many of them are even highly motivated to engage in privacy-protective practices. As a result, it is equally critical to look into the mechanisms and tools that consumers employ to preserve and protect their privacy. The practices that people have adopted to secure their online privacy include tactics such as deleting cookies, using private browsing, and ad block software.

2.5.1. Using ad blocking software

The practice of installing an ad blocking tool has risen significantly along with online advertising. Ad blockers are software programs that restrict or modify advertising content on websites. More specifically, during the loading of a webpage, the ad blocker evaluates the site's scripts and prevents any scripts that need to be blocked (Kolowich-Cox, 2015). Consequently, ad blockers enable users to avoid advertisements for the online content they consume. As Pujol et al. (2015) argue, there is a wide variety of ad block software for Internet users who want to evade or protect themselves from online and targeted advertising with the most popular being 'Adblock Plus' and as an alternative 'Ghostery'. Of course, many of them install an ad blocker with the aim to eliminate the annoying types of ads like banners and pop-up ads (Kolowich-Cox, 2015). An (2016) shows that in a sample of 731 ad blocker users in the U.K., U.S.A., Germany, and France, indeed the majority of them (64%) install ad blockers because of perceiving advertisements as annoying and intrusive. In particular, 73% of those users do not like pop-up ads, 70% do not like advertisements on mobile phones, and only 40% find advertisements on Facebook annoying. As a result, when consumers experience advertising negatively they are likely to install ad blockers. Ann (2016) also explains that the second most common reason for using an ad block tool is the disruptive nature of the advertisements (54%). For instance, while people are watching a video on YouTube and an ad suddenly appears on the video. Therefore, it seems that ad block users are mostly motivated to use an ad blocker because of perceiving personalized ads as intrusive rather than privacy-

invasive. More specifically, fewer people reported that they use ad block software because of security concerns (39%) and privacy concerns (32%). Concerning the former, the majority of websites host third-party advertisements, and consequently, people are concerned that the ad might be a virus, or a fraud (An, 2016). This is justified since the quality and the content of the advertisement cannot be checked by the retailer.

Similarly, privacy concerns are exhibited because of the lack of consumers' awareness regarding the collection, usage, and storage of their personal information. Thus, ad blocking can be seen by users as a means of maintaining control over personal data while browsing on the Internet. Interestingly, also more than 80% of respondents within all age groups desire software that can block all the ads on mobile phones (An, 2016). In this context, it is worth mentioning that the utility of ad block tools poses a tremendous threat for the advertisement as well as marketing industry and content publishers because regular Internet users can avoid paying for the free online content by blocking trackers, which prevents the disclosure of personal data to companies (Pujol et al., 2015).

2.5.2. Deleting cookies

Another often-used privacy protection strategy that people can use is deleting or declining cookies. In the context of this strategy, a survey of more than 1,000 US respondents that Pew Research Center conducted in 2013 revealed that people were worried about their personal data being available online. Accordingly, a clear majority (86%) of participants had taken action by erasing their digital 'footprints' and by clearing their browsing history and cookies. There are numerous opt-out tools at the disposal of consumers, which can take advantage of with the aim to preserve control of online privacy and eliminate online advertising. More specifically, consumers can use opt-out tools such as the "PrivacyMark" or the "Evidon Global Opt-Out" to set opt-out cookies for multiple advertising networks (Leon et al., 2012, p. 2). However, as Leon et al. (2012) observed, these tools are not only unfamiliar but also difficult for regular online users to understand and most of them tend to get confused because of the technical language in these tools. As a result, the majority of people are usually "unable to set opt-out or blocking preferences meaningfully on a per-company basis" and only privacy-sensitive people are motivated to learn how to handle successfully these blocking settings (Leon et al., 2012, p. 3).

The difficulty of these settings depends on the type of Internet browser, as these have different privacy settings. For instance on Internet Explorer in order to block third-party cookies, people have to navigate in the 'Advanced' menu, whereas on Firefox there are

specified and distinct settings for that purpose. Additionally, according to Wills and Uzunoglu (2016), the difficulty is determined by the nature of the browser extension tool as Adblock Plus is based on filter subscription lists (i.e. the EasyList and Acceptable Ads filter lists) by default to decide what kind of ads will block, but Ghostery does not have default options because it blocks user-selected cookies. At this point it is essential to state that these aforementioned practices (i.e. ad block software and deleting cookies) have a major drawback; advertisers can detect these practices and forbid consumers to visit the website or cause some parts of the websites to lose important functions (Leon et al., 2012). Lastly, even though consumers really like these privacy-preserving practices, concerning their effectiveness consumers are skeptical not only due to the usability flaws on the websites but also due to the limited protection that ad-blocking tools provide against third-party trackers.

2.5.3. Using private browsing

Private browsing constitutes one of the most popular and commonly used privacy-protecting features, as every modern browser includes such a mode. The use of private browsing enables the user to open a secure browsing window that does not save or track the user's browsing history/activity, cookies, and site data or search terms. In Firefox it is called 'Private browsing', in Google Chrome 'Incognito mode' and Internet Explorer has named it 'InPrivate browsing' (Aggarwal et al., 2010). According to a survey of DuckDuckGo, which was conducted in 2017 to explore consumers' perceptions of private browsing, 46% of surveyed users have used private browsing at least one time and 33% have reported using it on a daily basis. Moreover, younger people (i.e. between 18-29) were five times more expected to be aware of private browsing than older people but strikingly, more than 64% of all respondents did wish that their browser could protect their privacy more efficiently.

However, the efficiency of this privacy protection tool is also doubtful. More specifically, as stated by Hoffman (2017), private browsing does allow other applications on a user's computer (for instance a spyware application) to monitor browsing activity and accordingly, people who control websites and the website's server can still track and store user's personal information. Besides, it is a usual misconception that private browsing can protect users from being tracked by other Internet service providers as well as websites and hence personalized advertising. That is why the majority of people misunderstand the privacy protection that this tool provides and consequently 66% of consumers overestimate the protection of private browsing (DuckDuckGo, 2017). Furthermore, as Abu-Salma and Livshits (2020) describe, many respondents wrongly believed that private browsing could be

used to send encrypted e-mail, achieve online anonymity, or even visit a hacking webpage safely. Therefore, the effectiveness of private browsing lies mainly in searching for airplane tickets because travel companies usually keep track of people's browsing activity in order to adjust the prices, or when users do not want targeted advertising as well as annoying suggestions for searches that they are not within their interests (Aggarwal et al., 2010). For example, a woman may have bought a new car and she is searching on the Internet for an insurance company. Once she chooses a company to insure her car, she will not want to be bombarded with more suggestions in the future.

2.5.4. Privacy-preserving practices on Facebook

Facebook constitutes an important social network, especially for students because of the university Facebook groups and the need for both social interaction and network building. But many users are constantly negotiating the urgency for connecting with friends and colleagues with the desire to preserve their privacy. As Debatin et al. (2009) describe, on the one hand, there is the small and visible part of Facebook, where people are chatting, sharing content, and having fun, and on the other hand, there is the larger invisible part of Facebook, which is fueled by people's personal information and online interactions such as likes, comments or shares. This larger part serves marketing and advertising purposes as by gathering people's data, marketers are able to display targeted advertisements and increase the click-through rates.

Hence, since Facebook represents the most common social media with more than 2.6 billion monthly active users (Tankovska, 2021) it is normal for users to make use of specific online strategies to decrease privacy concerns. First of all, people who are concerned about their privacy on social media networks are inclined to provide only the essential personal information (i.e. name, surname, e-mail address, and day of birth) in order to be able to create an account and no additional sensitive or contact information (i.e. phone number, location, employment, age, and sexual orientation). The purpose of that practice is to prevent social media networks to make use of this data in order to display to people targeted advertisements. In fact, people can protect their privacy and avoid the collection of their information, by even putting false personal information, or modifying their information in privacy settings (Chen & Rea, 2004). However, it can be argued that only skilled and young users can utilize these social networks' privacy-protecting settings and tools to preserve their privacy (Brake, 2014). Thus, despite the fact that Facebook can be an integral part of people's lives, some of them are still engaged in privacy-preserving strategies.

The foregoing conceptual framework has explored the useful and beneficial role of personalized advertising for companies. By monitoring and collecting people's data, companies can deliver content that is relevant to consumers' interests. Subsequently, this marketing practice allows businesses to promote their products and services to specific audiences and therefore to increase their business profit in return. But since a vast amount of consumers' personal data is tracked, it is normal for people to react to this marketing practice and develop emotions towards targeted advertising. The reactions can be either positive or negative. Of course, some of the consumers adopt privacy attitudes such as apathy, concern, and get engaged in privacy-preserving tools and practices. Thus, these points inform the study's methodology, which will be discussed in the following section.

3. Methodology

The research method that has been employed for investigating Greek millennials' knowledge, experiences, as well as feelings around personalized advertising, was qualitative. A qualitative approach was adopted to obtain an in-depth account of consumers' perceptions and to gain an explicit understanding of them. According to Barnham (2015), qualitative research enables a more comprehensive insight into a phenomenon as the researcher goes beyond common sense explanations and consequently gets a 'deeper' level of understanding. Besides, qualitative research gives emphasis on seeing the social world from the viewpoint of the 'actor' and, especially in this research, of the consumer (Hannabuss, 1996). Furthermore, qualitative research allows for exploring people's experiences as well as inner feelings (Ghaljaie, et al., 2017). Therefore, it has been the best way of 'understanding' how people make sense of a certain and complex phenomenon and in this case of data tracking and personalized advertising. The following sub sections provide a justification of the data collection, a description of the method used to answer the research question and sub questions, the operationalization of the research question, the analysis of data, and lastly issues of credibility.

3.1. Sample

To answer how Greek millennials experience targeted and personalized advertising on their Facebook and Instagram feeds, a non-probability sampling technique has been used to collect the required data (i.e. interviews), and more precisely purposive sampling. Non-probability sampling enables the researcher to use his/her own judgment for choosing a sample of units from a population due to the restricted resources and time (Etikan et al., 2016) and hence not everyone in the population has the same possibility of being selected. Non-probability sampling is also the best solution if randomization is difficult due to the large population. First of all, with the use of purposive sampling the researcher can choose participants that meet specific requirements across a broad spectrum. Besides, it is often used in qualitative research since it enables to "identify and select the information-rich cases for the most proper utilization of available resources" (Etikan et al., 2016, p. 2).

3.1.1. Sampling criteria and data collection

The participants were selected from the researcher's personal network and were recruited by e-mail. The sampling criteria were as follows; a) to be students or young professionals of 22-28 years old (millennials), b) to be active on social media, and more

specifically spend a minimum of 2 hours a day and c) to have Greek nationality. Millennials or Generation Y, who are born between the 1990s and the 2010s (DeVaney, 2015) formed a criterion due to their use of social media platforms in general and Facebook and Instagram in particular. According to the 2020 Consumer Culture Report, Facebook was the most popular social media network among all age categories, with the millennial generation using it the most (Pickard-Whitehead, 2020). Furthermore, Instagram emerged as the most effective, with 94% of people influenced by Instagram clicking, sharing, or buying a product that was displayed on their feeds. Regarding the gender distribution, the aim was to collect a sample with at least two-thirds of females because it has been statistically proved that women spend more time on social media (Greenwood et al., 2016). Above all, limited studies have explored Greek people as consumers (i.e. Papafotikas et al., 2014), but no empirical study has ever investigated Greek consumers' reactions to personalized advertising, which makes this case unique.

3.2. Interview procedure

For the current study, qualitative interviews were the most suitable research method. This research decision was chosen because it was important to understand how people experience data tracking as well as personalized advertising. Moreover, this method is particularly useful in comprehending consumers' perspectives and emotions to answer properly the research question and sub questions of this study. As described by Kvale (1983, p. 174), a qualitative interview's aim is "to gather descriptions of the life-world of the interviewee with respect to interpretation of the meaning of the described phenomena". Moreover, in-depth interviews have been used as they enable the researcher to seek deep responses on that personal matter through their lived experiences, personal stories, and values (Johnson, 2011). Also, during an in-depth interview, the researcher can co-produce along with the respondent as "the informant becomes a collaborative partner" (Johnson, 2011 p. 9). Besides, semi-structured interviews are less rigid than structured interviews and allow the researcher to explore the topic more openly and the interviewee to express his/her thoughts in his/her own words (Esterberg, 2002). As a result, the researcher was able to understand Greek millennials' perspectives and opinions through her interaction with the participants. Also, the researcher managed to elaborate answers that the participants expressed in their own words without being influenced by suggestions from the interviewer (Foddy, 1993). Ultimately, the interviewer was able to achieve a deep level of knowledge and understanding of the complex phenomenon of targeted advertising. Moreover, the main goal of this research was to access

the perspectives of young consumers, who were interviewed, so open questions have been the most fitting choice. Lastly, due to this structure, the interviewer had the ability to do follow-up questions on interesting topics as well as clarifying questions.

