Surveillance? The influence of information asymmetry on consumers' perceptions of online personalization

Thesis for Two year Master, 30 ECTS
Textile Management

Elisa Toivonen

2019.5.09

THE SWEDISH SCHOOL
OF TEXTILES
UNIVERSITY OF BORÅS

Title: Surveillance? The influence of information asymmetry on consumers' perceptions of online personalization

Publication year: 2019

Author: Elisa Toivonen

Supervisor: Vijay Kumar

Abstract

Data collection and online personalization has become essential part of modern marketing, and thus, embedded into consumer's everyday life. This has emerged a lot of negative attention in the media and privacy concerns among consumers – however, their attitudes towards privacy seems to be controversial with lack of privacy enhancing behavior.

The purpose of this study was to find out what is consumers take on online personalization, data collection and GDPR. In order to the tackle the causing reasons of such perceptions, focus group discussions were performed. The emerging thoughts were analyzed with the concepts of privacy paradox and information asymmetry – how structural imbalance between the advertisement network, companies and consumers impacted to their thinking about personalization and which factors caused the unwillingness to enhance one's privacy, despite the attitudes that would predict different behavior.

The results showed, that many respondents do not mind personalization if they perceive it relevant. However, the intrusive nature of its practices made the participants, directly or indirectly, reluctant towards it, as it was highlighted that it is not personalization per se that made the respondents uncomfortable, but how it was done. Due to the advertisement networks' opaque nature, the participants founded challenging to comprehend how personalization was performed. Thus, conspiracy theories about surveillance, such as tapping via smartphone, were broad up to explain companies' ability to know and target them so well.

The main channel for companies to inform consumers about their privacy policy is terms and conditions. However, due to several reasons, the decision making for one's privacy face many hinders, that may influence in how consumers perceive their privacy and how their personal data is collected and used. A controversiality between GDPR's, companies' and consumers' view on privacy self-management is evident, as the regulation and companies rely too much on consumer's own responsibility.

Keywords: GDPR, online personalization, data collection, consumers, information asymmetry, privacy paradox

Table of content

1. Introduction

1.1. Background

Chen (2018) argue, that online fashion retailers are increasingly interested in developing a technology that carries the collection of customer's offline movements, an analysis of their online browsing behavior, product display interaction, as well as AI-performed and personalized marketing campaigns – it has become almost more essential for them to have an access to right technology rather than hiring talented designers. Additionally, H&M has recently employed one of the main character of Cambridge Analytica scandal, Christopher Wylie, to help them to implement big data and artificial intelligence in order to become more profitable and face consumer demand (Molin and Magnusson 2019).

As the value of e-commerce apparel sales was reported to be in the United States 68 billion dollars in 2016 and estimated to hit 200 billion by 2020, the online fashion retail market has continued its growth due to increased number of firms entering the market and changing consumer buying habits (Morisada, Miwa and Dahana 2019). Fashion industry and researchers has continued to find out new opportunities for e-commerce and the use of data, such as the effectiveness of popularity clues for evaluating products or brands at the pre-purchase stage (Yu, Hudders and Cauberghe 2018), personal data usage for mass customization services and products regarding of fit (Ashdown and Loker 2010), recommendation system for online fashion retailer using offline and online data (Hwangbo, Kim and Cha 2018) and valuable customer segment identification in online fashion markets (Morisada et al. 2019). BoF and McKinsey & Company (2018) argue, that products customization, curated recommendations, individualized communications and storytelling are the main channels through which personalization is currently implemented within the fashion industry.

As consumers spend more and more time with their devices and in different digital environments, it is key for marketers to be there where their customers are. According to Stevenson (2016), most individuals in the U.S. include using internet-connected products and services in their daily lives, such as smartphones and social media. Especially in the competitive online environments, due to the rapid development of available data and technology, companies have been embracing new possibilities for more sophisticated and personalized marketing practices. Compared to previous offline marketing efforts, consumers can now be easily profiled and targeted based on their browsing history, personal information and location (Nurse and Buckley 2017).

As Big Data, the Internet of Things and Cloud Computing have emerged as new innovative technologies in parallel to business models that are depended on data, personal information has been argued to become, likewise once oil was, the new raw material for the Information Age and economy (Burri and Schär 2016). There is a increasing demand for customer's online interactions data, such as search behavior, online reviews and social media activity, that produces valuable individual-level information for online firms (Kannan and Li 2017). Accessing to massive click-through data that eventually becomes digital traces of behavior,

marketers have now the ability to know detailed information about consumers's hope, beliefs and desires (Cinnamon 2017) – this massive database of needs and wants can then be archived, traced and utilized for different purposes (Gilteman 2013, p. 123). Stevenson (2016) argues, that personal data fuels the majority of the commercial web, such as search engines, social media, social networking sites, digital publishing, and content distribution, and it is highly dependent on the monitoring and monetization of human behavior. In addition, extra value can be created when online data is corresponded with offline, which enables more detailed consumer profiling (ibid.) In 2018, big data and business analytics was expected to generate 166 billion U.S. dollars worldwide and the global big data industry is estimated to reach value of 103 billion U.S. dollars in 2027 (Statista 2018). 96% of marketers acknowledge the essence of MarTech, consumer centric and technology driven business strategy, for reaching company's marketing objectives (DMA 2019). The difference is, whether you are targeting someone based on very general information or users with detailed data; an 18-35-year-old female who lives in Dallas, or an 37-year-old female who lives in Dallas, is married with 2 children, is loyal to Starbucks and loves The History Channel (Lineup 2019)?

However, this power of getting personal hasn't come without consequences. Nurse and Buckley (2017) argue, that in parallel to companies eagerness to pursue more novel ways for gathering information from consumers and utilizing that for optimal use, such as sophisticated digital marketing, user profiling and click-through data based behavioral targeting, a criticism towards these practices has emerged. Additionally, business models that monetize consumers' data have gained attention too, and some authorities have forced big corporations, such as Facebook, to take responsibility for exploiting their users' privacy for gaining profit (Koistinen 2019). The textiles field is also taking part of the consumer data utilization for new technologies, such as blockchain in luxury goods (O'Connor 2019), personalization services regarding of style (Stitch Fix 2019), size fit (Fitizzy 2019), and conversational commerce in which brand approach consumers through Facebook and Instagram DM's (Lieber 2019B). Thus, questions about privacy and consumers willingness to disclose data as an exchange for services are becoming more relevant in fashion industry too.

Moreover, recently the emphasis has been more in the negative consequences of such personalization practices, specifically in the technology that marketers now have an access to (Koistinen 2019). Using personal data and segmentation are noting new in marketing (Zwick and Dholakia 2004), however, data aggregation, data mining, segmenting, profiling, and behavioral marketing have not just made companies competitive in online environments, but potentially possess a threat of harming consumers. Concerns about information and power asymmetry (Nissenbaum 2010), surveillance capitalism (Cinnamon 2017), market manipulation (Calo 2014), discrimination (Barocas 2014), and further the influence of profiling to consumer's identity (Richards and King 2013) have been raised by researchers. Consumers themselves seem to have conflicting attitudes towards personalization; they are seemingly interested in receiving relevant and personalized content, but do not feel comfortable with disclosing too much of information (Gironda and Korgaonkar 2018). Mixed attitudes follow consumers thoughts regarding of privacy too, as previous research has emphasized, that although consumers do express concerns towards their privacy, their behavior do not follow accordingly with privacy enhancing activity (Kokolakis 2017).

Since information and its flow across the borders plays major role in today's modern economy, the rules for data governance has been a current topic and agenda for many countries (Burri and Schär 2016). Enforced in May 2018, European Union's contribution for setting rules for privacy and handling data has been General Data Protection Regulation. As a safeguard for consumers to have rights over their personal information, the overall aim of GDPR is to protect data and therefore secure the human rights to privacy in the digital world within European Union (Kurtz, Semmann and Böhmann 2018). The outcome of GDPR is that it gives certain rights for consumers and on the other hand obligations for marketers, as consumers possess greater control over how their data is collected and used, and forces marketing persons in charge to make data-use activities compatible with GDPR. In the context of marketing and e-commerce, companies need the consent for collecting and using one's personal data, as well as permission for one-to-one marketing.

Despite of the leap that GDPR has taken in protecting data subjects, little research has been made on how much the regulation has actually solved the key questions that collecting and using data holds. Wachter (2018) argues, that the potential for discrimination, weakness in security, lacks in anonymity and informed consent still exists, Additionally, in many cases, a lot of the implementation of GDPR rely on consumer's own activity and interest (Koops 2014). Grindrod (2016) states, that if companies focus too much on the technical side of the lawfulness of GDPR, such as relying on small printed term and conditions that justify the exploitation of the data collection, the contribution of the GDPR, increasing openness, trust and transparency between companies and consumers, might be hindered.

1.2. Research problem

Data-driven online and marketing personalization has emerged to become one of the main strategy companies to have. This activity is highly depended in consumer data, the process of personalization is complex, and involves variety of stakeholders and intermediates. Thus, it can be arduous for consumers to fully picture how their data is collected and used for online marketing personalization, or how targeting is performed (Stevenson 2016). Although online personalization and data collection has increased in consumer's daily lives, we still know little consumer's thoughts regarding of it.

Although GDPR is expected to enable more equitable digital advertisement space for all the stakeholders, the true effect of the regulation is still yet to be unknown. Especially, although few theoretical papers reviews already exist about GDPR, there is lack of research in understanding consumer's view regarding of collecting and using personal data. Currently, consumer's perceptions and attitudes regarding of personalized advertisement have been empirically tested (Baek and Morimoto 2012; Gironda and Korgaonkar 2018), but their experiences regarding of GDPR has not yet been fully explored. Thus, since GDPR has enabled consumers to have more control over their own data and thus privacy, one should know how their perceive data collection and usage after the regulation has been enforced.