3.2.1. Online interviews

In February and March of 2021, 14 interviews of 45-60 minutes were conducted with Greek millennials to meet the aims of the study. However, due to the Covid-19 restrictions and lockdown in Europe and especially in Greece, it was not possible to conduct face-to-face interviews. Accordingly, the interviews took place online via Zoom, which is a popular video conferencing application, and an invitation was sent to the participants 30 minutes before the scheduled interview. As Janghorban et al. (2014) suggest interviews that are held online enable participants with time and place limitations to have more favorable conditions as they do not need to manage a person-to-person meeting. Therefore, the main advantage of online interviews is that they allow both researchers and participants to overcome obstacles that are related to time, geography, and physical mobility and as a result, participant recruitment is made more convenient. However, conducting online interviews also has disadvantages. To begin with, the non-verbal communication cues such as body language, facial expressions and, proxemics are lost (Gruber et al., 2008). For instance, the interviewer cannot understand if the participant feels awkward, as the nervous body language is not able to be detected. As a consequence, it has been more difficult for the interviewer to establish rapport with the participants, which was crucial for the respondents to feel comfortable enough to share personal experiences and emotions. Lastly, during an online interview, it is very likely to face technical problems because of poor Internet connection, and of course, not all respondents would be familiar with the technology. As a result, some respondents did not know how to share the screen during the zoom meetings and sometimes the audio was not very clear.

The final sample comprised of a total of 14 interviewees and an overview of them can be found in Appendix E. All participants were Greek and 4 of them currently live abroad for studies. Regarding the gender distribution, 10 respondents were women and 4 were men. All participants were between the ages of 23 and 26 years old. Additionally, all participants were regular Internet users, active on Facebook or Instagram (or both) and all reported the potential of having Internet access on the mobile phone, which suggests having continuous access to social media. Furthermore, the interviews included mostly students and young professionals from various fields, for example, medicine, political science, economics, law, human resources, telecommunications, marketing, and psychology. Lastly, all the interviews were

held in English, since Greek youngsters are taught the English language at an early age at school.

3.2.2. Operationalization

Initially, the interviewees were welcomed to the interview, thanked for their time, and then were asked some general questions, for instance about their work experiences and hobbies during spare time. These simple planned questions (i.e. ice-breaker questions) are essential to build rapport between interviewer and respondent and establish a better interpersonal interaction. As Johnson (2011) reports, building trust during in-depth interviews is quite important as the participant feels more comfortable answering the questions and is inclined to provide more information for the study. Afterward, the researcher started asking questions to gather relevant and valuable information for this study. In Appendix C there is a detailed table about this process. Since the interviews were semi-structured, for better performance, an interview guide with some thought-out and follow-up questions was used in order to gather accurate data, assure coherence in respondents' answers and keep the conversation on track. The following section will provide an overview of the interview guide, and the full version of the guide can be found in appendix A.

In particular, the interview guide included three major concepts which were informed by the literature discussed in the theoretical framework and the sub questions. The first concept "social media and use" was operationalized by asking respondents about their use of social media, their favorite social media platform, from which device they log in et cetera. These questions were asked with the aim to provide some background information about the importance of social media in people's lives and about the type of personal information users feel comfortable sharing on these platforms.

Then the interview was focused on the second concept "personalized advertising" (Eldering, 2001) which is the core topic of this study. This concept was operationalized by asking respondents their feelings as well as by observing their reactions to personalized advertisements that were found on their Facebook or Instagram feeds. As a result, by asking questions like "How do you feel when you see targeted ads and banners on your social media platforms?" the researcher was able to collect relevant data regarding Greek millennials' attitudes towards personalized advertisement. This interview section was designed with the goal to answer the first sub question: How do Greek millennials react to personalized advertising when using Facebook and Instagram?. During the interviews, it was expected that some participants would not be aware of what personalized advertising means so a definition

was provided by showing a video. That video (Iabuk, 2012) explained how companies can obtain consumers' data to display personalized advertisements that are close to their interests. It also emphasized that no personal details are collected during that process and that with the use of personalized advertising people can receive interesting advertising content which can be useful for future purchases.

Additionally, to better understand their perceptions regarding targeted advertising on social media, participants were asked under which circumstances they perceive it as disturbing (Ruckenstein & Granroth, 2020). In that way, the researcher collected more in-depth answers based on users' personal experiences. Following, to answer the second sub question and report how Greek millennials users experience personalized advertising and data-tracking practices that companies use to display targeted advertisements, respondents were asked not only how companies make use of these practices but also how they feel about data surveillance and profiling.

As mentioned before, the interviews included digital participant observation. Becker and Geer (1957) argue that participant observation refers to the method in which the researcher participates overtly or covertly in daily life as well as activities of the people under study, with the goal to observe the changes in their behavior over a certain period of time. Hence, inspired by Møller and Robards (2019), the researcher has interviewed and observed respondents while they were visiting social media and scrolling down in their Facebook or Instagram feeds. In particular, the respondents have been asked to share their screen via Zoom in order to show which personalized advertisements they encountered while visiting social media feeds and were asked to express their feelings about these ads. This way, it was expected that participants would be more likely to share some of their own reactions, past experiences, examples, and concerns about targeted advertising. As a consequence, the researcher has collected more information about the event under study because she has spent more time with the participants during the latter's daily activities. Lastly, with the help of digital participant observation, this study has become more innovative (Møller & Robards, 2019).

The last concept was privacy with a focus on privacy-preserving practices and tools (Pujol et al., 2015; Leon et al., 2012; Brake, 2014). These concepts were operationalized by posing questions about how users feel about privacy on social media and what measures Greek millennials have taken to prevent data tracking and keep their personal information private. With the use of these questions, the researcher was able to collect relevant data concerning the third sub question and document the most common and effective ways to

preserve personal information. Towards the end, some questions about companies' terms of service (Obar & Oeldorf-Hirsch, 2018) were also asked in order to provide background information on whether or not these banners are considered important and efficient by users. In this section, a video explaining how companies utilize consumers' data for profiling purposes via social media, and two pictures about consumer surveillance were used as prompts (see appendix A) to make the interview more comprehensive, engaging, and interesting. Before the end of the interviews, all participants were asked if they had any questions, or if they want to add any information that they deemed important.

3.2.3. Research ethics: consent forms and pseudonymization

Collecting participants' information while conducting interviews can raise specific ethical issues (Johnson, 2011). Therefore, social researchers should ensure to protect subjects as well as their personal data by all means. Accordingly, in February as well as March 2021, interviewees from the researchers' personal network were invited by e-mail to participate with an attached information sheet as well as a consent form, which is enclosed in Appendix D. The consent form informed participants about their rights in terms of the interview, allowing them to withdraw from the research at any point. It is notable to mention that there has been no monetary compensation as it was included in the consent form that people's participation is voluntary. Thus, in order to signify willingness as well as acceptance to get interviewed, people had to return the consent form signed. The vast majority of the participants (i.e. 12 out of 14) signed the consent form, whereas the remaining two preferred to consent only orally. Moreover, Oliver (2010) suggests that since the ethical guidelines for social research must be explicit and comprehensive, the researcher should inform participants a) for what purposes the material from the interviews will be used and b) who will have access to this data. Consequently, the respondents were notified that this research is conducted for only academic purposes and that the data will be used only by the researcher. The consent form also ensured the potential respondents that they will not be identified as the researcher has used only general data such as age, gender, and occupation.

The concepts of confidentiality and pseudonymization are of utmost importance in social research. To be more precise, according to Wiles et al. (2008), every researcher ought to protect and preserve respondents' confidentiality, when conducting research. Hence, by omitting data and by changing participants' main attributes, the researcher has been able to prevent the identification of the people who participated in the study. Most of all, the primary way to keep participants' personal information safe is through the process of anonymization

(Wiles et al., 2008). Thus, after conducting the 14 interviews, all respondents' names were pseudonymized, and they were named with 14 usual Greek names as table 1 shows.

Table 1: participants' pseudo names

| Participants | Pseudo names |
|----------------|--------------|
| Participant 1 | Anna |
| Participant 2 | Chris |
| Participant 3 | John |
| Participant 4 | George |
| Participant 5 | Demy |
| Participant 6 | Maria |
| Participant 7 | Kate |
| Participant 8 | Angie |
| Participant 9 | Elena |
| Participant 10 | Nickie |
| Participant 11 | Julia |
| Participant 12 | Pavlos |
| Participant 13 | Zoe |
| Participant 14 | Barbara |

3.3. Data analysis

Once all the data of the in-depth interviews was gathered, it was essential to convert the audio-recorded data into textual data in order for the researcher to analyze it. Hence, after transcribing the interviews from the digital audio recorder, the transcriptions have been analyzed through thematic analysis inspired by the three analysis phases of (constructivist) grounded theory. As Clarke and Braun (2017) argue thematic analysis is a methodological approach suitable when researchers are looking for people's opinions, thoughts, and experiences of a certain phenomenon and when research is based on qualitative data, such as interview transcripts. Thematic analysis also constitutes the best option for approaching lengthy interview transcripts and identifying themes as well as patterns. Hence, thematic analysis constitutes the best way of identifying specific patterns of meaning (i.e. themes) across the data, which are relevant to answering the research question of this study (Clarke & Braun, 2017).

Regarding coding, a constructivist grounded theory procedure has been used. To begin with, constructivist grounded theory is a methodological approach appropriate for exploring important matters that people experience (Glaser, 1978; Strauss & Corbin, 1990). Thus, it is suitable for this research, which concerns online and personalized advertising. Following Strauss and Corbin (1990), the research question and sub questions of this study were informed by theory in a constructive manner. In other words, the inductive analysis allowed themes to emerge from the interview data in a bottom-up manner whereby theory did not determine the analysis process. While coding with the use of the constructivist grounded theory, the researcher tried to approach the data with an open mindset and have no preconceived ideas and predetermined thoughts. Indeed as Glaser (1978) describes, the researchers should be sensitive towards and avoid interpretations based on pre-existing hypotheses and biases. Strauss and Corbin (1990) agree with the aforementioned statement adding that in grounded theory the truth is “enacted” rather than pre-existing. Hence, the grounded theory emphasizes the researcher must be close to the participants’ ideas during the analysis, and only through constant comparisons of all data the process of analysis can be successful (Mills et al, 2006).

According to Glaser (1978), coding constitutes the way of converting raw data and in this case interview transcripts, into social theoretical constructions. More precisely, at the first stage, the open coding must be a line-by-line coding based on the content of the transcripts (see coding scheme in appendix B). The researcher should constantly compare the transcripts to find similarities between the concepts discussed, and conceptualize data always by staying close to the text (Kendall, 1999). Moreover, during the process of open coding a computer-aided qualitative data analysis software has been utilized; Atlas.ti. This tool is commonly used for the qualitative analysis of large bodies of textual, visual, or audio data in various as well as numerous researches (Smit, 2002). After open coding follows axial coding, where several open codes are clustered into some descriptive axial codes. For example, the open codes “ads with free services are beneficial”, “ads with sales and discounts are welcome”, and “ads with informative content are helpful” are grouped into the axial code “useful features of personalized advertisements”. Thus, axial coding is used to identify themes that emerged from the data, since the researcher makes comparisons and connections between the categories of open coding (LaRossa, 2005). In that way, the researcher is able to capture the ideas that he/she sees in people’s personal stories and experiences to understand better how consumers perceive as well as react to targeted advertising (Strauss & Corbin, 1990). The final coding process in grounded theory is called selective coding and it aims to explain the behavior of the

respondents or of the phenomena under study. During the selective coding phase, the researcher returns to theory to link the predominant themes with core categories of existing literature. For instance, the axial codes “ads are annoying”, “conditions that advertisements can be annoying”, and “consumers’ fearful reactions of personalized advertising” are all described by the selective code “drawbacks of personalized advertising”. Consequently, this approach has enabled the researcher to look into the text in much detail as well as depth and find certain patterns or systems of meaning in order to connect them with literature and finally answer the research question with data that serve as relevant evidence.