1.3. Purpose

The purpose of this study is to investigate how consumers perceive data collection, online marketing personalization and GDPR in order to find out the reasons why they think this way, especially if any incoherence is there to be discovered from their opinions.

Questions

Thus, in order to study this gap in the current research, one question is guiding this research:

Q1 How consumers perceive data collection, online marketing personalization, and GDPR?

1.4. Delimitation

Marketing and e-commerce personalization is multidisciplinary, complexed and highly networked activity. Due to limited empirical data that is available from the topic, and since this paper follows qualitative data collection, inevitable the nature of this paper is more general. Online marketing personalization is a multidisciplinary activity that requires the combination of information from research domains of retrieval, machine learning, data mining, analytics, statistics, economics and psychology in order to fully understand and predict consumer behavior (Calo 2014). This paper will focus on the marketing practices that are driven by technology and data, aiming to accomplish deeper consumer insights, and thus, deliver more targeted content for them. As GDPR involves all organizations and companies within the EU to comply with it, this paper will only focus on the marketing side of the regulation.

2. Literature review

This literature review starts by conceptualizing what online marketing personalization is. Further, we take a look of the main data-driven marketing practices from the collection of data to its processing and usage for different type of advertisement activities.

We then continue to discuss about the key principles of GDPR and how the regulation enhances them by setting up different obligations for organizations to follow and certain data-ownership rights for consumers. Finally, as a last perspective, the literature review will present consumer view for the personalization and data collection.

2.1. Online and data-driven marketing personalization

As new possibilities to reach customers and practice marketing have evolved, marketing concepts have gone through an evolution that seems not to have an ending; from direct and one-to-one marketing that have mainly referred to reaching customers directly via email, to terms that reflect the use of more sophisticated technology and consumer's accessibility, such as real-time marketing, relationship management, technology-enabled marketing, Internet marketing, database marketing, and e-marketing. They all have two things in common. Firstly,

they all refer to a strategy that identify customer's need with technology, and thus, fulfill her/ his needs. Secondly, based upon the insights marketer have from the customer, the marketing mix is modified according to that individual, on the other words, personalized (Montgomery and Smith 2009).

More than ever, marketers have embraced this opportunity to deliver personalized content for consumers through online environments and devices. In addition to customized ads, online personalization can take multiple of forms, such as discounts, products recommendations, e-commerce prices, and content on social media platforms. Further, based on the combination of verified and estimated consumer data, the tailored content can be displayed for a specific individual. There is nothing new in market segmentation and customizing marketing efforts according to anticipated audience attributes, but seamless computer networks, available technology for online advertisement, and increased consumer information offering by third party companies have all together boosted data-driven advertisement to be more efficient and targeted that we have ever seen (Stevenson 2016). Aslam and Karjaluoto (2017) have linked Internet advertisement with activities of location-based targeting, data-driven user profiling, the segmentation of the markets, retargeting, performance analysis and interactive pricing. Whereas, they refer digital advertising as an implementation of different technologies, digital platforms, and a network of different stakeholders in a complex eco-system (ibid.). Thus, data-driven online advertisement requires number of activities that can take different forms, be performed in variety of online environments, and is an outcome of complex advertisement network of multiple participants. Therefore, the literature review full further discuss the core practices, procedures and the infrastructure that are involved in manufacturing personalization.

2.2. The process of personalization

Personalized advertisement has emerged as a essential form of digital marketing paradigm. Gironda and Korgaonkar (2018) defined personalized advertisement (PA) as customized promotional messages based on consumer's personal information, such as demographics, psychographics, past buying history and lifestyle interests, that are distributed to consumers in paid media context. Instead of reaching the whole segment of consumers as in PA's precursor market targeting, the idea is to take one step ahead and offer specific consumers precisely personalized content, that aims to fulfill his/her needs, interest, and preferences. Vast amount of consumer's personal and behavioral data is collected, analyzed and then utilized.

The process of personalization cab be divided to three stages of learning, matching and evaluation. The first stage involves understanding consumer's needs by collecting and analyzing his/her data (Aguirre, Mahr, Grewal, Ruyter, Wetzels 2015). Data is integrated from online and other customer touch points in order to gain holistic view from the customers and as a product of analytic program, customer profiles are created and then placed to segments that other similar customer belong to as well. Analytic and personalization software are used for determining what those needs are and optimize their product or service offering accordingly (Danna and Gandy 2002). Then, this insight about the consumer is used for matching the right content with the right person and therefore guarantee a personalized

experience for the consumer. Finally, the effectiveness of the offered content is evaluated as a measurable feedback, such as analyzing click-through rates of that advertisement. Every stage include the view of learning about and adapting to customer needs (Aguirre et al. 2015).

Collection of data

Personalization starts with the collection of data. The engagement of the customer on cognitive, emotional and behavioral levels is only possible if companies are ready invest in knowing their preferences, likes and dislikes, thoughts, feelings, and actions. However, instead of knowing their customers personally like local brick-and-mortal shop owners and establishing a real-life relationships and thus information about them, marketers are now eagerly seeking ways to imitate this relationship in digital platforms by deploying technology and replacing these intimate insights about their customers with other external sources (Martin and Murphy 2017). Marketers have now resources and abilities to determine consumers, who will and will not buy, and if their reaction to different advertisement efforts been negative or positive (Hill and Martin 2014). Further, by gaining this knowledge, companies can understand online behaviors, develop their marketing strategies, and measure the effectiveness and outcomes of the marketing itself (Kannan and Li 2017).

In parallel to the expansion of Internet-enabled technologies and increasing Internet use, more opportunities to collect personal data have emerged, as the volume, variety, and velocity at which personal data is generated remains on the rise (Stevenson 2016). Tapsell, Akram, and Markantonakis (2018) define user-data as:

> *"A set of data that represents and is associated with the identity, activities and service-offerings associated with a unique individual. Whether in an identifiable (non-anonymised) or non-identifiable (anonymised) form - collected/process/shared by an organisation (or its partners) to either provide/tailor a service to the respective individual."*

Grindrod (2016) states, that the increasing amount of available data for analysis forces one to think how personal information can be both connected to and from individuals. Fore example, they can be identified based on name or address, or at the other extreme, attached to large population segments based on socio-economic, behavioral, tribal (such as football team allegiance), or genetic grouping. As technology has and will takes leaps forward and new sources of data keep emerging, there are more opportunities for gathering Personal Identifiable Information (PII) that is by nature more reliable and contextual, and thus intrusive. Such as, mobile devices have further lead to the rise of sophisticated geo-location technology, enabling the development of geo-targeted ads (ibid.).

Additionally, behavioral data and its detailed monitoring has been routinely established in online environments for marketing purposes. Powerful indicators for interest may be the recorded 'hover time' that user's mouse cursor moves over the displayed online ad or the seconds or milliseconds that one spends with each specific content, while scrolling through individual social media newsfeed (Stevenson 2016). According to Yuan, Abidin, Sloan and Wang (2012), users can be identified and profiled with browser data alone without cookies or

other tracking files. Once the identification of the user has been accomplished, they can be tracked across the websites and other publishers web sites that share the same advertisement and data exchange network (ibid.).

The ability to truly know your customer has reached up a new level due to the use of big data and marketing analytics (Martin and Murphy 2017). In fact, as Big Data has made possible to follow customer during their customer journey, becoming a basic element for optimization of advertisement campaigns and budgets (Leeflang, Verhoef, Dahlström and Freundt 2014). Big Data is characterized by high volume, value and velocity. The omnipotence of Big Bata emerges from its ability to know detailed information about us and predict our behavior (Oliver and Vayre 2015). A real life example of this powerfulness was witnessed when Target's technology was able to know a girl's pregnancy by monitoring her shopping patterns – not before this customer received coupons for new baby clothes and cribs her pregnancy was revealed for her parents (Hill 2012). Inevitable, due to the emerge of Internet and Big Data, it is possible to gain access to data without any cooperation. Therefore, questions regarding of privacy, ownership, identity and consumer's reputation are highly relevant in Big Data paradigm (Oliver and Vayre 2015).The risk that comes along with the new opportunities to sort, combine and analyze both sheer volume and personal data, may not be perceived at all by consumers, since data that appear to be mundane, has the probability to evolve into sensitive information with the assistant of Big Data technologies (Burri and Schär 2016). These abilities are under the control of few gatekeepers and characterized with lack of transparency (ibid.).

Marketing analytics

The ability to analyze massive amount of consumer behavior that is generated in online environments is both a opportunity and challenge for marketing managers. A variety of services are currently available for Big Data analytics and intelligent techniques applications to assist in interpreting consumer data (Pantano, Giglio and Dennis 2018). Additionally, the best way of 'making sense' of vast amount of data is to use data mining, which has become essential part of processes that are used in companies (Danna and Gandy 2002). By understanding the past consumer behavior and preferences, marketers and sales professionals can forecast future patterns and trends (Brito, Soares, Almeida, Monte and Byvoet 2015) .

However, the process should not be misunderstood as simple. On the contrary, through domain knowledge, heuristics and clustering algorithms, data is partitioned, sliced, diced, and pivoted, finally reduced and filtered for identifying customer segments and supporting knowledge discovery activities (Zwick and Dholakia 2004). Finally, different type of data is creates a variety of knowledge. For example, Internet time analysis is performed after the advertisement has been established in the digital environment. If customer does not react to the provided content according to the profile the person is assigned should, as a repetition of a process that happens seamlessly and instantaneously, new calculations are made to ensure more relevant advertisement in the next interaction between the customer and digital environment (Danna and Gandy 2002). Van Ooijen and Vrabec (2019) argue, that individual's control for data processing might be challenging in the data economy. Although consumers give their consent by approving user policy for their data collection and therefore approve the

primary use of the data, it is likely that the secondary and reuse of their information remain unclear (ibid.).