3.4. Credibility: reliability and validity

As stated by Noble and Smith (2015), qualitative studies are regularly criticized for restricted scientific rigor due to the nature of the qualitative method adopted and the subjective opinions of the researchers. As a consequence, throughout the research, it was important to pay attention to the two central concepts of credibility (i.e. reliability and validity). To begin with, reliability is about “the degree to which the findings of a study are independent of accidental circumstances of their production” (Kirk & Miller, 1986, as cited in Silverman, 2011, p. 360). To achieve reliability it was important to primarily make the research progress transparent by providing a detailed explanation of the theoretical framework, the selected methods, and the progress of data collection as well as analysis of the current study. Additionally, as suggested by Moisander and Valtonen (2006), it is essential to pay attention to “theoretical transparency” by providing an explanation about the interpretative decisions of the data. Hence, with the use of the two aforementioned ways, the progress of the study is transparent, it obtains methodological rigor and lastly, the readers can be convinced about the study’s trustworthiness (Moisander & Valtonen, 2006). Regarding the interviews, to make sure that this research was reliable, it was important for the researcher to ensure that each and every interviewee understood the questions in the exact same way, in order for their answers to be coded with consistency (Silverman, 2011). For that reason, the topic list of the interview was pretested and then adjusted according to the feedback (for example some questions were rephrased or clarifications were added).

On the contrary, validity refers to “the extent to which an account accurately represents the social phenomena to which it refers” (Hameersley, 1990, as cited in Silverman, 2011, p. 367). As stated by Glaser (1978), when using grounded theory as a method, the researcher should have no preconceived ideas and predetermined hypotheses about the phenomenon under study. Thus, to further ensure that this dataset was valid the tool

of analytic induction through the constant comparative method was used (Silverman, 2011). Consequently, all data fragments in this case regarding personalized advertising were compared to find out not only similarities but also differences to ensure that all different perspectives were equally reported. Of course, the researcher needed to take into account also deviant cases that did not meet her expectations, to make sure that the findings are valid. For that reason, all the interview transcripts were included in the final dataset. Lastly, to ensure the reliability and validity of the findings, the approach of triangulation was also selected. According to (Flick, 2018), with the aim to increase the validity of the results, good research practice obligates the researchers to use the method of triangulation. To be more precise, triangulation refers to the combination of methodologies used during the investigation of the same phenomenon (Denzin, 1978). Hence, by combining interviews along with the participant observation method, the findings became more trustworthy. Finally, the coding scheme that can be found in appendix B makes the aforementioned research choices and the whole research progress transparent. Therefore, the next section presents an in-depth overview of the main themes identified in the coding scheme.

4. Results

After analyzing the findings using the constructivist grounded theory approach, five broad themes emerged from the 14 performed interviews. These five themes provide an understanding of Greek millennials' positive and negative perceptions of personalized advertising on Facebook and Instagram, their knowledge about personalized data-tracking practices, and the measures that Greek millennials have adopted to prevent data tracking and protect their privacy.

The predominant themes that occurred during the in-depth interviews will be explicitly discussed in the following sub sections. A preparatory overview of the themes is provided in the following table 2.

Table 2: themes and subthemes

| Themes | Subthemes |
|---|--|
| Acknowledging the benefits of personalized advertising | Useful features of personalized advertisements for consumers |
| | Useful features of personalized advertisements for business |
| Drawbacks of personalized advertising as perceived by consumers | Personalized advertising is annoying for the consumer |
| | Consumers' fearful reactions to personalized advertising |
| Consumers' knowledge of data-tracking practices | Understanding of consumer surveillance |
| | Consumers' assumptions of ads' origins |
| Consumers' privacy attitudes | Apathetic responses of personalized advertising |
| | Privacy concerns |
| Consumers' privacy negotiations | Privacy-preserving practices |
| | Self-disclosure strategies on social media |

4.1. Acknowledging the benefits of personalized advertising

A recurring theme was participants' pleasant feelings when they were asked to

describe their reactions towards personalized advertising. Of course, pleasure was not the only prevalent feeling and for that reason, it is essential to elaborate on the conditions that make personalized advertising on social media, like Facebook and Instagram, desirable.

4.1.1. Useful features of personalized advertisements for consumers

Consumers react positively to online advertising that is personally relevant and close to their preferences because they feel that the algorithm understands their needs and displays interesting content to them (De Keyzer et al., 2015). Consequently, consumers perceive personalized advertising not only as useful but also as helpful for them. This research reflects on the aforementioned statements and provides insights into which types of ads are appreciated by the respondents.

All participants agreed that it is better to receive advertisements that are close to their interests than irrelevant ones. In particular, Anna who is a medical student believes that it is really helpful for her when she gets advertisements displaying medical applications or medical pages because otherwise, she could not find them. Moreover, Chis, who is a computer engineer, recently wanted to purchase a specific Personal Computer, but he was struggling because that PC was not sold in Greece. However, one day he saw an advertisement about a company in another country that had that specific product. Hence, with the use of that personalized advertisement on Instagram, he managed to buy it. Julia provides an example of a helpful advertisement:

I think something helpful was when I was looking for a pair of shoes and I really wanted to buy a specific kind of shoes, but I couldn't find it, like exactly the thing that I wanted. And one day I was scrolling, I don't know on Instagram or something. And I saw a pair that I really liked, and then I clicked on it. But then of course on every page that it went, it was like this advertisement. Uh, but it was really helpful because finally I bought the boots. So this, this is that I wanted. So it was very helpful for me, uh, because I couldn't find exactly what I wanted by the time I saw the advertisement.
(Julia)

Participants were very positive when receiving personalized advertisements with content that provided information about a service or a product. In fact, George points out that he is happy with 90% of the advertisements he receives on social media. A good example of this can be found in the interview with Zoe who saw on her Instagram feed one interesting post about a tour guide in Europe:

Uh, well, these is one advertisement about, traveling about tour guiding in Europe, and

for me, it's really interesting because through this, I can see places where I'm interested to go, to travel, to visit. And it's really useful because, it mentions this advert mentions the prices or some discounts about the trips. (Zoe)

Elena also thinks that since she is a master's student and she is keen on the marketing field, ads about Google classes are not only interesting but also beneficial for her. This kind of advertisement is useful for her because she can discover new ways to improve her skills and gain new knowledge. As a result, all participants were happy when receiving advertisements with useful content on social media and none of the participants exhibited concerns about companies knowing their interests.

4.1.2. Useful features of personalized advertisements for businesses

In addition to the personal benefits highlighted by all respondents, half of them also acknowledged the value for businesses. John, in particular, recognizes that, while he uses free services, those services or applications were invented and developed by others. Accordingly, he does not mind targeted advertising. In fact, he tries to support creators by watching personalized advertisements on social platforms intentionally. To exemplify:

After some point I just realized that when somebody is creating the music, they also want to get paid for that. And, sometimes I take the ad block off in order to support, uh, either musicians or content creators in YouTube...I actually want to support the YouTube channels or media creators and content creators in Facebook that use these advertisements to earn some source of payment for the content they create. (John)

Indeed consumers understand that although social media companies like Facebook and Instagram offer freely available services on the Internet, they still need to earn money. As McFarlane (2020) admits, the primary way that social media like Facebook make money is by selling advertising to other companies. Tabora (2019) also verifies this practice, by stating that when consumers do not pay for the product they use, the product is them.

Moreover, with the use of targeted advertising companies can deliver “the right content to the right person” (Aguirre et al., 2015, p. 2) and subsequently increase business profit while receiving more click-through rates on their advertisements (Ur et al., 2012). Elena, whose family owns a small business speaks not only as a consumer but also on behalf of business owners. She confirms that personalized advertising can be very advantageous for small companies, as it constitutes a good marketing technique to reach new audiences. As a result, personalized advertising that is relevant to consumers' lifestyle can be very beneficial for businesses, too:

To be honest, I also see it from the other side, not only from the consumer perspective... Like it really helps small companies and I mean, maybe someone searches from the Netherlands, for example, searches Greek islands. And because my parents have a hotel in a Greek island, my company will come up and he may be a potential client. So actually social media has created so many new ways and so many new paths of getting new clients and making more money, even the small businesses, not like let's not say about Google, uh, which already has so many money, so much money, but yeah, I'm, I'm kind of like thankful that there are tools for also smaller businesses to yeah increase the profitability. (Elena)

4.2. Drawbacks of personalized advertising as perceived by consumers

On the contrary, the second overarching theme that can be derived from the interviews refers to the drawbacks of personalized advertising on social media. During the in-depth interviews and while scrolling through their social media feeds, participants expressed not only pleasure but also annoyance towards some advertisements.

4.2.1. Personalized advertising is annoying for the consumer

All respondents believe that social media does not constitute the ideal place for marketers to advertise products or services. In particular, when they were asked for what purposes they use social media, the most prevalent answers were: a) communication, b) entertainment, c) keeping in touch with friends and family, and d) artistic reasons. This reveals that none of the respondents used social media with the aim to watch personalized advertising. As a result, personalized advertisements on social media, and especially on YouTube and Instagram stories, are believed to be disruptive and people get annoyed because of their appearance. For instance, Chris admits that he finds personalized advertising disturbing as well as disrupting because he usually logs in to his Instagram account during his office breaks to check his friends' posts and not advertisements. Similarly, Anna feels that scrolling on Instagram to see her friends' posts takes her double the time due to online advertising. Hence, she gets annoyed and she characterizes targeted advertising on social media as "a waste of her time".

On YouTube there is also a major drawback; advertisements cannot be easily skipped and consequently, it makes them even more interruptive as well as irritating. This is observed from the conversation with Demy. She hates advertisements on YouTube because she is not able to see the video that she wants either to skip the advertisement easily. This kind of

advertisement pops up out of nowhere at different parts during the video and the user is obliged to watch the first 15 seconds of the advertisement to skip it. As discussed in the theory section, consumers feel distracted when receiving advertisements in a medium that is designed for personal communication and amusement. This mirrors the argument of Ur et al. (2012), that when people come across disrupting advertisements and pop-up banners their irritation is evoked.

The majority of participants (i.e. 8 out of 14) agreed that getting the same advertisement, again and again, is very disturbing for them. Elena considers personal advertisements helpful but she reminisces one time when she visited a site only once and for the next two weeks she was receiving the same advertisement everywhere in her social media feeds. She describes that experience as intrusive and she adds that she has not visited that website since then. This reveals that automated market algorithms can fail to match consumers' desires with appropriate advertising content (Ruckenstein and Granroth, 2020). Similarly for Barbara, annoying is the fact that she keeps "watching the same thing again and again and again". Angie summarizes all of the above with the following quote:

I think it related to the frequency that I see these advertisements. So if I see something once I just ignore it, so it's okay, maybe after some minutes I will forget about this, but when I see something often, then I'm like what's going on? Why do I see this all this time? (Angie)

It also appeared that participants were deeply bothered with the content of specific ads. That content was mostly about gender characteristics, violence, and political issues. Anna argues that since she is a female, marketers display her advertisements about dresses and perfumes. When Angie was asked to describe one advertisement that was really annoying for her that was her answer:

I notice that very often that there is an advertisement of Clear Blue, the pregnancy prediction tests. That I have talked about it with some friends that they also have the same advertisement and that happens very often. Eh, I don't really understand why, because I don't think that I had searched for it. But maybe they are making big campaigns through social media at girls of my age, probably. (Angie)

For Angie, advertisements that emphasize gender inequality or gender traits are not only bothering but also unethical. Indeed, Ruckenstein and Granroth (2020) verify that consumers do not want to be categorized based on their gender because marketers tend to promote advertising that emphasizes stereotypical gender roles and displays.

Political advertising is another instance where its content was found to be disturbing.

Political beliefs tend to be considered as a very personal choice and should not be advertised on social media. Participants like Kate state that they have even received a sponsored advertisement regarding a political party that was against their political ideology. That is why Pavlos considers it inappropriate for political parties to persuade voters by using personalized advertising. Indeed, corporate marketing can fail to understand the needs as well as the interests of the consumer (Ruckenstein and Granroth, 2020).

4.2.2. Consumers' fearful reactions to personalized advertising

The outcome of the in-depth interviews also generates fearful perspectives concerning consumers' data tracking and personalized advertising. Zoe, who has limited technical knowledge and basic computer skills, admits that she is afraid of clicking targeted advertisements on social media. More precisely, since she does not know the creator of the advertisement, she believes that it may be derived from hackers and thus "they can easily steal or steal money from you, especially when they just want your number from credit card". Moreover, Zoe experiences fearful reactions when receiving personalized advertising because of the possibility that advertisements on social media contain viruses. As she says, that can be disastrous for her laptop and her stored files.