Segmentation

In addition to analytic programs, consumer's profiles are essential in the process of personalization – according to marketers needs and preferences, data is after mixing and matching constructed, deconstructed and reconstructed to customer profiles. The holistic view that has been gained through the collected and processed data is further used to place consumers into segments, which members share the similar characteristics with each others (Zwick and Dholakia 2004). Thus, in order to target specific groups based on demographics, psychographic, and behavioral data, the creation of such profiles is essential (Degeling and Nierho 2018).

France and Ghose (2018) argue that segmentation is key activity for marketers, and define it as a process of seeing a rather heterogeneous market constituted by smaller homogeneous markets, being one of the most classical used marketing strategy. Grounded in the principle that, rather than aiming to satisfy every existing customer, companies divide the market into segments, and then target the most appealing group of customer in terms of profitability and sustainability (Brito et al. 2015). Brito et al. (2015) argue, that although the outcome of the segmentation correlates with the input of variables, compared with information that demographics, psychographics, geographic and lifestyle can provide, behavioral data (such as buying frequency or consumer's response to sales promotions) have shown to be the most efficient when more refined segmentation is required. Since social network users voluntarily discloser their information and their accounts are used through different devices, profiling is easy to perform in these platforms. Although outside these networks profiling is more demanding, cookies and properties of the browser able tracking and the identification of the individual user, and hence, constitute in attaching attributes to the consumer usually without their explicit awareness (Degeling and Nierho 2018).

Zwick and Dholakia (2004) point out, that rather than just constituting the individual, the database also enables companies to act strategically towards the consumers. Since databases can constitute in constructing the variety of representations of the same consumer in one marketplace, consumer can be part of several profiles and may present multiple of personas in at the same time. As consumers are divided, contrasted, related, regrouped, classified and derived from one another through the rules of formation, databases inscribe personalities and identities *onto* consumers (ibid.).

Targeting through advertisement

Finally, after the previous stages are completed, the advertisement takes place. Calo (2014) argues, that relevance is one of the key objectives of today's digital marketing. Advertisement network aims to deliver content that is relevant to its receiver, therefore, the optimization of advertisement tendency is to maximize the impression of the display of an ad. Currently, three main categories for using and selling space for promotions in online advertisement are search engine, social media, and online display advertisement, following the classical principles of display advertisement, established since the existence of Internet marketing. However, as the

marketing infrastructure has grown and its network expanded from these days, the process in which publisher sells a display space for advertisement based on the impressions or clicks for the marketer has evolved towards more complicated phenomenon (Aslam and Karjaluoto 2017).

Degeling and Nierho (2018) describe the current advertisement as an exchange system, where online ad spaces are traded on 'high frequency bidding platforms'. Based on forces of demand and supply, four main players are responsible for the interplay as ad inventories are traded: ad exchanger, advertiser, publisher and user. An advertiser wish to get the promotions displayed and publishers sells these displays in return of revenues, whereas ad exchange service works at the administrational way in between these two, so that marketers can find the right audience for their products (Yuan et al. 2012). Additionally, data exchange (DX) is sold and served all of these parties by providing real-time information about consumer data. In case of behavioral targeting, the data can be sold directly to the marketer in real-time bidding (RTB) for securing better match between ads and users (Stevenson 2016).

In addition to complex network that participate in the complex supply of advertisement exchange and data, the process of advertisement itself is becoming more automated (Stevenson 2016). Sometimes referred as programmer advertisement, instead of traditional media or ad-slot-buying, this practice enable precise audience targeting in real-time, that is stimulating a new growth for big data-driven online advertising format. By bringing right audience and best-matched advertisers together, even more efficient matter than before (Li, Yuan, Zhao and Wang 2017).

Third party companies

The phenomenon of personalization both fuels and is affected by advances in information technology and joint forces for consumer data collection efforts. As an outcome, new nexus of business interests and cooperation among commercial website and app developers, third party data providers, marketing services, and media companies has emerged (Stevenson 2016). Therefore, when discussing about personalization, dismissing the third party companies role in data collection, processing, and usage mean that a big part of the personalization process would be ignored.

One more source for offline and online data is provided by third-party companies that are responsible for demographic and psychographic databases, which can be further aggregated into data warehouses and 'mined' (Danna and Gandy 2002). Acting as an intermediate, these non-visible companies perform between consumers and them facing companies, are able to collect and distribute consumer data further to marketers (Stevenson 2016).

In addition to harvesting vast amount of data, these third party companies offer site traffic insights for web editors and optimize the content for advertisement space, provide advertisement banners, videos, are responsible for retargeting activities and intermediate 'liked' and 'shared' content on social media. The more accurate profile these companies are able to create from the users, the more valuable this information is for advertising (Sørensen and Van den Bulck 2018). Through techniques of real time internet cookie synchronization

across web properties, executing consumer surveys, aggregating online and offline financial transactions, these data brokers can both identify and classify the internet users. Individual's offline and online activities create a trace of records that are given certain further meanings and identifiers, and can vary from one's race, income and family status to previously purchased brands (Stevenson 2016).

As an important link between marketers and consumers, 'data brokers' are firms that have specialized in different supportive actions within the complex digital marketing supply chain (Stevenson 2016). The trade of data is performed between data management platforms and other actors within the marketing value chain, such as sell-side, demand-side and real-time bidding platforms; within user-profiling and segmentation companies; and providers of personalized and programmatic advertising. Since this exchange has remained hidden from the public view, the evaluation of these activities is rather challenging (Sørensen and Van den Bulck 2018).

2.3. Consumers, personalization and data collection

Personalized advertisement (PA) has been argued to benefit both consumers and marketers. For consumers, since the communication messages they receive are based on their preferences, PA enables them to focus on what they really want and safe time, whereas for marketers, PA has shown to be a promising tool for reaching efficiency in costs and ad distribution and plays central role in customer relationship management (Baek and Morimoto 2012).

However, in parallel to marketer's excitement for personalized marketing, concerns towards these data collecting methods and their usage for marketing purposes have emerged among consumers and media, such as Facebook leaking data for third-party firms. In addition to better informed and data-conscious consumers, many perceive targeted advertisement or too personal customization as 'creepy' (Gironda and Korgaonkar 2018) emerging unpleasant feelings and experiences (Kshetri 2014). In fact, Aguirre et al (2015) have reported that consumers get irritated about personalized marketing practices and may generate feelings of discomfort when information has been collected without their consent. Fashion retailer Urban Outfitters was forced to change their website that was uniquely adjusted accordingly to its visitor's gender, since this personalization was claimed to be too personal and the information about the users was collected without their awareness (ibid.). To explain the contradicting attitudes about personalization, researchers have developed a 'personalization-privacy paradox' concept. Gironda and Korgaonkar (2018) describe the paradox situation emerging, when consumers have wishes towards relevant content and personalized advertisement, but are not fully comfortable with the practices that are involved with it.

The collection of data by the providers of digital services is not only limited to cookies, but social network sites are an additional source of information, which design make it easy for the consumer to voluntarily disclose information. The trade-off with the short-term gain of using the platform versus the long-term benefit of enhancing their privacy may be blurry for the consumers, but also as revealing information has become the new norm in the sharing

economy. Thus, protecting one's privacy can be challenging when more and more the participants of this new paradigm expose and share individual's data with the other stakeholders (Krämer and Wohlfarth 2017).

Montgomery and Smith (2009) argue, that defining privacy may be rather challenging, since the meaning can vary from a contractual agreement between the participants to a basic human right. Therefore, when personalization is in consideration, both perspectives, businesses objectives and consumer rights, should be balanced and understood (ibid.). Privacy concerns and feelings of lack of control over their personal information have emerged among consumers, since they feel that in today's world it is unclear how much companies know about them and in what extent they use their personal information (Gironda and Korgaonkar 2018). As marketers have been able to go beyond traditional consumer observation with new data aggregating tools that synthesize data from multiple of places, even from sources that consumers may not expect, the resistant towards these sophisticated marketing tactics and data usage appears to be growing (Martin and Murphy 2017). An outcome of too personalized advertisement may be consumer's reactance, if they suspect that their data have been invaded by unknown advertiser or third party companies, and end to threaten consumers' perceptions of freedom to control how personal information is used (Baek and Morimoto 2012).

Transparency may be difficult to achieve in online content personalization. Stevenson (2016) argue, that there is lack of openness on how online ads are personalized and algorithms for personalization are used, and may be considered as trade secret that are not open for public view. Inevitable, internet users may be unaware of the level of personalization, the extent the content they receive differ from others, and what consumer information has actually been included for that personalization process. As the use of smartphones and other daily use of interactive media has kept rising, automated content personalization practices including highly targeted advertising techniques may pose new challenges for both marketers and consumers (Stevenson 2016).

Ooijen and Vrabec (2019) highlight three major issues that are involved when consumer data is being collected and may hinder consumer's control over their own data; the intangible nature of that data that makes it challenging track where their data has been collected to; the flow of data in the complex network that participates different activities around data; and consumer's limitation to fully understand what they have agreed upon by giving a consent for their data collection and its processing. Degeling and Nierho (2018) argue, that the ability to track and profile Internet users do not only possibly harm their privacy, but also the power unbalance between the online platform participants may outcome as reproducing stereotypes, price discrimination and indirect exclusion.

2.4. GDPR

2.4.1. What is GDPR

Consumer's control over their personal data has been challenges by many factors - not only by the vast amount of data they produce in every online transaction, but also due to increased technological complexities and multiple data-exploiting business practices (van Ooijen and Vrabec 2019). Previous data protection law, Data Protection Directive from 1995, has now

been taken over by General Data Protection Regulation, since especially within the marketing field, there has been major leap in technological development and proliferation of consumer data, and change in consumers' attitudes too (DMA 2018).

Modernizing and harmonizing the protection of data within the EU as a main objective (Burri and Schär 2016), the General Data Protection Regulation (GDPR) establishes the first legal reference framework for companies to adopt and implement a culture of privacy and the protection of personal data, thus, is a new prescriptive norm for companies to follow (Martínez-Martínez 2018). The regulation has an effect to our contemporary digital surrounding, to multiple different stakeholders: not only the self-determination of European citizens' information is enhanced, but also the way how intermediaries and companies control, process, and use personal data liable (Burri and Schär 2016). Van Ooijen and Vrabec (2019) state, that compared to earlier regulations, the importance of individual control has been stated more explicitly in GDPR.

There is three acknowledged parties in GDPR: data subject, controller and processor. The technical term of data subject refers to an individual whom particular data is about. Controller is an person or organization that decide how and why to collect and use the data and is responsible of verifying that the processing of data is performed according to data protection law. Whereas, a processor is external person or organization that processes (including collecting, recording, storing, using, analyzing, combining, disclosing or deleting) data on behalf of the controller, and have less legal obligations compared to controllers (ICO 2019).

2.4.2. Obligations for companies

GDPR's philosophy can be met if personal data is collected for legitimate reasons, it fits for the purpose it is collected, the amount of data has reduced to the minimum necessary level, and the processing of data is implemented in fair, lawful and transparent way (Axinte, Petrica and Bacivarov 2018). Watcher (2018) argue, that transparency is essential for achieving user's awareness of data collection and processing, and thus, one can generate trust by utilizing technology and tools that enhance privacy and compliance through data protection. In GDPR, transparency and trust can be achieved in several ways, such as informing data subjects about the existence of automated decision making and profiling, making them aware of the rules, safeguards and rights they have regarding of processing of personal data, and notifying them about data breaches in case of such (ibid.).

GDPR consists of seven key principles: lawfulness, in which data should be processed with fairness and transparency; the purpose for data collection is specific and legitimate; data is processed sufficiently and only what is necessary for that context, which fulfills the principle of data minimization; the information that the data controller holds from the data subject is accurate and updated when needed; the storage of the data is limited until the data is not needed; the processing is proceeded in secure matter; and accountability (Burri and Schär 2016). Rather than offering a comprehensive guidance that by following companies shall know what to do in each data-involved scenario, organizations are required to set their own policy and decide themselves how to implement and comply with GDPR. In order to achieve

this, companies are required to show how they have collected the data, state why they need it for, how it is used, how the data is secured, and the legal basis for processing it in the absent of clear and defined answers. Additionally, companies should set technical, organizational measurements, and audits to justify and prove every action and decision the company has made (DMA 2018). Hence, accountability is the combination of responsibility for compliance and demonstrating it - organizations are required to be proactive towards data protection, be in charge for what they do with personal data and how well they fulfill the other principles, and be able to track their past behavior and made decisions regarding of data (ICO 2019).

Thus, the principles are delivered through accountability – since GDPR focuses in enhancing privacy by protecting the individuals data and informing them about its collection and usage, Tapsell et al. (2018) argue, that privacy notices and terms & conditions should be unambiguous and clear, thus, online users that accept these notifications should give their consent mindfully as form of affirmative action. Since consumer's consent designate the processing of data as lawful, they should be right to know what data has been or will be collected from them and how it will be used, and alongside, who has the access to it (Dewar 2017).

2.4.3. Impact on marketing

As personalization, and hence online tracking and consumer profiling, has become part of the advertising field, the lack of transparency and consumer choice have been stated as main problems of the tracking ecosystem that collects and aggregates vast amount of data from the Internet users. These negative impacts to consumer's privacy has been taken into account in GDPR, and is expected to change the industry too by the means of bringing more transparency towards the used practices, although the impact on tracking and profiling itself may be rather little (Degeling and Nierho 2018). However, although the effectiveness of the regulation depends on each unique context and situation, individuals should have the opportunity to (1) deny the use of personal data for profiling, (2) have the right to be informed about the existence of profiling, and (3) power to object direct marketing activities (ICO 2019).

Since communicating to customers is essential for company's commercial success, direct marketing has been stated as a legitimate interest in GDPR, which means that out of six legal grounds for processing personal data according to GDPR's principles, marketers are likely to use consent and legitimate interest. Consent must not be passive and companies are demanded to be able to track individuals consent for processing of their personal information. Thus, automated decision making, such as the use of segmentation, targeting, profiling and analysis, can be covered through legitimate interest (DMA 2018).

2.4.4. Consumers' rights

The General Data Protection Regulation highlights the control that individuals should have over their own personal data. The regulation has listed eight data subject rights that can be

splitter into three sections of (1) information and access to personal data, (2) rectification and erasure, and (3) the right to object and automated individual decision-making. (van Ooijen and Vrabec 2019).

Right to informed is probably the most commonly featured part of the regulation, that is embodied in companies' privacy policies. Before any processing of personal data takes place, consumers should be able to know the contexts that the data will be processed for, the identity of the data controller (who will decide how the data is used), who will handle the collected data, and the period of time the collected data will be cached. Additionally, any information regarding of automated decision making, such as profiling, or the possible consequences of such practice, should be announced (van Ooijen and Vrabec 2019). Burri and Schär (2016) argue, that this knowledge should all together increase transparency about data-related activities.

Bestowed by GDPR, DMA (2018) lists the eight consumers rights as followed:

The right to be informed - to know what happens to the collected information
The right of access - ability to access the collected and stored data without additional cost
The right to rectification - data should be kept accurate
The right to erasure - the right to have data deleted or to be forgotten
The right to restrict processing - where the data subject believes the data is inaccurate, the processing is unlawful; data subject challenges the data controller's legitimate interests
The right to data portability - to transfer data from one supplier to another
The right to object - to stop data from being processed
Rights in relation to automated decision making and profiling - not to be pro led or to have a human make automated decisions (such as algorithms).

2.4.5. Critical view

Despite the achievement the regulation has accomplished within the area of data ownership and use, some researchers have already identified some aspects that may decrease the effectiveness of the regulation – factors that weaken the consumer power and the GDPR itself. Burri and Schär (2016) argue, that there are main three pitfalls; too much emphasis on informed consent and individual choice; the regulation's bureaucratic nature that focus on the technical implementation; and dismissing the role of data in the contemporary economy. Martínez-Martínez (2018) point out, that the legal ground for the regulation is more theoretical than real, and due to the lack of practicalness the right for data protection may remain vague. Krämer and Wohlfarth (2017) argue, that the initial thought of strengthening the interests of the consumer may be hindered, as they may not be aware of how their newly-gained privacy rights function in reality, such as who shall one be in contact with in case of the right to be forgotten is wished to be implemented.

Koops (2014) has addressed more the problems that are involved with having too much weights on consent, which acts as a legal ground for many of the data-related activities. He

also states, that the concept of consent is highly theoretical, since although by paper the Internet user's are truly informed when accessing the websites, they still have not fully invested in understanding the privacy statements, or be fully aware of the extent and conditions their data is being processed and used. Additionally, there is little to choose – not many of us have the opportunity or the will not to use online services such as Google Facebook, making most of the users to accept the privacy policies by force (ibid.). Additionally, Hull (2015) lists that since consents are usually dubiously given, privacy preferences are challenging to enhance in practice, and not participating in privacy-harming websites unrealistic in modern society; consumer's self-management might threat their privacy instead of protecting it.

Krämer and Wohlfarth (2017) state, that nevertheless consumer's right to their personal data and its usage bestowed by GDPR, this grant may only become challenged due to conflict it faces with digital data-driven business models, and thus, the effectiveness of such right may be questionable. Moreover, consumer's given consent, especially in free services and platforms, can be carelessly licensed for companies, making the permission for collecting and using consumer data more formal than factual (ibid.). In order the consent to be meaningful, the consumer must understand what she/he is giving the permission to – due to information asymmetry, neither knowing or understanding how their data is utilized may be the reality for many (Hull 2015).

3. Theoretical framework

We now take a closer look to the concepts of the theoretical framework: information asymmetry and privacy paradox.

3.1. Information asymmetry

The concept of information and power asymmetry is commonly know and used in business sciences. However, the late technological development and rise of information economy have spread the use to describe the asymmetry between consumers and companies (Nissenbaum 2010; Gitelman 2013).

Being in some extent observed on e-commerce platforms should not become a surprise, in fact, it has taken a root as a common business standard. However, in parallel to companies' ability to create behavioral profiles that are derived online and in-store shopping consumer behavior, they hold the power to know their customers in detail (Martin and Murphy 2017). Thus, when one party does not know what another party knows, information asymmetry occurs. In personal data asymmetry, in today's "one-way mirror society", this means a situation where other party, marketing firm for instance, collects and stores data that describes the attributes of another party, an individual, that is unable to see, know, correct or control this data, dividing these stakeholders to advantage or disadvantage parties. Due to the complexity of data sharing agreements and third-party providers, it is difficult to point out the exact

organization that may exploit the data and offer it for personalize the online ads that the Internet users phase while exploring the web (Stevenson 2016).