On the other side, Pavlos expresses his fear for a completely different case. Pavlos, like others participants, perceives personalized advertising as a tool that companies can either use for good or bad purposes. But, when companies own such a "powerful tool" it is hard to keep a balance and not use it for their own profit.

The problem is when you cross the line...And I don't think the problem is the tool, I don't think it's a problem of having cookies, advertising, and analytics in internet. I think this is a good tool, but people, I think getting the temptation of using it for bad causes. Because they give you faster money. So yeah, I think that can happen a lot. And I'm aware that this has also happened for, there was a lot of involvement of this type of analytics in politics. They can influence the results of voting and yeah, this sometimes can be dangerous. (Pavlos)

This previous quote does not only give information regarding consumers' fearful reactions to personalized advertising, it is also a subtle reference to the Cambridge Analytica scandal. In that case, Facebook covertly collected and harvested the personal data of more than 87 million users in order to send personalized messages to users and ultimately influence their vote for the 2016 United States presidential election (Tarran, 2018). As a result, people feel like losing control over their privacy and perceive personalized advertising with fear and

hesitation (Bleier & Eisenbeiss, 2015).

4.3. Consumers' knowledge of data-tracking practices

The third overarching theme is about consumers' knowledge of personalized advertising on Facebook and Instagram. Consumers were familiar with the data tracking mechanisms that companies use to display targeted advertisements. They were also able to detect the type of personal data that companies monitor and store to show people advertisements relevant to their preferences and lifestyle.

4.3.1. Understanding of consumer surveillance

Many companies utilize data tracking and personalized advertising as forms of consumer surveillance (Pridmore & Zwick, 2011). These practices are used with the aim to understand the consumer better and deliver to individuals advertisements that are most interested in (Eldering, 2001). This is supported by the findings of this study because they show that the majority of respondents are aware that companies track personal data by setting cookies on websites. Furthermore, respondents were able to understand and detect when and how businesses make use of cookies for data tracking. As a result, marketers are able to collect consumer data and that is why consumers get to see personalized advertisements based on their interests.

Kate, who is an undergraduate psychology student, states that once she accepts cookies on the websites she visits, she automatically gives permission to companies to collect her data and send her relevant advertisements. Elena also believes that companies use cookies to track consumers' interests. She specifically states:

You visit their site and you say that I allow cookies and therefore they see that you, um, search for a specific product. So that way this company, the same company will give you ads of stuff that you put on your card or from stuff that you recently viewed or similar companies. For example, let's say I went to the Adidas site and put a specific, uh, the superstar shoes in, in my card. Then of course, if I allow my cookies, I will see advertisements of this specific shoe. (Elena)

This is partly contrary to the view of scholars (Ur et al., 2012; Boerman et al., 2017) that consumers lack knowledge about how personalized advertising works. People do understand how companies gain access to their data. As John explains, given the fact that almost every website runs with cookies, companies gain access to consumers' information by collecting and analyzing these cookies. Pavlos also thinks that:

Cookies are there to sell our data. And, when you use an Internet site or an application or whatever these cookies are used by the person owning the site or the app to collect those data and then transfer them to other companies or people who are interested in your data. So, for example, if I was a company interesting to sell some products to people between 25 and 35 that have searched of basketball or I don't know, sports or whatever, then these sponsored advertisements would like just focus myself because I'm in between the 25 – 35 age gap, and I have also searched in the past about basketball or something like sports. (Pavlos)

During the interview a video (Iabuk, 2012) that explained how personalized advertising works was displayed to the participants in order to report if they had any gaps in their current knowledge. Most of the participants were familiar with the way that consumer surveillance mechanisms work but they reported that it constitutes a complex practice. Demy argues:

That's pretty much how it works. Uh, well, there more to that than the video. It was very simple and self-explanatory, so it was useful, but there are more tricky parts than the video. So yeah, it was a very simple way of explaining the process, but I don't think that's only the process. There are like a million parts in there that we didn't see, but yeah, I was a helpful video. It explained a couple of steps. (Demy)

Indeed, personalized advertising is a multidimensional procedure and consequently, it cannot be presented explicitly in one short video. Surprisingly, many participants had doubts regarding the trustworthiness of the video (Iabuk, 2012) and more specifically about the statement that companies do not track and collect consumers' personal information such as name, address, and phone number. They also thought that the video was biased since it was focused more on the business perspective and only on the beneficial part of personalized advertising. To exemplify, George points out that he is not completely sure if companies do not track and collect his personal information like his name. Moreover, Pavlos is suspicious because he thinks that the video is trying to simplify a complex topic by not looking equally at both sides; the consumer's and the company's. Kate explains after watching the video:

Also at some point in this video, there was that they're not collecting information such as my name or my address or something personal. I don't think that this is accurate 100%, I think sometimes so though it's not right, they're collecting this kind of information and yeah, it's showing the only one aspect of the advertisement industry. (Kate)

These opinions are justified by the fact that before the GDPR was put in effect,

companies could covertly collect consumers' data without informing them. Moreover, as Eldering (2001) argues, companies are not transparent about what kind of data they collect, how they are used, and for how long will be stored.

4.3.2. Consumers' assumptions of ads' origins

As was aforementioned, the interviews included participant observation. With the use of that practice, participants were asked to describe what kind of data they thought that companies had been collected based on the personalized advertising they came across on social media feeds. The majority of the interviewees (i.e. 8 out of 14) assumed that personalized advertising was based on browsing history. In particular, respondents were not surprised with the online suggestions that social media displayed to them because they have searched similar products in the past by using online searching machines like Google. For instance, Nickie detects that the sponsored advertisement regarding jewelry that was on her Facebook feed was displayed to her because of checking the product's website a few days ago. Another respondent Demy agrees that she has noticed that if she searches for a product online, then she will receive a personalized advertisement of that product. Additionally, for Julia personalized advertisements include not only websites that she has checked before but also products similar to the ones that she has purchased online.

I saw many, many times many different advertisements for roller skating, for roller skates because recently I bought a pair and I saw like everywhere was in my, in my feed. It was like everywhere, really, for many, many brands, not just from the brand that I bought it from. (Julia)

One more common assumption among the participants was that the targeted advertising on social media was based on participants' location. Nevertheless, it appeared that participants were not aware as well as interested in advertisements that were displayed with criterion people's location. John, who lives the past 2 years in the Netherlands, admits that he has no idea about the sponsored advertisement concerning the Dutch political party "D66". However, he believes that since he lives in the Netherlands and uses a Dutch Internet provider it is normal to see these advertisements. The same applies to Anna, who lives in Romania for studies for more than 4 years.

(I get) Romanian (products) because I am in Romania, I believe it's not all of them Romanian, but now we're like but most of them are Romanian, but I believe it's because I live in Romania. So probably the way their advertisement system works which according to the current location mostly so because if they sent me something

that is in the USA, I couldn't get it. So it's I think it's normal for them to show me products that are local, Romanian, which I have easier. (Anna)

These assumptions are confirmed by literature since various consumers' data and daily actions such as online purchases, likes, time spent on websites, and browsing history are monitored and collected by the companies. This personal data provides companies valuable information to determine the applicability as well as the effectiveness of each advertisement (Eldering, 2001). Again, contrary to the claims of Ur et al. (2012) and Boerman et al. (2017), the respondents showed that they are knowledgeable and can detect the type of personal data that is collected by companies. Therefore, Greek millennials were not surprised by the targeted advertisements they got.

4.4. Consumers' privacy attitudes

The fourth overarching theme refers to the privacy attitudes that consumers have adopted. More specifically, consumers' privacy apathy was a common response to personalized advertising due to the lack of online privacy. Of course, many respondents also raised privacy concerns due to the collection of their personal information.

4.4.1. Apathetic responses of personalized advertising

Based on the findings, it was clear that participants were aware of the data tracking mechanisms that companies use to display targeted advertisements. Another noteworthy finding was that even though people acknowledge the risks of self-disclosure, they are still willing to provide their personal data on companies via social media. Barbara states that she does not care that companies use her data for marketing reasons and as a result, she has no second thoughts when self-disclosing on the Internet.

It's not going to change, you know, so I'm compromising and because I have worked in digital agency, um, I can understand to a point that they need to do this. So as a company, I can get behind that. As a consumer, it's not the best, but because I have worked in these types of companies and I know the system I'm compromising.

(Barbara)

This reveals that it is a common attitude for people to adopt an apathetic response towards consumer surveillance for marketing reasons. According to Xie et al. (2019), people are willing to disclose their personal data because they have knowledge of the data tracking system and it is unavoidable to resist. This is in agreement with this study because respondents feel that it is inevitable to protect their personal information on social media.

Thus, Angie outlines that she has also compromised with the idea that whatever data she puts online, even after deleting her accounts, social media companies can still have access to it.

As Tabora (2019) argues when consumers do not pay for the product they use, the product is them. That is why John and Elena do not try to prevent data tracking as they understand the way that the market works and companies make money. People feel obliged to provide some personal information and consequently they believe that there is no point in trying to prevent data tracking. To exemplify, John explicitly states:

I understand that I'm also the product of the social media. So my information are being sold to ad companies. So since I understand how capitalism works and how social media works, uh, I wouldn't say that I find them annoying or something. (John)

Sharma and Crossler (2014), point out that the explanation of privacy apathy lies in participants' belief that it is inevitable to keep their personal information private on social media. This proved to be the case because during the interviews, participants were asked how they feel about their privacy on the Internet, and, surprisingly, all participants of this study replied to that question by stating that there is no privacy on the Internet. For Julia, privacy does not exist on the Internet, and for Angie, there is no privacy at all on social media. Demy admits:

I don't think there is much of that. Like no, there is no privacy. Like apart from really personal stuff, like passwords and the e-mail accounts and stuff like that. Yeah. No privacy, whatever you put on the Internet, it's public knowledge. Like if someone knows how to look for it, they'll find it. (Demy)

From the responses, it is obvious that information disclosure and a perceived lack of privacy go hand in hand as the more information gets exposed the less privacy people experience. Individuals feel that once they disclose personal information on social media, it cannot be characterized as private anymore.

According to Sharma and Crossler (2014), one more explanation of such behavior is due to consumers' past privacy invasion experiences. Hence, if consumers have already provided their data to companies it is inevitable to protect it for the future and consequently, many people adopt this unconcerned behavior. As a result, if people have already exposed themselves on social media they will not care about their personal data anymore. Thus, George thinks that Google knows everything about us and he explains the reason.

I mean, eventually they have everything about me. I'm pretty sure, but they know everything about me. But I think that like in, in near, like near past, I think, no, I have not given like any consent but. Yeah, as always, you have to consent in everything in

those applications. So either way they, they know everything about me, I'm pretty sure, and of course I can understand that from the, from the ads that I get on Instagram. (George)

It was also interesting to observe the privacy apathy when participants visited a website. Almost half of them accepted the terms of service/policy without reading them. All those participants report that each and every websites' terms and conditions are not only written in a vague language with complicated technical terms but are also lengthy and boring. For instance, Pavlos states that "they have some really general rules in their consent forms of monitoring various interest points, but this is not so clear to a person what this means and not even clear to experts". Consequently, Nikie believes that reading terms of service is a waste of time since she must accept any way to be able to visit the website. Hence, reading terms of policy is considered useless firstly because people are obliged to accept them and secondly because even if consumers read them, they will not comprehend them. This reflects the argument of Obar and Oeldorf-Hirsch (2018, p. 5) that accepting these terms of service without reading and understanding them is "the biggest lie on the Internet".

4.4.2. Privacy Concerns

One more prevalent sub-theme is participants' privacy concerns due to data tracking practices that companies make use of. Participants acknowledge the value of consumer data for companies and five of them believe that companies take advantage of this data not just for commercial and advertising purposes. In particular, they think that big companies like Facebook and Instagram collect personal data that users disclose on social media and then sell a massive amount of people's data to third parties. Kate finds this practice not only unethical but also anti-democratic because companies use personal data "for other reasons" without having users' permission.

You know, it's, um, it makes me worry sometimes, that if someone start to use these factions not for consumerism, not for reasons regarding to consumerism but they can do it for other things. Like they're doing it in some, not so democratic countries. And I mean, it's official that they're doing it. If they can do it for companies, for companies who want to sell products, they can do it and for other reasons, that are against democracy. (Kate)

Pavlos puts himself in advertisers' shoes and argues that it is hard to store a large amount of personal data and not use them for innovative as well as profitable reasons. He thinks that it is "a big dilemma" and "hard to control myself and not using all the data I can".

It was also interesting to observe that during the interviews, most of the participants raised privacy concerns by reflecting on their own personalized advertising experiences. The vast majority of them were really worried about receiving personalized advertisements about products after talking on the phone or after having a conversation about them with friends. All participants find this type of personalized advertising worrying and creepy since they claim that they have never searched these products online and as a result, a feeling of constantly being monitored has been created. Chris refers to a recent conversation with his colleagues about motorcycles. He admits that whilst his phone was off, and he has never searched or been interested in motorcycles, he received a relevant advertisement:

Motorcycles is something that I never searched, I never see a video about that, I never searched it in the Google. It's completely irrelevant with me, and a week later, or some days later to be accurate, the Instagram provided me with advertisements with that, to buy motorcycle... if you can think about it...It's scary. (Chris)

Almost all participants had a similar experience to describe but Demy took it even further; “I did an experiment at a time. We're talking about babies and babies' clothes and we're talking like an hour long about babies' clothes. (laughing) And then there were babies' clothes on my feed. That was weird”. She also adds that although the practice of hearing her phone conversations is creepy and makes her feel being stalked, nowadays it has become a common situation.

Consequently, participants feel that social media are watching them and this type of surveillance has no limits. None of the participants has ever consented to monitor his/her mobile's microphone and camera. These quotes highlight the argument by Bleier and Eisenbeiss (2015) that consumers are expected to express worrying feelings when the online targeted advertising mimics their behavior at a highly personalized level. This is justified because people get a feeling of being spied on or monitored and subsequently, personalized advertising is perceived not only as privacy intrusive but also invasive.

On the other hand, Elena and Pavlos have a different explanation regarding those personalized advertisements. In particular, Pavlos deems that people provide all their interest points either by self-disclosing on social media platforms or by searching on Google. As a result, these companies have stored so much data about people that can actually predict their interests. Elena also believes that there is a misconception “because we see so many things and so many advertisements and so many friend requests that we don't really pay attention to them. But when we catch something that we recently saw or talked to, yeah, we make a big deal of it”.

Similarly, in line with this topic Fowler (2019) reports that it is technically possible for applications to secretly record users' conversations but to date, there is no research evidence found of such practice. Hence, it is more likely that consumers have unconsciously searched for particular products or paused in their feed to check products or services that they were discussing with a friend online. Finally, big companies like Facebook and Google record personal information (i.e. names, birthdates, credit card info) simply by asking for it and consumers' browsing habits by cookies or transparent image files like "Facebook Pixel" (Fowler, 2019).

4.5. Consumers' privacy negotiations

The fifth overarching theme describes the various practices that consumers have taken to protect as well as preserve their personal data. Additionally, it refers to the self-disclosure strategies that social media users have adopted to manage their online privacy.

4.5.1. Privacy-preserving practices

Privacy concerns have an impact on how participants try to prevent data tracking and on what kind of privacy-preserving practices they have adopted. As Büchi et al. (2017) point out personal privacy protection has become a necessity in modern life. During the interviews, many common privacy-preserving negotiations such as changing passwords frequently or setting strong passwords, and using fingerprints to enter mobile applications have been reported. However, it is interesting to investigate the more complex ones.

The findings verify the study of Boerman et al. (2018) which found that declining or deleting cookies and browsing history constitute the most common practices for people to protect their online privacy. For instance, Julia admits that when entering a website, she accepts only necessary cookies with the aim to minimize the risk of her information being used by companies. Demy also makes use of that practice and sometimes she attempts to even reject cookies. However, the majority of the participants like Demy report that they are obliged to accept cookies because otherwise, they are not able to access the website "I don't accept the cookies. Which is sometimes a problem because if I don't, they won't let me in a website".

Since people feel forced to accept cookies, another often-used privacy protection strategy that participants adopt is deleting cookies. More specifically, when erasing cookies, participants like Chris report that they protect their privacy by not overcharging their laptops with personal information. However, many female participants answered that they do not

have the knowledge to delete cookies. Indeed, on the basis of literature, regular online users are unfamiliar with these technical settings and as a result, they cannot erase their digital ‘footprints’ (Leon et al., 2012). Furthermore, every browser has different privacy settings, which makes it even harder for average users to utilize those tools.

Two male interviewees, who have enhanced computer skills, use practices that are not so widespread among regular Internet users. The first is Virtual Private Network (VPN) and as Chis argues he uses VPN on a daily basis to prevent his ASP provider from storing his personal information. According to Hoffman (2020), truly VPN can provide users a secure connection to another network over the Internet and prevent their browsing activity to be tracked by companies’ prying eyes.

Pavlos takes it even further by using TOR (i.e. The Onion Router). As he describes, Tor includes both multiple layers of VPNs and anonymity and subsequently, his data is re-encrypted several times. Pavlos wants to keep his personal information safe when he communicates with other people, and that is the reason he has installed this multi-level encryption application.

In line with privacy-preserving practices, other respondents provided information that indicated that they use private browsing, which is one of the most popular and commonly used privacy-protecting features for ensuring privacy on the Internet. Private browsing enables the user to open a secure browsing window that does not save or track the user’s browsing activity (Aggarwal et al., 2010). Maria uses private navigation on the Internet when she does not want to reveal her identity.

I have done this a few times, for example, for LinkedIn to check one person I used, through private mode or from my company, yes because they, I don't want them to see that it's me or that, uh, yeah. I try to hide some info. (Maria)

Similarly, participants like Chris use incognito mode to search on the Internet without revealing their preferences as well as their interests. Hence, they believe that they are less likely to get personalized advertisements based on personal data. On the other hand, some respondents have doubts about the effectiveness of private browsing because they still have to accept cookies. Elena does not think that incognito mode or deleting cookies can be efficient.

I would still get advertisements. Like it would not solve the problem for me, it would be nice if I didn't get any ads, but I don't think that there's something that I can do to totally eliminate the problem. (Elena)

This quote highlights the fact that private browsing actually permits other applications on a user’s computer to track consumer browsing activity and store personal information in

order to display targeted advertisements (Hoffman, 2017). However, they acknowledge the useful features of private browsing which makes it ideal for searching for airplane tickets or buying gifts. In fact, half of them admit that they use private navigation for booking cheap airline tickets.

Even though ad block constitutes a popular privacy-preserving tool in Greece, all participants who have downloaded this software reported that they use it mainly on annoying advertising on YouTube. In particular, Julia uses ad block only on YouTube because she wants to see videos and listen to music without having annoying ads disrupting her. Kate agrees by stating “it's really annoying to see advertisements everywhere. Like every three video, every three stories. There is an advertisement. That's why only because it's annoying, I mean, not because I'm concerned for my personal data and stuff like, only because it's annoying”.

As a result, ad block is considered a great tool for reducing or even eliminating personalized advertisements, and that is the reason that its use is focused only on YouTube and not on social media like Facebook and Instagram. This is also mirrored in the empirical research of An (2016), in which it was found that the majority of people use ad blockers due to the annoying and disruptive nature of the advertisements and not for protecting their online privacy.

4.5.2. Self-disclosure strategies on social media

Towards the end of the in-depth interviews, participants were asked if and how they protect their personal information on social media. All of the participants responded positively and as a result, various self-disclosure strategies have been reported. All participants seem to adopt a responsible attitude on the Internet concerning their personal information by setting a limit in self-disclosure, with the aim to not expose themselves and their data. Based on these findings, the connection to the CPM theory can be clearly perceived. This theory approaches the different ways that people manage their private information and their attitudes towards privacy (Petronio & Durham, 2015). Additionally, it justifies the reasons that people hesitate to disclose personal information to preserve their privacy online.

In particular, the vast majority of the participants keep both their Facebook and Instagram accounts private to limit the visibility of their personal data. Hence, the privacy settings of both Facebook and Instagram seem to be appreciated by users. Based on the participants' responses, it is apparent that they feel more comfortable self-disclosing only on friends and family members rather than on strangers. Julia has changed her Instagram account

from public to private because she is no longer inclined to share personal moments with people she does not know. For that reason, she even uploads Instagram stories, using Instagram's "Close Friends" feature, which allows her to post only for a selected group of followers. The same applies to Barbara:

I don't want people to have access in my life. (laughing) I want them to see only what I want them to see. And also I think this is kind of childish, like to... when I was 14 years old, maybe if I had a relationship I would post that on Facebook, but no, definitely not now. (Julia)

In line with the previous concept, when Barbara is asked to specify the personal data she usually discloses, this is her answer:

I always allow for the camera to have access in my photos, never location, only use it while using the app. Never my mobile phone. Um, I think that Facebook used to ask for the address. I would never put that as well now. Like basic information, like the things that you need to fill in, in order to create an account. So for example, name, last name, age, e-mail, password, username, stuff like that, but very personal information, like where I live or what my mobile phone is or my personal status. Like if I'm married, et cetera, I would never put these. (Barbara)

Thus, regarding the type of personal information that participants disclose, there is again homogeneity in the findings; only basic personal information. It is common knowledge that it is essential for users to provide some personal data to create a profile on social media and as a result, participants feel comfortable providing personal data such as name, surname, and e-mail address. However, it is clear from participants' responses that there is a hesitation in sharing personal information like address, phone number, and relationship status.

According to Chen and Rea (2004), people who want to protect their privacy on social media networks are inclined to disclose only essential personal data like name, surname, and e-mail address to be able to create an account and no extra information like phone number, location.

As Anna explains, although Facebook asks her to write about her hobbies, the place that she lives or to put a job description, she believes that there is no reason for revealing her personal information online. But there is one case that participants are willing to provide more than the basic information about themselves. In particular, 4 female participants have agreed to provide personal data such as age, phone number, and address but only for professional reasons. For instance, Angie has no hesitation to disclose her personal information if she receives advantages in return. In fact, recently she found an application that helps young people to find a job nearby.

I provided everything they asked me because if not, you could not proceed to the next step and complete your profile so that you can start searching for jobs nearby...I didn't feel weird or that I shouldn't do it because this was also in order to find a job. So I felt that it would have a benefit for me if I do so. (Angie)

Indeed, the privacy calculus theory refers to the decision-making process that consumers are engaging in order to assess the costs and benefits of a potential self-disclosure practice (Dinev & Hart, 2006). Accordingly, the more hypothesized benefits consumers get in return for a self-disclosure, the more motivated they are to provide their personal data online.

5. Conclusion

The main goal of the current study was to investigate how Greek millennials experience targeted and personalized advertising, on their Facebook and Instagram feeds. What follows is an overview of the main findings of this research, by highlighting how these contribute to existing literature. After discussing the implications of personalized advertising, this study concludes by answering the main research question, addressing the limitations, and providing recommendations for the future.

5.1. Summary of the findings

After coding the transcripts of the 14 in-depth interviews, five themes were representative of the results. These themes show that Greek millennials have specific reactions and perceptions of personalized advertising on social media, which provide an answer to the first sub question of this research. These perceptions were divided into the first theme of “acknowledging the benefits of personalized advertising” and the second of “drawbacks of personalized advertising as perceived by consumers”. More precisely, the two most important findings that were discussed under the first overarching theme were the useful features of personalized advertisements for both consumers and businesses. In accordance with De Keyzer et al. (2015) consumers were pleased when receiving advertisements that were personally relevant and close to their interests. The findings highlight that targeted advertising that is relevant to consumers’ preferences is perceived as not only useful but also helpful for them. Moreover, participants acknowledged the business opportunities that personalized advertising created for them. Personalized advertising was found to be a beneficial tool for companies because it constitutes a good marketing technique to reach new audiences and increase business profit. Another noteworthy finding concerned consumers’ understanding that when they are using services or applications like Facebook for free, these companies track consumer data to make money. This mirrors the findings of McFarlane (2020), who argues that social media companies earn money by selling advertising to other companies.

On the other hand, the second overarching theme analyzes the drawbacks of personalized advertising on social media. It was reported that the two primary purposes of using social media were communication and entertainment. Consequently, social media does not constitute the ideal place for receiving advertisements. This is in line with (Ur et al., 2012) who found that advertising on social media is perceived as disputing and irritating for users. It was also clear that consumer annoyance is linked with the repetition and the irrelevant content

of the advertisement. One more negative feeling was fear. Consumers raised fearful reactions due to online risks such as hacking, fraud, and misuse of personal data. This mirrored the findings of Bleier and Eisenbeiss (2015).