Additionally, as van Ooijen and Vrabec (2019) state, contemporary web environments are challenging for consumers to comprehend, since today the data is processed by sophisticated algorithms which mechanism have remained unknown, and further, the outcomes unpredictable. The information that the consumer receive about the data collection and usage may remain abstract and the final receiver of that consumer data unrevealed, resulting in information asymmetry between the the individual and data collector (ibid.). Moreover, as authors argue, as even the data controller themselves are unfamiliar with the final destination of the collected data, lack of informational control exists (ibid.). Additionally, consumer's decision-making about privacy can be hindered due to imperfect or asymmetric information, a burden of digital economies (Acquisti, Taylor, and Wagman 2016).

3.2. Privacy paradox

The view of information asymmetry has been recently applied to the concept privacy paradox (Bergström 2015), which reflects the situation when human behavior do not match with privacy related attitudes, thus, they appear to be in conflict with each others (Deuker 2010). For example, as Hull (2015) writes, the paradox may occur when individual express their concern for their privacy, but easily trade their personal information for low value in online environments or other exchange circumstances. In fact, privacy paradox can be used to interpret that, since people's actions and attitudes towards their privacy are controversial, individuals do not actually care about privacy in great extent (ibid.).

The trade-off between disclosing information and perceived benefits that are gained through that action has been studied several years - the economic approach has been that users seek to maximize their utility constantly by balancing costs and benefits (Deuker 2010). Thus, risk-benefit calculation plays a major role in the context of information privacy, known as the freedom to decide with whom, how and to what extent personal data is shared. The calculation to maximize the benefits and minimize the risks of information discloser takes place as the information is exchanged, when individual weight negative outcomes against expected positive benefits (Barth and de Jong 2017).

Kokolakis (2010) argue, that most people are lacking the cognitive ability to calculate privacy risks and disclosure benefits and do not have access to all necessary information in order to make informed judgments about the trade-offs that are involved in privacy decisions. Thus, as individuals make privacy decision in limited time having incomplete information about risks and benefits, and are not able to calculate all the relevant parameters, their privacy decisions are constrained by incomplete information (ibid.). Deuker (2010) writes about two types of incomplete information: (1) the situation when users may not be aware of the extent that their behavior is observed, stored and processed without their knowledge, meaning that individuals do not fully picture what data they disclose, and (2) the unawareness of the consequences of that disclosed data, since the it might be available to other parties or aggregated with other sources of data that individual has little control to. Additionally, Bergström (2015) emphasize,

that many consumers lack of awareness of the possible risks and skills on how to protect personal information.

4. Methodology

Research design and process

Since the aim of this study is to gain a deep understanding of the studied phenomenon, online marketing personalization, data collection and privacy from he consumer approach, the paper will follow single case study strategy. Thus, taking into account the complexity of the studied object with holistic perspective (Punch 2014, 120). In addition to finding out how consumers perceive the studied topic, the main objective of this study is to understand why they reason and think certain way, as it will describe the in-depth experience of a group. Therefore, the social phenomena is studied by analyzing the individual case (Punch 2014, 121). In this study, the case will be focus groups, from which the empirical data will be collected through direct observations and interactions. The process of this study is deductive - according to linear approach, the research questions will guide the paper as data is collected with qualitative methods. Finally, the results of the focus groups, the method of data collection, are analyzed with theoretical framework, forming a synthesis of the participants experience.

Data collection

The overview of digital marketing was formed by searching different type of marketing and advertisement strategies – in order to gain comprehensive picture from online personalization, variety of keywords were used for searching articles from Scopus and Web of Science, such as digital marketing, direct marketing, behavioral marketing, targeted marketing, programmed marketing and display advertisement. Additionally, searches with topics of big data, data mining, marketing analytics, marketing infrastructure, segmentation, profiling, personalization, third party and data broker was conducted in order to gain wide perspective from the topic. The wide scope of search with variety of keywords was essential, since many papers focused on narrow view of the topic, and holistic perspective would not be otherwise successfully accomplished. Further, all the relevant available information regarding of GDPR were explored. Thus, the importance of focusing the consumer side in this study was emphasized by the lack of current research about the of consumer view of GDPR. In addition to database article search, knowledge about information asymmetry and privacy paradox were prospected from peer-reviewed articles and their reference lists.

In order to gain a consumer view regarding of the research topic, primary data collection was accomplished through a focus group discussion that was recorded for transcripts. This paper will focus in qualitative primary data collection, since instead of following strict format, ’post-structure’ approach allows research participants to explain their view in their own terms (Punch 2014, p. 87), which is important when studying something as complex as GDPR and online personalization. Thus, how respondents explain the research topic in their own words offers an interesting angle to the research problem.

Focus groups

In order to gain consumer's perspective and reasoning regarding of the topic, in total 4 focus group discussions were conducted. Focus group discussions were chosen as a method for data collection, since it was seen to correspond the scope of research: understanding consumer's thoughts regarding of online personalization, data collection, and GDPR. Since the chosen perspective to view the results were information asymmetry and privacy paradox, and the reasons that lead to their existence are multiple, it was crucial that the data collection method would allow a variety of data to be discovered. Additionally, according to Bryman and Bell (2014, p. 514), focus groups offer deeper apprehension about the causing factors, as well as demonstrate how individuals collectively reason about the phenomenon and construct meanings around it. Thus, enabling variety of views to emerge and a place for the participants to share their opinions. Other contribution of this technique is data that emerges from the group itself - the way in which individuals discuss the given theme in the group, interact with each other's view, and how the discussion evolves as new ideas emerge in the group (Bryman and Bell 2014, 512).

Each group consisted of 5-8 individuals, since bigger groups are difficult to manage (Bryman and Bell 2014, p. 517), and in total, four focus group discussion was performed – one as a pilot to test the agenda of the discussion and rest as normal. The demographics of each group it listed in table 1: *group 1* (pilot) participants were Finnish, working, had an age between 28-29 and women; *group 2* were international students, had an age between 23-25, and had 5 women as participants; *group 3* were Finnish, working, had an age between 22-27, and consisted of 5 women and 1 man; and group 4 were international students, had an age between 24-32, consisting of 4 women and 1 man. The demographics of the participants were from Finland, Sweden, Nepal, Estonia, Germany and Japan, all living in Sweden instead of group one. In total, four focus groups had 21 participants, from which 10 were students. Additionally, as the table 1 shows, the majority of the participants were woman.

Focus group 1	Abbreviation	Demographic	Gender	Age	Occupation
	1A	Finland	woman	28	working
	1B	Finland	woman	28	working
	1C	Finland	woman	28	researcher
	1D	Finland	woman	29	working
	1E	Finland	woman	29	working
Focus group 2					
	2A	Sweden	woman	24	fashion marketing student
	2B	Sweden	woman	23	fashion marketing student
	2C	Germany	woman	24	design student

	2D	Germany	woman	25	fashion marketing student
	2E	Sweden	woman	24	fashion marketing student
Focus group 3					
	3A	Finland	woman	27	working
	3B	Finland	woman	25	working
	3C	Finland	woman	27	working
	3D	Finland	woman	33	working
	3E	Finland	man	22	working
	3F	Finland	woman	24	working
Focus group 4					
	4A	Japan	woman	32	fashion marketing student
	4B	Finland	woman	26	fashion marketing student
	4C	Nepal	woman	24	fashion marketing student
	4D	Sweden	woman	25	media student
	4E	Estonia	man	27	fashion marketing student

Table 1. The list of groups and participants

Before the focus group talk was conducted, the participants were informed about the main topics of the discussion, which were online personalization, data collection, and GDPR. The participants were not obligated to do any preparing research regarding of the topic beforehand. The discussion started with short introduction of the topic, and the participants were courage to express their thoughts freely in a form of a conversation. The moderator made sure, that each topic were covered during the discussion, and intervened only, if the conversation drifted too much to side tracts.

The focus group discussion proceeded as followed; starting from what thoughts data collection and usage emerged, the talk moved to map the feelings towards personalization and how they think it works; further to GDPR and how well they acknowledged the rights they have as consumers and on the other hand the obligations companies possess; and finally to online privacy and how they personally enhance it. The discussions were recorded and their length varied between 45 minutes to 55 minutes and were recorded by the moderator. Finally, transcripts of the focus group discussions were made for further data processing.

Sampling

The type of sampling was selected to be purposive, which as non-probability form of sampling do not aim for find the participants on random basis. Rather, the people are recruited based on their relevance to the research questions and variety is secured by other means (Bryman and Bell, 429). Since it was essential that the focus group participants would be able to discuss about data collection, GDPR and targeted marketing, and additionally have some idea about targeted marketing and data collecting in wider perspective, the sampling was based on non-random factors. Therefore, the majority of the participants were chosen based on their educational level and age, 22-32, since they probably feel natural using technology and Internet-connected devices in their everyday lives. Additionally, the most likely, have experiences regarding or targeted marketing in online environments through their social media channels and other Internet platforms, as they search information, socialize, seek for entertainment and purchase as well. The diversity of the group was secured by having both students and people from working life from different backgrounds and demographics as participants. Thus, this reflected to the emphasis and opinions, that appeared to vary sometimes much between the participants and groups.

Qualitative data analysis

The first step of qualitative data was analysis was performed through content analysis, which involved practices of coding and memoing. Other key elements of such analysis was data reduction and verifying conclusions – reduction starts with categorizing the data through coding, finding themes, patterns, and further concepts, whereas after the data is organized and summarized, conclusions can be thus verified (Punch 2014, pp. 171-172). Two techniques, coding and memoing, was be performed alongside each other. Coding refers to a systematic approach that attaches meanings to the pieces of data, and either uses descriptive codes that label what is in the data, or inferential paternal codes, that interprets the data under the analysis. Whereas, demoing records the ideas that emerge from coding, offering deeper and creative touch for the data, and vary in between substantive, theoretical, methodological or personal perspective (Punch 2014, pp. 173-177).