The third theme “consumers’ knowledge of data-tracking practices” refers to consumers’ knowledge about personalized and data-tracking practices. Thus, this theme answers the second sub question, which is about consumers’ perceptions of targeted and personalized advertising practices. Regarding data-tracking practices, interestingly, the majority of the participants were aware of the tracking mechanisms companies use to display personalized advertising. The use of cookies in websites was the most common response. As a result, consumers were not surprised by their personalized advertisements because by accepting cookies they allow marketers to detect their interests. Besides that, it was highlighted that data tracking is a complex practice that many companies try to simplify by hiding parts of it. Concerning the ads’ origins, consumers were knowledgeable that companies track their browsing history, location, and online purchases as Eldering (2001) has pointed out.

This study also discusses the concept of privacy on social media. The fourth theme “consumers’ privacy attitudes” discusses how Greek millennials feel about their online privacy. The knowledge of data-tracking practices led some consumers to hold an apathetic attitude towards personalized advertising. In particular, it was reported that since it is unavoidable for consumers to preserve their personal data private on the Internet, they decide to disclose them. This reflects on the privacy apathy theory as discussed by Xie et al. (2019). Moreover, consumers have compromised with the idea that in free services they constitute the product, and accordingly, they are obliged to provide some personal information. This research also indicated that there are several concerns strongly related to data tracking when receiving personalized advertisements. These concerns were associated with the use of people’s data for non-commercial reasons without having their permission. Strikingly, all participants felt that companies intruded in their lives and monitored them when receiving personalized advertisements based on private conversations. This is a similar position to the argument of Boerman et al. (2017) that advertisers should be careful with the level of personalization because advertising that is too personal is perceived as privacy-invasive.

Those privacy concerns motivated participants to prevent data tracking by utilizing various privacy-preserving practices and tools. Hence, the fifth theme “consumers’ privacy negotiations” mentions the measures they have taken to protect their privacy and prevent data tracking and answers to the third sub question of the study. Unexpectedly, participants have

adopted responsible behavior on the Internet concerning their personal information by setting a limit in self-disclosure. More precisely, they tend to disclose only basic personal information (i.e. name, last name, e-mail), which is essential to create an account on social media. None of them provided extra information about address or relationship status. Hence, consumers choose to manage their personal information and adjust their attitudes towards privacy with the aim to preserve their privacy online. This practice is clearly linked with the CPM theory. According to Petronio (2013), people believe that they are the owners of their personal data and consequently, they are in charge of guarding and managing private information. Additionally, they also tend to decide if the risk of a potential self-disclosure is worthwhile or if they get an advantage in return, which reflects on the privacy calculus theory as described by Bol et al. (2018). Many of the respondents referred to the privacy-preserving practices they use, with the most prevalent being deleting cookies, private navigation, and the least common VPN use.

Overall, by reviewing all these themes together, it is now clear how Greek millennials experience targeted and personalized advertising, on their Facebook and Instagram feeds. So to answer the research question, consumers experience personalized advertising on social media in different ways; with pleasure, annoyance, fear, or even apathy. One important aspect to understand is that the positive perceptions are related to the usefulness of targeted advertising for both consumers and businesses, whereas the negative perceptions are due to the collection and misuse of people's data. Thus, privacy attitudes and privacy-preserving practices go hand in hand with consumers' privacy concerns. As a result, personalized advertising when used with transparency can constitute a powerful tool not only for businesses but also for consumers. Therefore, companies need to use it while respecting consumers' personal data and privacy. In that way, consumers, and personalized advertising may end up having essential value for one another.

5.2. Societal and scientific relevance

The summary above indicates the scientific relevance by emphasizing how this study mirrors, contrasts, and builds on research about targeted advertising, privacy management, and privacy-preserving practices in the context of an understudied sample of Greek millennials. Moreover, the findings of this study also have societal relevance, as there are several important implications. In particular, personalized advertising is considered the future of advertising (Boerman et al., 2017). Hence, the information of this study can be used by companies to develop more consumer-centric advertisements aimed to grant users more

privacy than just business profit. Policymakers can also tighten and systemize the existing privacy regulation. This can be accomplished by obligating companies to offer more transparency about the data-tracking mechanism they use. The effects of the GDPR are undoubtedly positive but the terms of service need to be written in a simple as well as understandable for the consumer language. Also, more focus should be provided on increasing people's awareness about social media as well as data tracking methods. This knowledge gap can be filled by providing high school students education about social media self-disclosure practices and raising their awareness about online risks. Additionally, recent developments like Google's announcement about using no more tracking cookies on its Chrome browser by 2022 (Boiten, 2021) show that the digital environment is constantly and rapidly changing. These developments will have important implications for consumers, marketers, and society. Thus, it is important to keep an eye on these changes, as they may open up a whole new field of research.

5.3. Limitations and future research

The present research has contributed interesting and important insights into consumers' perceptions of personalized advertising. However, as with any research, it is crucial to identify the limitations and report them. To begin with, this study was conducted in a time frame of a few months. In particular, due to the restricted time schedule, the sample of this research was limited as only 14 interviews were conducted with 10 females and 4 males. On the one hand, this is justified by the fact that females tend to spend more time on social media (Greenwood et al., 2016), but on the other hand, it can also be considered a limitation because it is out of balance. Thus, a larger sample size and equally divided between the sexes could provide a more range of valuable opinions to help inform the research's outcome. Due to the purposive sampling method, this sample size cannot be representative of the overall Greek millennial population because the researcher used her own judgment for choosing the sample (Etikan et al., 2016). The generalization of the population is impossible because the sample was based on certain criteria and not randomly. Besides, in qualitative research, generalizability is not the prime goal because the phenomenon must be studied in-depth (Ghaljaie et al., 2017).

Notwithstanding the relatively limited sample, this work offers valuable insights into Greek millennials' perceptions and knowledge of personalized advertising, as well as into the privacy-preserving tools and practices they use. Of course, there are cultural differences among counties and the educational level may vary from generation to generation. The

inclusion of different age groups may have enriched the data as younger people with varied backgrounds might have less knowledge of data tracking practices and different reactions to personalized advertising. Hence, the findings refer only to Greek millennial perceptions of personalized advertising and generalization of the population is also not possible.

Consequently, the aforementioned restricted sample size constitutes a great opportunity for future research. More precisely, a future study can investigate a younger group age and most specifically teenagers. It was reported that during puberty most participants created their Facebook profiles. So it would be interesting to ask that age group what kind of data they disclose. Since several questions still remain to be answered about self-disclosure, further work needs to be done to better establish under which circumstances and what type of data people provide when creating their social media. Furthermore, it was clear from the findings that millennials have a more mature mindset and responsible online behavior now than in the past. This is due to their current knowledge and their own experiences of data tracking practices. Hence, teenagers that tend to be reckless and have a different educational level than millennials will probably react differently to personalized advertising.

References

- Abu-Salma, R., & Livshits, B. (2020). Evaluating the end-user experience of private browsing mode. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-12. <https://doi-org.eur.idm.oclc.org/10.1145/3313831.3376440>
- Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). An analysis of private browsing modes in modern browsers. *USENIX Security'10: Proceedings of the 19th USENIX conference on Security*, 79-94. <https://elie.net/static/files/an-analysis-of-private-browsing-modes-in-modern-browsers/an-analysis-of-private-browsing-modes-in-modern-browsers-slides.pdf>
- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49. <http://doi.org/10.1016/J.JRETAI.2014.09.005>
- An, M. (2016, July 13). Why people block ads. *Hubspot Research*. <https://blog.hubspot.com/marketing/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers>
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 30(1), 13-28. <https://dl-acm-org.eur.idm.oclc.org/doi/10.5555/2017284.2017287>
- Barnham, C. (2015). Quantitative and qualitative research: perceptual foundations. *International Journal of Market Research*, 57(6), 837–854. <https://doi-org.eur.idm.oclc.org/10.2501/IJMR-2015-070>
- Becker, H. S., & Geer, B. (1957). Participant observation and interviewing: a comparison. *Human Organization*, 16(3), 28–32. <https://doi-org.eur.idm.oclc.org/10.17730/humo.16.3.k687822132323013>
- Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3), 390–409. <http://doi.org/10.1016/j.jretai.2015.04.001>
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Blocking ads and deleting cookies: a longitudinal study examining online privacy protection behavior. *The Proceedings of the 2018 Conference of the American Academy of Advertising*, 85-86.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral

- advertising: a literature review and research agenda. *Journal of Advertising*, 46(3), 363-376. <http://doi.org/10.1080/00913367.2017.1339368>
- Boiten, E. (2021, March 8). Google's scrapping third-party cookies – but invasive targeted advertising will live on. *The Conversation*. <https://theconversation.com/googles-scrapping-third-party-cookies-but-invasive-targeted-advertising-will-live-on-156530>
- Bol, N., Dienlin, T., Kruike-meier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, 23(6), 370–388. <https://doi-org.eur.idm.oclc.org/10.1093/jcmc/zmy020>
- Boyd, D., & Marwick, A. E. (2011). Social privacy in networked publics: teens' attitudes, practices, and strategies. *A decade in internet time: Symposium on the dynamics of the internet and society*. <http://ssrn.com/abstract=1925128>
- Brake, D. R. (2014). *Sharing our lives online: risks and exposure in social media*. Palgrave Macmillan.
- Büchi M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of internet skills for online privacy protection. *Information, Communication & Society*, 20(8), 1261–1278. <https://doi-org.eur.idm.oclc.org/10.1080/1369118X.2016.1229001>
- Carr, C. T., & Hayes, R. A. (2015). Social media: defining, developing, and divining. *Atlantic Journal of Communication*, 23(1), 46–65. <https://doi-org.eur.idm.oclc.org/10.1080/15456870.2015.972282>
- Chen, J. (2021, February 3). 36 essential social media marketing statistics to know for 2021. *Sprout Social*. <https://sproutsocial.com/insights/social-media-statistics/>
- Chen, K., & Rea, A. I. (2004). Protecting personal information online: a survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems*, 44(4), 85–92. <https://www-proquest-com.eur.idm.oclc.org/docview/232578985>
- Clarke, V., & Braun, V. (2017). Thematic analysis. *Journal of Positive Psychology*, 12(3), 297–298. <https://doi-org.eur.idm.oclc.org/10.1080/17439760.2016.1262613>
- Darmody, A., & Zwick, D. (2020). Manipulate to empower: hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society*, 7(1), 1-12. <https://doi-org.eur.idm.oclc.org/10.1177/2053951720904112>
- De Keyzer, F., Dens, N., & De Pelsmacker, P. (2015). Is this for me? How consumers respond to personalized advertising on social network sites. *Journal of Interactive Advertising*, 15(2), 124-134. <https://doi.org/10.1080/15252019.2015.1082450>

- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. <https://doi-org.eur.idm.oclc.org/10.1111/j.1083-6101.2009.01494.x>
- Denzin, N. K. (1978). *The research act: a theoretical introduction to sociological methods* (2nd ed.). McGraw-Hill.
- DeVaney, S. A. (2015). Understanding the millennial generation. *Journal of Financial Service Professionals*, *69*(6), 11–14. <https://web-b-ebSCOhost-com.eur.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=1&sid=ddbc3f73-ec22-45a6-9b30-d7351c8c396c%40sessionmgr103>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. <https://doi-org.eur.idm.oclc.org/10.1287/isre.1060.0080>
- DuckDuckGo. (2017, January 27). A study on private browsing: consumer usage, knowledge, and thoughts. *Spread privacy*. <https://spreadprivacy.com/is-private-browsing-really-private/>
- Durham, W. T. (2008). The rules-based process of revealing/concealing the family planning decisions of voluntarily child-free couples: a communication privacy management perspective. *Communication Studies*, *59*(2), 132–147. <https://doi-org.eur.idm.oclc.org/10.1080/10510970802062451>
- Eldering, C. A. (2001). Consumer profiling system. *U.S. Patent No. 6,298,348*. Washington, DC: U.S. Patent and Trademark Office.
<https://patentimages.storage.googleapis.com/13/30/c9/68897fff2eafc4/US6298348.pdf>
- Esterberg, K. G. (2002). *Qualitative methods in social research*. McGraw-Hill.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Evans, D. S. (2009). The online advertising industry: economics, evolution, and privacy. *Journal of Economic Perspectives*, *23*(3), 37–60. <https://doi-org.eur.idm.oclc.org/10.1257/jep.23.3.37>
- Flick, U. (2018). *Doing triangulation and mixed methods*. SAGE Publications.
- Foddy, W. H. (1993). *Constructing questions for interviews and questionnaires: theory and practice in social research*. Cambridge University Press.
- Fowler, B. (2019, July 10). Is your smartphone secretly listening to you? *Consumer Reports*.

- <https://www.consumerreports.org/smartphones/is-your-smartphone-secretly-listening-to-you/>
- Ghaljaie, F., Naderifar, M., & Goli, H. (2017). Snowball sampling: a purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, 14(3), 1-4. <https://doi-org.eur.idm.oclc.org/10.5812/sdme.67670>
- Glaser, B. G. (1978). *Theoretical sensitivity: advances in the methodology of grounded theory*. Sociology Press.
- Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. *Pew Research Center*, 11(2), 1-18. <http://downtowndubuque.org/wp-content/uploads/2017/01/Social-Media-Update-2016.pdf>
- Gruber, T., Szmigin, I., Reppel, A. E., & Voss, R. (2008). Designing and conducting online interviews to investigate interesting consumer phenomena. *Qualitative Market Research: An International Journal*, 11(3), 256–274. <https://doi-org.eur.idm.oclc.org/10.1108/13522750810879002>
- Hannabuss, S. (1996). Research interviews. *New library world*.
- Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10(21), 3737–3757. <https://ijoc.org/index.php/ijoc/article/view/4655/1738>
- Hoffman, C. (2017, July 5). How private browsing works, and why it doesn’t offer complete privacy. *How-to geek*. <https://www.howtogeek.com/117776/htg-explains-how-private-browsing-works-and-why-it-doesnt-offer-complete-privacy/>
- Hoffman, C. (2020, October 15). What is a VPN, and why would I need one? *How-to geek*. <https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/>
- Iabuk. (2012, July 18). *How online behavioural advertising works* [Video]. YouTube. <https://www.youtube.com/watch?v=Y9Y4Efyxmk4&t=8s>
- Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: the new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health & Well-Being*, 9(1), 1–3. <https://doi-org.eur.idm.oclc.org/10.3402/qhw.v9.24152>
- Johnson, D. (2021, April 6). A guide to internet cookies, the small files that store information about your online activity. *Business Insider*. <https://www.businessinsider.com/what-are-cookies>
- Johnson, J. M. (2011). In-depth interviewing. In Jaber F. Gubrium & James A. Holstein (Eds.), *Handbook of Interview Research* (pp. 103-119). SAGE Publications.

<https://doi.org/10.4135/9781412973588>

- Kendall, J. (1999). Axial coding and the grounded theory controversy. *Western Journal of Nursing Research*, 21(6), 743–757. <https://doi-org.eur.idm.oclc.org/10.1177/019394599902100603>
- Kolowich-Cox, K. (2015, October 1). How ad blocking works: everything you need to know. *Hubspot Research*. <https://blog.hubspot.com/marketing/how-ad-blocking-works>
- König, R., Uphues, S., Vogt, V., & Kolany-Raiser, B. (2020). The tracked society: interdisciplinary approaches on online tracking. *New Media & Society*, 22(11), 1945–1956. <https://doi.org/10.1177/1461444820924629>
- Kshetri, N., & DeFranco, J. F. (2020). Is privacy dead? *IT Professional*, 22(5), 4–12. <https://doi.org/10.1109/mitp.2020.2992148>
- Kumar, V., & Gupta, S. (2016). Conceptualizing the evolution and future of advertising. *Journal of Advertising*, 45(3), 302–317. <https://doi-org.eur.idm.oclc.org/10.1080/00913367.2016.1199335>
- Kvale, S. (1983). The qualitative research interview: a phenomenological and a hermeneutical mode of understanding. *Journal of Phenomenological Psychology*, 14(2), 171–196. <https://doi.org/10.1163/156916283X00090>
- LaRossa, R. (2005). Grounded theory methods and qualitative family research. *Journal of Marriage and Family*, 67(4), 837–857. <https://doi-org.eur.idm.oclc.org/10.1111/j.1741-3737.2005.00179.x>
- Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. (2012). Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 589–598. <https://doi-org.eur.idm.oclc.org/10.1145/2207676.2207759>
- Lyon, D. (2007). *Surveillance studies: an overview*. Polity.
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 540–565. https://kb.osu.edu/bitstream/handle/1811/72839/1/ISJLP_V4N3_543.pdf
- McFarlane, G. (2020, February 7). How Facebook, Twitter, social media make money from you. *Investopedia*. <https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx>
- Mills, J., Bonner, A., & Francis, K. (2006). The development of constructivist grounded theory. *International Journal of Qualitative Methods*, 5(1), 25–35. <https://doi-org.eur.idm.oclc.org/10.1177/160940690600500103>

- Mohsin, M. (2020, August 6). 10 social media statistics you need to know in 2021 [infographic]. *Oberlo*. <https://www.oberlo.com/blog/social-media-marketing-statistics>
- Moisander, J., & Valtonen, A. (2006). *Qualitative marketing research: A cultural approach*. Sage Publications.
- Møller, K., & Robards, B. (2019). Walking through, going along and scrolling back, *Nordicom Review*, 40(1), 95-109. <https://doi.org/10.2478/nor-2019-0016>
- Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, 18(2), 34–5. <https://doi-org.eur.idm.oclc.org/10.1136/eb-2015-102054>
- Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), 128–147. <https://doi.org/10.2139/ssrn.2757465>
- O'Donnell, K., & Cramer, H. (2015). People's perceptions of personalized ads. *Proceedings of the 24th International Conference on World Wide Web*, 1293-1298. <https://doi-org.eur.idm.oclc.org/10.1145/2740908.2742003>
- Oliver, P. (2010). *The student's guide to research ethics*. McGraw-Hill Education.
- Papafotikas, I., Chatzoudes, D., & Kamenidou, I. (2014). Purchase decisions of Greek consumers: an empirical study. *Procedia Economics and Finance* 9, 456–465. [https://doi.org/10.1016/S2212-5671\(14\)00047-1](https://doi.org/10.1016/S2212-5671(14)00047-1)
- Petronio, S. (2010). Communication privacy management theory: what do we know about family privacy regulation? *Journal of Family Theory & Review*, 2(3), 175–196. <https://doi-org.eur.idm.oclc.org/10.1111/j.1756-2589.2010.00052.x>
- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13(1), 6-14. <https://doi.org/10.1080/15267431.2013.743426>
- Pickard-Whitehead, G. (2020, February 6). Millennials still using Facebook more than any other social media site. *Small Business News*. <https://smallbiztrends.com/2020/02/2020-consumer-culture-report.html>
- Pridmore, J., & Lyon, D. (2011). Marketing as surveillance: assembling consumers as brands. In D. Zwick & J. Cayla (Eds.), *Inside marketing: Practices, ideologies, devices* (pp. 115-36). Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199576746.003.0006>
- Pridmore, J., & Zwick, D. (2011). Marketing and the rise of commercial consumer surveillance. *Surveillance & Society*, 8(3), 269–277. <https://doi->

org.eur.idm.oclc.org/10.24908/ss.v8i3.4163

- Pujol, E., Hohlfeld, O., & Feldmann, A. (2015). Annoyed users: ads and ad-block usage in the wild. *Proceedings of the 2015 Internet Measurement Conference*, 93-106. <https://doi-org.eur.idm.oclc.org/10.1145/2815675.2815705>
- Redmond, E. C., & Griffith, C. J. (2006). A pilot study to evaluate the effectiveness of a social marketing-based consumer food safety initiative using observation. *British Food Journal*, 108(9), 753–770. <https://doi-org.eur.idm.oclc.org/10.1108/00070700610688386>
- Ruckenstein, M., & Granroth J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, 13(1), 12-24. <https://doi.org/10.1080/17530350.2019.1574866>
- Scott, C., Klein, D. M., & Bryant, J. (1990). Consumer response to humor in advertising: a series of field studies using behavioral observation. *Journal of consumer research*, 16(4), 498-501. <https://www.jstor.org/stable/2489461>
- Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, 13(5), 305–319. <https://doi-org.eur.idm.oclc.org/10.1016/j.elerap.2014.06.007>
- Silverman, D. (2011). *Interpreting qualitative data. A guide to the principles of qualitative research (4th edition)*. Sage Publications
- Smit, B. (2002). Atlas.ti for qualitative data analysis. *Perspectives in education*, 20(3), 65-75. <https://journals.co.za/doi/10.10520/EJC87147>
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York University Press.
- Steinfeld, N. (2016). “I agree to the terms and conditions”: (How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior*, 55, 992-1000. <https://doi-org.eur.idm.oclc.org/10.1016/j.chb.2015.09.038>
- Strauss, A. L., & Corbin, J. M. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Sage Publications.
- Tabora, V. (2019, November 1). In big data, the consumer is the product. *The Startup*. <https://medium.com/swlh/in-big-data-the-consumer-is-the-product-ad9bf0423d9a>
- Tam, K. Y., & Ho, S. Y. (2006). Understanding the impact of web personalization on user information processing and decision outcomes. *Mis Quarterly*, 30(4), 865–890. <https://doi-org.eur.idm.oclc.org/10.2307/25148757>

- Tankovska, H. (2021, April 8). Facebook users in Greece from September 2018 to March 2021. *Statista*. <https://www.statista.com/statistics/1029764/facebook-users-greece/>
- Tarran, B. (2018). What can we learn from the Facebook—Cambridge Analytica scandal? *Significance*, *15*(3), 4-5. <https://doi.org/10.1111/j.1740-9713.2018.01139.x>
- Technology Services at Illinois. (2016, March 31). *Social media data privacy awareness* [Video]. YouTube. <https://www.youtube.com/watch?v=UhhYSrUHnao>
- Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: getting to know one another a bit at a time. *Human Communication Research*, *28*(3), 317–348. <https://doi-org.eur.idm.oclc.org/10.1111/j.1468-2958.2002.tb00811.x>
- Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, *51*(5), 546–562. <https://doi-org.eur.idm.oclc.org/10.1509/jmr.10.0355>
- Tutaj, K., & Van Reijmersdal, E. A. (2012). Effects of online advertising format and persuasion knowledge on audience reactions. *Journal of Marketing Communications*, *18*(1), 5-18. <https://doi-org.eur.idm.oclc.org/10.1080/13527266.2011.620765>
- Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: perceptions of online behavioral advertising. *Proceedings of the eighth symposium on usable privacy and security*, 1-15. <https://doi-org.eur.idm.oclc.org/10.1145/2335356.2335362>
- van der Velden, M., & El Emam, K. (2013). "Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media. *Journal of the American Medical Informatics Association*, *20*(1), 16–24. <https://doi-org.eur.idm.oclc.org/10.1136/amiajnl-2012-000949>
- Vranica, S. (2019, June 18). Advertising (a special report) --- How privacy rules will affect the ad Business: we asked major players from across the industry about the impact of the new regulations. Here are their predictions. *Wall Street Journal*. <https://search-proquest-com.eur.idm.oclc.org/docview/2241888488>
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Wiles, R., Crow, G., Heath, S., & Charles, V. (2008). The management of confidentiality and anonymity in social research. *International Journal of Social Research Methodology*, *11*(5), 417–428. <https://doi-org.eur.idm.oclc.org/10.1080/13645570701622231>

- Wills, C. E., & Uzunoglu, D. C. (2016). What ad blockers are (and are not) doing. *2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 72-77. <https://doi-org.eur.idm.oclc.org/10.1109/HotWeb.2016.21>
- Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, 38(7), 742–759. <https://doi-org.eur.idm.oclc.org/10.1080/0144929X.2018.1552717>
- Yoo, C. W., Ahn, H. J., & Rao, H. R. (2012). An exploration of the impact of information privacy invasion. *Proceeding of Thirty Third International Conference on Information Systems, Florida*, 1–18. <https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/2/>
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: the internet privacy paradox revisited. *Information Communication and Society*, 16(4), 479–500. <https://doi-org.eur.idm.oclc.org/10.1080/1369118X.2013.777757>
- Ziegeldorf, J. H., Wehrle, K., & Morchon, O. G. (2014). Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742. <https://doi-org.eur.idm.oclc.org/10.1002/sec.795>
- Zwick, D., & Cayla, J. (2011). *Inside marketing: practices, ideologies, devices*. Oxford University Press.