The cause of the analysis was not seek for empirical evidence of the existence of privacy paradox existence – the conflict between attitudes and behavior. Rather, through the analysis, the aim is the deeper understanding of why consumers reason or feel as they do regarding of data collection and online personalization. Thus, what kind of impact information asymmetry and privacy paradox has on the participants. Hence, as Acquisti et al. (2016) argue, the conflict between privacy attitudes and actual behavior is an outcome of many reasons, that in parallel challenge consumer's privacy related decision making, such as asymmetric information. Therefore, since there might be several significant causes for the paradox itself, Deuker (2010) states they are arduous to find or combine in one meta-theory. Thus, this paper will focus on the roles of information asymmetry and privacy paradox, since they play increasingly big part in today's data-driven and hyper-connected online environments and proposed in empirical research to have an impact to privacy decision-making (Acquisti and Grossklags 2005).

Research quality

In order to increase internal validity, pilot focus group was executed before the actual groups to test whether the asked questions were placed in the right order and the respondents could find them reasonable. The feedback from the pilot group was utilized for adjusting the final questions and finding the right emphasis for the topics that should be covered during the discussion. Additionally, as the focus group discussions were performed, the moderator tried to intervene to the discussion as little as possible in order to have as natural group interaction as possible. Therefore, this study have aimed to increase validity by choosing the right methods for studying the topic of the research, as Bryman and Bell (2015, 400) suggest.

Since this study is qualitative by its nature, the external validity may be weak, since qualitative approach makes standardized comparisons rather challenging (Punch 2014, p. 87). Despite the advantages focus groups offer, they come with some limitations. Bryman and Bell (2014, p. 514) mention, that due to unsystematic nature of the sampling and small number of participants, problems regarding of generalizability in single case study may occur. However, as Punch (2014, 122-124) argue, since the emphasis is to understand the complexity and multiplicity of the case, in fact, the method do not aim for generalizability. Rather, case studies can contribute in other valuable way, such as offering in-depth insights about problematic research area or complex human behavior. Hence, this paper will try to find new aspects by collecting data through focus groups, since that method has not been applied much within this research area.

Research ethics

Since the focus group discussions were recorded with smartphone for transcripts, the participants' consent were required. The voice files were deleted after the transcripts were finished, so the personal data was kept no longer than needed. Additionally, the participants identity has been protected, as they have been intend marked by abbreviations.

5. Empirical findings

The groups themselves had different emphasis for the topics that were covered during the discussion. Mainly, the attitudes varied the most with how they perceived the concept of personal data itself, how worried they were in general about privacy, and how they perceived online personalization. However, although the overall tone of the discussion varied in between the groups, common themes that connected all of the groups were found. We will first take a look on what emphasis each group had with an overview of each focus group discussion, and then further continue to the discovered common themes.

5.1. Overview of the group

Group 1 (pilot) - Anxiety and concerns

Group characteristics: Working in Finland, Finnish.

Throughout the conversation, concerns towards one's privacy were present. Although the participants were spooked about the phone listening and over all feelings about surveillance, the emphasis in data collection and use was highly involved in personal data, such as contact details and pictures in social media. The participants mentioned different ways that information is collected: visited webpages, what you have search from Google, age and gender, Internet's IP address, and social media platforms (especially Facebook). The main types of information that the participants felt like the commercials that they saw were based on demographics (age and gender) and online behavior. When seeing ads that they could not identify the source of the information it was based on, they questioned the method of collecting such data and were suspicious that it was done covertly. Since they could not explain how the collection was made, as they could when receiving commercials right away after visiting a certain brand's website, a theory about about phone listening were broad up to reason this.

In general, the participant of this group were mostly concerned about their personal information being abused by a third party person as an identity fraud. Two participants had experienced the abundance of personal information by a third party person, unauthorized use of email address for a Spotify account and the use of personal information for fake LinkedIn-profile. The collection of data for marketing purposes was mostly perceived neutral. However, extending the use of collected information for other purposes than marketing, was considered as worrying. The views about online marketing personalization was divided into two: on the other hand, if the received content was relevant, the ads were seeing useful, but how the marketing itself was performed felt too pushy, and the used methods for targeting emerged anxiety among the group. One participant mentioned, that if Zalando and Interned know what you have been shopping, the most likely they know more than just that. Unauthorized, covert information collection and further selling was broad up many times. In addition to phone listening, Huawei phone models that collect phone data and send that to China, and how two Finnish administrative bureaus make profit through selling consumers information for marketing purposes, were discussed and judged.

When it came to online privacy, some participants highlighted the important of common sense and considering what information you want to share with whom to minimize the likeliness for frauds. Although few participants had knowledge regarding of GDPR due to their work with customer service, the connection with over all privacy and data protection were weak in the discussion. The most common act to enhance online privacy was to delete information from own social media accounts and apps that might collect phone data covertly, but half of the participants did not mention any. In fact, as one of them claimed, it is difficult to know how to protect your privacy in the first place or know how your information has been used. No one claimed to read companies terms and conditions for data collection, and denying cookies were perceived to be impossible, since some of the used websites do not allow authorize you to use the page without accepting them.

Group 2 - Privacy as a trade

Group characteristics: International students and studying in Sweden, majority marketing students.

In this group, the emphasis of the discussion was more in data collection in wider perspective, rather than focusing in more personal data as in previous group. In general, many was not concerned the data collection itself - in fact, many stated quite often that they do not have 'anything to hide', so someone collecting information in that sense did not worry them. However, not knowing what information companies have from them and how it is used was the main concern among the participants. Additionally, they felt lack of control in how they could restrict the collection of data anyhow, since they perceived there were not much tools to stop them from continuing. Disallowing the companies would not make any difference, since either they already know or you cannot do much to stop them.

The attitudes towards online marketing personalization varied from highly negative and suspicious to more positive views. It was acknowledged, that with the amount of information companies have from consumers, they can offer more relevant content for them, and therefore, be useful. Feelings towards the personalization system itself were mixed. It was sometimes perceived clumsy, as few participants felt irrelevant to see commercials from the products they already have bought, and in cases when they felt that with all the informations companies have from them, they *should* know what commercials they want to be exposed to. Adversely, the ability for cross-device tracking and utilizing your search browsing history was conceived as intrusive. The participants stated, that personalization would receive more acceptance if you would be able to know in which terms the personalization has actually been made. In this group too, conspiracy theories about covert information collection were a popular topic, such as someone listening you through your phone. Just to be sure, few participants explained to cover their laptop web camera with a sticker.

The discussion proceeded towards privacy and its role in today's society. Privacy was sawn as a trade for openness, and many agreed, that inability to participate social life in Internet and other social media platforms would in fact loose an access to a lot of information and take part in modern life. However, more transparency was required from the companies, as although this group had guide good understanding of how the networked advertisement process worked, they felt there were many grey areas, and thus, it was difficult to have a good understanding of the use of the collected data. Thus, more transparency in the personalization would make them trust more the companies and decrease consumers worries towards the used practices targeting requires.

When the participants moved to discuss about terms and conditions (T&Cs) for data collection and the use of cookies, majority felt that they were difficult to understand. The concept of cookies, what they are and how they work was blurry, as well as T&Cs for their use. Many argued, that the formal and legal tone of the used language made their reading more challenging, which might have been done purposefully by the companies in order to confuse the reader. Additionally, they acknowledged that they are very time-consuming and effort-requiring to comprehend, or even to read them. Companies way to inform consumers about the cookies and data collection emerged a lot of emotions. The participants emphasized, that some companies have made impossible for the consumer to deny the use of cookies, since

in many cases, you cannot either see the content in the website without accepting them, or by visiting the website you accept the cookies by default. This made some participant frustrated, but they felt that there is little they could do to change the situation. In this context, trust was mentioned again - the less you trusted the website you visited, the less you wanted to enter the website if the site's policy for cookies made them to feel suspicious. The participants admitted that there were not really a red thread in their decision making for agreeing or denying cookies, as it was more connected with their own mood and how they felt towards the website they visited.

Group 3 - The fuss with GDPR and conspiracy theories

Group characteristics: Working in Sweden, knowing basics of GDPR, Finnish

This group was not worried about data collection in wider perspective, although some conspiracy theories were quite commonly mentioned during the discussion, such as phone listening. Mostly, the concerns were related to personal data breaches, the availability of information in Sweden, and privacy in social media platforms. However, during the discussion, many realized that companies may actually have a lot of information about them, making them discomforted with the idea of not knowing what information and which companies have been doing the collecting. One participant referred to a privacy scandal, in which a customer found out at the cashier that the grocery chain had collected much more information about him than they should have had, or what he thought they were able to do, since he had done some privacy settings to prevent this.

When the talk proceeded to data collection to online marketing personalization, many participants were indifferent towards the data companies collect from them to marketing purposes. For example, especially one participant claimed 'I don't have anything to hide' and 'if you want to know what underwear I have bought go ahead' with a dismissive tone. The system of targeted marketing was sawn almost as 'obtuse', a simple mechanism that based by online behavioral data targets the products that you have previously watched - the third party participation, segmentation, profiling, extensive data exchange and collection were not really considered during the discussion. However, although the personalization itself did not make them feel concerned, cross-device tracking and information sharing, such as your online behavior and information in online traveling booking websites can that spread to similar websites too, raised some confusion.

The majority had a neutral perspective towards personalization itself. It was emphasized, that there might be some benefits in targeted marketing when searching of something specific like beds in a foreign country, but on the other hand was perceived weird companies knew her customs and knowing too well what they wanted. Additionally, the timing and execution of personalization was highlighted as well, as getting commercials for a traveling location that was already visited an year ago did not feel so relevant anymore.

All of the participants of this group worked in the same company with the area of customer service. Therefore, due to their work, they had basic knowledge about the basics of GDPR and how to handle customer's personal data according to the regulation. Majority of the group

participants had been witnessing the enforcement of GDPR and how that impacted the company - as a result, the company had to change a lot how they worked with customer's personal data in everyday flow of work. Many felt, that yes, GDPR have made people more aware and interested towards their personal data, but also had a view that it is just a trendy phase of being conscious about it that may pass by as the regulation will stabilize its position in peoples everyday life. Additionally, the views about GDPR varied in between the participants, as one suspected, although GDPR had change a lot of how the company they work in handle data, that companies may still be sloppy with handling information. Whereas, other saw the companies and the digital world outside EU almost as wild west, giving a lot of value for the regulations power in protecting the citizens, for example in case of hackers.

In general, attitudes towards reading companies terms and conditions for data collecting and cookie policies were ignorant. Some acknowledged that it is too much of a work load to read the T&Cs and sometimes companies do not allow you to deny the use of the cookies, but otherwise the topic seemed not to be interesting. The emphasis in the privacy related discussion was mainly concentrated in how someone might abuse or access too easily to their contact information, such as address. The availability of personal contact information in Sweden was therefore perceived paradoxical in relation with GDPR. They questioned the role of regulation: what is the point of it if their information is being accessible anyhow? The group did little to enhance their privacy in online. Some mentioned having a private social media account or giving false information, such as the date of birth, to the companies.

Group 4 - The neutrals with demand for regulations

Group characteristics: International students studying in Sweden, majority marketing students

From all of the groups, these participants were the least concerned of personal data breaches or data collection in wider spectrum. However, the discussion was characterized by the ethics of the platforms that are run by algorithms and a view that regulations are needed for both making consumers aware of data collection, and how consumers should be protected from the attends of influence, such as in cases of political elections.

In regards of targeted marketing, the group saw some benefits in it and had neutral approach towards the practice. However, they questioned how personal the personalization system actually is, as they viewed targeting being based on your segmentation group and behavioral data. In fact, as well as in other groups, the targeting was sawn as clumsy, due to its prone to advertise you products that you have once bought or searched. One participant argued, that as fashion is all about fun, the personalization's constricted way of offering products selected by similar attributes make it less interesting.

Although the participants were not particularly worried about data collection, as the conversation proceeded, they started to think how the personalization and data collection is performed, they became more aware of the topic and realized how networked and complicated it actually is. The power of Google and its role for data collection through the

different functions (gmail, Google account, Chrome) was discussed – instead of being anxious regarding of this remark, they perceived that there is not much they can do to control how corporations with better resources can collect and use data.

Only one participant this group knew more about GDPR in detail – what does it mean in terms of obligations that companies must now face and the right consumer have gained. Regardless, this group was able to discuss about the regulation in general. They were aware that data collection have had a lot of negative attention in media, and therefore hold negative association, although all data collection is not done covertly or its usage is abused. The common opinion was, that the regulation was useful in a sense that it has made people more aware of the vast amount of information companies actually collect from them, and how companies now have more responsibilities towards the data they have harvested. On the other hand, they presented a critical view, questioning how much GDPR has influenced to the data collection in general and who is auditing that the companies actually comply with the regulation.

As the discussion proceeded to terms and conditions for data collection, the participants had a common view that they were too time consuming to read them, as well as using too complicated language making the comprehension of the text even more challenging. Although they perceived that consumers do have some responsibilities regarding of approving or disapproving data collection, currently, there might be too much of emphasis on consumer's own activity and cognitive abilities. Additionally, the cooperation with third party companies were argued to be difficult to understand from companies' T&C, and some argued that using complex legal text is used to confuse the consumer, in order to create loopholes for data collection and use. Many was not concerned about companies using cookies for collecting data from their website, since they thought that they are easy to delete from the computer afterwords.

Finally, although the overall tone of the discussion was objective with little personal concerns and emotion, one participant argued that the level of anxiety regarding of data collection and use may go hand in hand with how engaged and aware you are of technological devices. The participant stated, that it may be challenging to know how to enhance your online privacy, which can further influence on how safe or concerned you feel like. The others seemed more confident with their technical skills, although that had little impact to their willingness to enhance their privacy.

5.2. Individual views

Online personalization

Targeted marketing was sawn to be based by online behavioral data, such as searching and looking for specific product and then seeing commercials based on that online activity. Additionally, gender was perceived to influence to the content they faced in their own social media accounts, since many had experienced seeing ads for pregnancy tests. Although few had good comprehension about from what the system of personalization consist of, such as

the presence of Google and Facebook, the use of algorithms, and utilizing cookies for data collection – in general, it raised confusion. Especially the connection and cooperation between third parties and companies was thought to be ambiguous, as well as the ability for cross-device and platform tracking.

> *2E But do you know if like, because I know cookies are like gathered on your computer, because you can go into the settings and clear out the cookies, when you accept the cookies on one webpage, can they then see all of the information about the other cookies of you that you have in your computer? I'm trying to tell you that I don't even know what it means.*

> *4D When you read terms and conditions and such, they are always talking about this third party, which is not always clear what this third party actually is and complicated, and not really easy for people to know how much information they collect about us, and they will just get anything they get*

Many seemed to have quite neutral approach towards online marketing personalization: after all, it has been established already few years ago on social media platforms and consumers have had time to adjust to the idea. However, attitudes varied a lot from negative to positive ones among the participants. Some stated that they feel anxious about the commercials that are targeted for the individual, whereas others could see the usefulness of such practice in saving time and seeing more assortment from the specific product they were looking for.

> *Sometimes it makes sense, if you haven't bought the dress and they want to reminder you that it still exists so that you can buy it, but sometimes you have bought the dress and it still pops up as an example (2B).*

> *As being in foreign country and you don't know all of the assortment, it might be useful if you are buying something specific, like I have been buying a bed, and seeing offers in your feed. So it is much easier for the consumer in that sense that everything is "delivered" for you easily so it saves time since you don't have to search for the products. But on the other hand, it's sometimes distressing, like how do you know what I want and my customs (behavior). Depends on my need (3F).*

Additionally, although some argued that the targeting system can be sometimes impressive, as it was able to know such detailed information about the participant, its accuracy was questioned too. Perceiving the targeting system somehow 'clumsy' was popular view among the participants, whether it was expressed directly or implicitly – either the system should have know them better or offer more relevant content for you.

> *Sometimes I'm actually pretty impressed how detailed they can follow you, but then sometimes I'm also really disappointed because I'm think: "Hey Internet, you should know that I would never buy this" - so on the one hand it's super customized and on the other hand super random, so when you collect my data it would make so much more sense to enhance this or to give something that I'm interested in, because then it*

could even support you, even if you are not looking for it, you would be at least interested of it (2C).

Data collection and privacy

When asking what information companies collect from you, the majority mentioned age, gender, online searches, and visits in websites. Additionally, logging in a website and creating an account, were mentioned as one form of source. At this point, or later as the discussion proceeded, some argued that companies can collect basically anything they want. Emphasis was on data being collected from online environments, rather companies having the ”full picture” of you. Furthermore, the participants attitudes to data collection varied. On the other hand, many had views about data collection as a surveillance, since sometimes they had seen commercials that they could not identify in which information they had been based on. The network that collect and share information appeared as fuzzy, and it was unclear how the cooperation is performed among the members of the advertising exchange network, having a negative connotation in the participants' minds. However, controversially, many seemed to have an apathetic approach to data that is collected for targeted marketing purposes, although conspiracy theories were commonly mentioned during the discussion.

I have actually heard that in the supermarkets when you are walking and you have your phone with you, and this is just what I have heard so I'm not 100% sure, but that they have some frequencies in their speakers that reach the phone, so this is also if you buy sometimes, or when I have bought some specific yogurt, I then at some point I have ads from this brand in Instagram or Facebook, so I'm just like: how is this connected, I didn't search for it. And apparently this is what they do with those frequencies in a way that we don't hear it as a consumer. So this is also how they collect our phones and mobile devices with these speakers. I think this is one of the most scariest things what I don't like at all (2D).

The concerns towards data varied as well. Some were more disturbed by the thought that someone has access to their personal information (such as email and address), and thus abuse it for identity frauds, or companies may breach that sort of information to outsiders, as others had more emphasis on the view that you cannot really know what information companies have from you and how it is used. Additionally, few argued that they are not worried about data collecting in wider sense, since it concerns as all – we are in this together, and the collected information is not really used against you as an individual.

Well, but I have never given any information to the companies that I would be in some way secret, so I'm not that worried (3B).
Me neither, like you know what I shop, so what? (3D).

Many of the individuals came to the same conclusions as the conversation moved towards privacy: it does not exist anymore. However, instead of stating that with great deal of emotions, it was rather stated almost cynically – it is what it is and there is not much you can do about it. Consumer's responsibility in data collection was stated as well, but with different emphasis. The first group had a view that one should use common sense when sharing

personal information with unfamiliar or rather shady companies, minimizing the risk of getting scammed, whereas group number four also saw the consumers responsibility in reading companies terms and conditions for collecting data in their websites.

> *We have been raised to think that you should always read the terms before buying, if you make a mistake or a consumer does, so the procurers can say that you should have read it. In these things they always put pressure on consumers, so it gives a lot of responsibility to consumers, but maybe now it tries more to even it out and is more equal playing ground? And give more responsibility for the producers (4C).*

In general, privacy was seen challenging to enhance. Some listed going through their social media accounts, making them as private in their settings, deleting apps that may detect other apps on their phone or delimiting the app's access to other phone functions, such as microphone and address book, but facing a widespread system of information collecting network, many argued feeling powerless, and having lack of skills and knowledge in acknowledging how even to do it.