Appendix A - Interview guide

Social media

- Can you tell me a little bit about yourself?
- Can you also tell me more about your work experience?
- Which social media platform do you use the most on your daily basis and which one do you prefer the most? Why?
- How do you use social media in your daily life? Can you give me some examples?
- From which device do you usually log in to your social media accounts?
- Can you think of a recent situation where you provided your personal data on a platform? What kind of data was it?

Personalized advertising

- Can you please log in to your favorite online social platform? If you feel comfortable you can share your screen with me. When you scroll down on your account apart from posts of your connections, can you tell me what else do you see? Do you notice advertisements? What kind of ads are they? Can you give me some examples?
- Can you please describe to me a personal experience when you searched for a product or a service and afterwards you saw a banner of that product on your social media platform? Does that happen often to you?
- How do you feel when you see targeted ads and banners on your social media platforms? Could you provide an example of a time that you found an ad helpful and one that you found an ad annoying?
- What are your views on the ethical aspect of online advertising? According to your perspective when an advertisement can be intrusive?
- Can you please describe to me how companies may use your data to display personalized ads?
- Video explaining online behavioral advertising
- How do you feel after seeing that video? Were there any gaps in your knowledge?

Privacy and privacy-preserving practices

- How do you feel when you provide your data to companies? What about your privacy?
- How do you feel about your privacy on the Internet/social media?
- Have you ever changed your behavior due to online advertising? How and why?
- How do you protect your privacy on the Internet/ social media?

- Have you ever tried to delete cookies or to install ad block software? Why do you think these practices are effective to protect your privacy?
- Can you please now visit a website when you usually read news articles? Did you notice the banner with the terms of policy? Do you usually read them? Why or why not?
- Why do you think it is important / or not important to read those terms in order to protect our private and personal data?
- How do you feel that companies make profiles of customers?

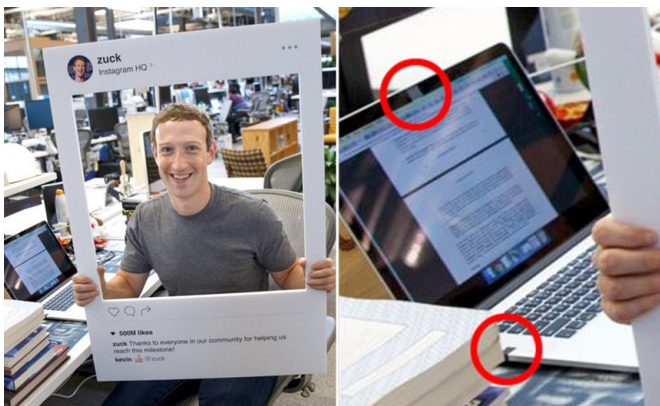
Videos

How online behavioral advertising works

<https://www.youtube.com/watch?v=Y9Y4Efyxmk4&t=8s>

Social media data privacy awareness <https://www.youtube.com/watch?v=UhhYSrUHnao>

Pictures



Your phone when you say you want to buy something



Appendix B - Coding scheme

| Selective code | Axial code | Open code |
|--|--|---|
| Acknowledging the benefits of personalized advertising | Useful features of personalized advertisements | ads with free services are beneficial |
| | | ads with informative content are helpful |
| | | useful; ads based on consumer's interest |
| | | helpful; no need for searching |
| | Good marketing technique | interesting suggestions when in need |
| | | good for small businesses |
| | | fast way to shop; there is a link to click |
| | | good way to reach an audience |
| | Pay for the free content | support to media creators |
| | | the creators must get paid |
| | | companies make money |
| | | pay for free usage |
| | Drawbacks of personalized advertising | Advertisements are annoying |
| people can search on their own | | |
| time-consuming | | |
| social media is not suitable for advertising | | |
| algorithms can fail | | |
| unnecessary on social media | | |
| Conditions that advertisements can be annoying | | constant ads |
| | | ad for something people have already bought |
| | | ads based on personality traits |
| | | ads on Instagram stories |
| | | ads while listening to music and |

| | | |
|---|--|--|
| | | watching videos |
| | | ads with insulting/unethical content |
| | | when people cannot skip them |
| | | content against people's beliefs |
| | | getting irrelevant ads |
| | | getting the same ads |
| | | getting the same ad on different social media |
| | | political ads |
| | Consumers' fearful reactions to personalized advertising | afraid to click because of viruses |
| | | afraid of hacking data |
| | | misuse of personal data |
| | | fear of being exposed |
| | | scary; knowing people's personality traits |
| | | threatened by knowing everything about people |
| | | fear that companies have access in people's life |
| Consumers' knowledge of data-tracking practices | Understanding of consumer surveillance | big companies sell people's data to companies |
| | | by accepting cookies companies track consumers |
| | | by self-disclosure companies collect data |
| | | companies collect data from searching machines |
| | | companies already have people's data |
| | | companies know everything about consumers |

| | | |
|---|---|--|
| | | companies pay social media to have people's data |
| | | companies collect also user's personal information |
| | | companies use people to make a profit |
| | | companies track people's clicks |
| | | cookies have access to people's p.i. |
| | | cookies track people's data |
| | | p.a. is a complicated practice |
| | | people provide their interests via searching |
| | Consumers' assumptions of ads' origins | ad based on consumer's clicks |
| | | ad based on consumer's similar interests |
| | | ads based on user's browsing history |
| | | ads based on consumer's downloaded apps |
| | | ads based on consumer's behavior |
| | | ads based on consumer's gender |
| Privacy attitudes | Apathetic responses of personalized advertising | ads based on consumer's interest |
| | | ads based on consumer's location |
| | | ads based on consumer's traits |
| | | ads based on previous purchases |
| | | ad based on a phone conversation |
| | | compromised with the practice |
| people have already exposed their data | | |
| does not care about people accessing his data | | |

| | | |
|--|-----------------------------|--|
| | | no concerns; just an individual |
| | | everyone has access to people's data |
| | | sooner or later companies gain all data |
| | | that is the way advertising works |
| | | takes surveillance as a joke |
| | | nothing private on social media |
| | | no privacy online |
| | | knowledge leads to apathy |
| | | Google knows everything about us |
| | | inevitable to remain private |
| | | tos are hard to understand |
| | | accepting tos without reading |
| | Consumers' privacy concerns | concern about companies knowing everything about people |
| | | concerns about companies using people's data |
| | | concerns about credit card |
| | | worried about speaking and getting an ad |
| | | concerned; without consent social media collect data |
| | | worried that companies sell people's data |
| | | worried that companies monitor people |
| | | concerned about companies having access in people's life |
| | | concerns when self-disclosing |
| | | companies intrude in people's lives |

| | | |
|---|--|---|
| Consumers' privacy negotiations | Privacy-preserving practices | accepting only necessary cookies |
| | | not accepting cookies |
| | | covering the mobile camera |
| | | checking websites before visiting and disclosing |
| | | using encryption apps |
| | | using fingerprints to enter e-banking |
| | | using TOR |
| | | using VPN |
| | | changing passwords frequently |
| | | setting strong passwords |
| | | deleting cookies and browsing history |
| | | exiting the website because of cookies |
| | | incognito mode for hiding identity |
| | | incognito mode for hiding preferences |
| | | no privacy-preserving practices due to basic technical skills |
| | be more careful with p.i. on the Internet | |
| | never save p.i. online | |
| | Self-disclosure strategies on social media | deciding what kind of data providing |
| | | using Facebook's privacy settings |
| | | private account |
| self-disclosure when there is a benefit | | |
| self-disclosure for professional | | |

| | | |
|--|--|---|
| | | reasons |
| | | self-disclosure only on friends/close people |
| | | thinking before posting |
| | | being responsible with p.i. |
| | | set a limit when disclosing |
| | | read tos before self-disclosure |
| | | providing only essential information to create an account |
| | | not posting herself |
| | | providing basic information |
| | | not providing new information |
| | | not providing personal information |
| | | not posting on social media |
| | | searching before disclosing |

Appendix C - Operationalization

| Sub questions | Information I need to collect | Example of question asked |
|---|--|--|
| 1) What are Greek millennials' reactions when using Facebook and Instagram? | Importance of social media in people's life | How do you use social media in your daily life? |
| | Which platform is the most popular and most used | Which social media platform do you use most on your daily basis |
| | Which device they use to log in | From which device do you usually log in to your social media accounts? |
| | What kind of data users disclose on social media | Can you think of a recent situation where you provided your personal data on a platform? What kind of data was it? |
| 2) How do Greek millennials perceive targeted and personalized advertising practices? | Feelings to personalized advertising | How do you feel when you see targeted ads and banners on your social media platforms? |
| | Reactions to personalized advertising | Could you provide an example of a time that you found an ad helpful and one that you found an ad annoying? |
| | Personal experiences to personalized advertising | Can you please describe to me some personalized advertisements on your feed? |
| | Under which circumstances personalized advertising is disturbing | According to your perspective when an advertisement can be intrusive? |
| | Users' knowledge of data-tracking practices | Can you please describe to me how companies may use your data to display personalized ads? |
| | Reactions to profiling | How do you feel that companies make profiles of customers? |
| 3) What, if any, measures have | Feelings about privacy on the Internet/social media | How do you feel about your privacy on the Internet/social |

| | | |
|--|---|---|
| Greek millennials taken to protect their privacy, and reduce or prevent data tracking? | | media? |
| | Feelings about disclosing personal information on the Internet/social media | How do you feel when you provide your data to companies? What about your privacy? |
| | Privacy-preserving practices | Have you ever changed your behavior due to online advertising? How and why? |
| | Privacy-preserving tools | How do you protect your privacy on the Internet/ social media? |
| | Effective or not effective | Why do you think these practices are effective to protect your privacy? |
| | Read or not terms of service | Can you please now visit a website when you usually read news articles? Did you notice the banner with the terms of policy? |
| | Important or not reading terms of service | Why do you think it is important / or not important to read those terms in order to protect our private and personal data? |

Appendix D - Consent form

CONSENT REQUEST FOR PARTICIPATING IN RESEARCH

FOR QUESTIONS ABOUT THE STUDY, CONTACT:

Kelly Tsatsarou

k.tsatsarou@gmail.com

DESCRIPTION

You are invited to participate in a research about targeted and personalized advertising that can be found on Facebook and Instagram. The purpose of the study is to understand how Greek young adults interpret and react to targeted and personalized advertising that they find on their Facebook and Instagram feeds.

Your acceptance to participate in this study means that you accept to be interviewed

In general terms,

The questions of the interview will be related to targeted and personalized advertising. Unless you prefer that no recordings are made, I will use a tape / video recorder for the interview.

You are always free not to answer any particular question, and/or stop participating at any point.

Every time I want to accompany you in any activity I will ask you your permission again.

RISKS AND BENEFITS

A. As far as I can tell, there are no risks associated with participating in this research. I will make sure that you cannot be identified as I will always use pseudonyms and I will not present identifiable information in the study, but only mentioning your general information (i.e. age and gender).

B. I am aware that the possibility of identifying the people who participate in this study may involve risks. For that reason I will not keep any information that may lead to the identification of those involved in the study. I will always only use pseudonyms to identify participants.

I will use the material from the interviews and my observation exclusively for academic work, such as further research, academic meetings and publications.

TIME INVOLVEMENT

Your participation in this study will take 45-60 minutes. You may interrupt your participation at any time.

PAYMENTS

There will be no monetary compensation for your participation.

PARTICIPANTS' RIGHTS

Appendix E - Overview of participants

| Participants | Gender | Age | Occupation | Pseudo name |
|----------------|--------|-----|---------------------|-------------|
| Participant 1 | Female | 23 | Bachelor student | Anna |
| Participant 2 | Male | 23 | Computer engineer | Chris |
| Participant 3 | Male | 25 | Master's student | John |
| Participant 4 | Male | 25 | Master's student | George |
| Participant 5 | Female | 24 | Internship | Demy |
| Participant 6 | Female | 23 | Internship | Maria |
| Participant 7 | Female | 23 | University graduate | Kate |
| Participant 8 | Female | 24 | Master's student | Angie |
| Participant 9 | Female | 26 | Master's student | Elena |
| Participant 10 | Female | 24 | University graduate | Nikie |
| Participant 11 | Female | 24 | Bachelor student | Julia |
| Participant 12 | Male | 22 | Bachelor student | Pavlos |
| Participant 13 | Female | 23 | Bachelor student | Zoe |
| Participant 14 | Female | 25 | HR assistant | Barbara |