> *The thing is that this relates with your own interest and knowledge about this, because in everyday life we have other things to do, and all with this technology and terms & conditions, if you don't know so much about it or have an interest, you don't care so much. Maybe I worry a little bit, but what can I do? So I appreciate these talks, this makes me a awake little bit more what I do with my personal information (4A).*

GDPR

Clearly, those who knew the most about GDPR were people who had previous or current experience from customer service. Those people mostly knew what obligations companies have regarding of handling personal data and could list some rights that consumers have gained through the regulation. However, for the majority, the regulation was not familiar further than its aim for protecting consumer data. Additionally, those who knew GDPR previously through working with consumer data in customer service, did not link it to the wider spect of data collection.

General opinion seemed to be, that GDPR has influenced on how they collect and handle personal data. How much it has actually impacted to companies were argued from different perspectives, as the conversation around this topic proceeded and the critique of the impacts of the regulation were also visible. Who audits the companies so that they comply with regulation, and has it really changed how companies handle the data?

> *Not in specific terms, but be aware that this is going to be changed and this is how your privacy is now protected, so in general terms yes. But because of this change we are more aware of the right to deny them and also right to change our preferences. And a right to opt out of certain things, which we probably knew before but now we know how. So because of GDPR we are little bit more acknowledgeable in a sense,*

and we see that companies are implementing it with their privacy policies, it means that they are obligated to do it. So in both sides know their obligations and rights I guess (4C).

Although the participants were not sure the extend the regulation had influenced companies, many thought that it has made consumers more aware of the vast amount of information companies actually collect from them, that was previously made invisible for the consumers. Another view was, that after the regulation was enforced an year ago, many people are currently into securing their online privacy and want to know how companies handle their data, but as time will pass, bigger masses may loose their interest towards it.

Or at least to give their consent whether they allow businesses to use their data or not, it's acting like a gate way I think, like they open the door and businesses are coming, but that's the max I know, must be the tip of the iceberg (4C).

Terms & conditions and cookies

The discussion regarding of companies' terms and conditions for data collection on their websites and cookies was unified among all of the groups. All agreed, that companies use too complicated language in their terms so that they are difficult to understand and challenging to comprehend even after reading how the collected information is actually used. Additionally, they are inconvenient and time-consuming to read, as they are consisting of many pages that may be exhausting to fully go through. Some argued, that companies use formal language to confuse consumers on purpose.

But then again who reads those fine prints anymore? No one does, so you can write anything in there, and I think the agreement is written by purpose like that, so you can interpret in any way (4E).

Finally, the groups touched the topic related to cookies, either by their own initiative or the administrator of the focus group directly asked about it. All had noticed how complicated it sometimes is to deny them, as some websites has made it impossible to access them without accepting the cookies. Some found this annoying and felt, maybe with good reason, that companies do this intentionally. By convenience, as many perceived, they are easy to be ignored as one want to browse Internet smoothly.

And out of convenience for sure. Sometimes you are just way too lazy to read and all this. As you said before, sometimes you are more dedicated to your own safety and your own concerns. But yeah, I think the most of our decisions are based on convenience: so if it's easy to click huge big button of 'accept', so you just go there in stead of searching for the little small exit, disagree button or whatever (2D).

6. Analysis

The analysis will focus on explaining why the participants felt and answered certain way regarding of data collection, online marketing personalization, and GDPR. This section is divided into two themes, that had the most emphasis during the discussions: firstly, the analysis will explain *the power imbalance* with the information asymmetry approach; and secondly, explaining *enhancing privacy – and the lack of it* using the concept of privacy paradox as a theoretical reference.

6.1. The power imbalance

The lack of control and a feeling of being under a surveillance was mentioned several times during the discussions. In fact, as this was broad up repeatedly in all four focus groups, it emerged to become one of the major emphasis in the analysis. Since the information asymmetry is structural (Hull 2015) and thus, acts as a default setting in consumer-company-third party (advertisement network) relationship, the analysis of the focus group discussions is centralized more with the approach of how such imbalance will impact the consumers, as well as to their thoughts and feelings. Hence, the emphasis will be on the outcome of the information and power asymmetry between the stakeholders.

There were multiple data points from which this theme was composed: the awareness of the power that big corporations have on online environments, the feeling of someone following our movements and tracking your, the uncertainty of who has collected your information and what that information is, conspiracy theories about someone spying on you through microphone or camera, and the lack of control in resisting data collection and usage activities by companies and third parties:

> *It Sounds like it can be definitely possible (when speaking of cookies). They have so many systems that they can just track everything that you do, and also in depended on their own website, I think as soon as they gone onboard with you, they will be on your back, and you will just carry them around like a backpack where ever you go (2D).*

Perhaps due to the media attention Facebook has lately received, the company's name was articulated severally. This was usually either done with criticism or expressing lack of control in intervening to data collection they and other big online corporations do, as the participants shared the mutual feeling that it was really out of their hands if companies want to target you or utilize your data. Thus, they perceived that there is not much you can do in order to stop them, they know already or will find a way to do so, you are exposed and cannot hide:

> *Facebook knows anyhow what you do and they are doing financially so well with the data they monetize. Once you put some information online you will never get it out (1D).*

Sometimes I expect that, I don't have to care anyhow, because you know everything already, or if they would find something out or they want to know something - they would do it anyhow. So that's why I'm like "ok, I don't have to care" (2C).

But at the moment I feel nothing is a secret, you can't hide (4B).

As the discussion proceeded, many seemed to understand that it is challenging to know which companies have information from you, what that information consists of, and how it has been collected. This information asymmetry was discovered in different ways in the participants' daily lives: after buying a holiday trip seeing ads about the same destination popping out on the other online travel booking website; receiving a contact from a company in a situation that was out of context; finding out that companies know much more information about you than expect based on the information you have decided to disclose; and through the received targeted advertising, realizing that your information has been collected and used without your control:

An additional thought that I have is that companies collect so much of data, or other parties, and the some they don't even use, but they collect so much of data that some of that data you don't even know what it is, and they might not know what it is but they still have it. So you have all this data about me but I don't know how you are going to use it. For me that's is a bit scary, because they have collected all these things about you, and you are just "I don't know I'm just going to get some personalization services" (2B).

Local newspaper got in touch with me and asked if I wanted to have my birthday announcement in their paper, although I never been their client before. That made me realize how much companies share the data between them and how much they actually sell that forward to other companies (3F).

That's also strange, when you think about Momondo and other traveling booking websites, if I have search something in there I might ran to some offers regarding of my search in other similar platforms (3D).

This emerged mostly, not perhaps surprisingly, negative emotions: mistrust, anxiety, and discomfort. Many appeared to think, that if they know this about me, what other things they have collected without my awareness? Thus, the participants did not have much against data collection or personalized advertisement per se, it was in fact sometimes perceived as useful, but the lack of transparency about the targeting and the usage of that data were seen as problematic, what has been collected, why and for which purpose:

Sometimes I feel anxious by the fact how much they know (3C).

I would not have a problem of sharing a lot of things, because at the end I don't care, so I wouldn't have the problem, but you just don't know what they collect (2C).

There is a lot secretes behind it, it's so non-transparent, you don't really know exactly what they are aiming for, would be nice to know their motives, and then everything would be much more trustworthy (2D).

The connection between different platforms and devices was also considered as disturbing, such as, after searching for a certain product with Google coming across targeted ads on the phone about previously looked equal item. This cross-device tracking and hyper-connectivity, the tracking and following your movements, raised negative feelings among the participants:

Noticed it at the first time when I was looking for Masters, because then on Instagram schools were coming up and really shocked about that, so some private schools advertise completely through Instagram. So it was interested on how they found out, but of course I was googling schools with Master's degree and Swedish Schools of Textiles (2C).
This is how you then connect your movements and your computer. And this is also really scary that those different channels are inter-aligned and they work together (2D).
As you guys mentioned, sometimes when I'm at my computer, what I have looked up comes as an advertisement in my phone. I'm not sure if I like that, I find it weird that they know that this is my computer and this is my phone (2B).

It was really spooky when one of our work colleague was searching some product with our work computer to our customer and then ran into the same product in her Facebook feed on her phone. How was that possible? That was weird (3B).

Inevitably, this omnipotence was be questioned, and thus, explained with different theories about surveillance and spying. The intangible data distribution and exchange network can easily appear as mysterious, since it does not have many channels to reach consumers, but rather operates back scene. During the discussions, many participants explained a situation in which they did not recognize the information that had been used for the commercial they had seen. For example, after visiting a certain brand's website receiving their ads in another online environment, such as in Facebook. Since in most of the cases personalized advertisement is based on behavioral information that online users produce in their daily basis, when confronted with advertisement that they could not logically reason how the personalization for them was performed, many conspiracy theories were broad up to explain this irrationalness. Thus, due to structural information and power asymmetry between consumers and companies, conspiracy theories about surveillance have fruitful ground to grow. As it was highlighted in one participant's comment, instead of considering the fact that the supermarket might sell consumer's purchase history from that shop to another company that utilizes this information for targeted marketing, this theory about frequency-collecting and phone-reaching speakers was shared with others:

I have actually heard that in the supermarkets when you are walking and you have your phone with you, and this is just what I have heard so I'm not 100% sure, but that they have some frequencies in their speakers that reach the phone, so this is also if you buy sometimes, or when I have bought some specific yogurt, I then at some point

I have ads from this brand in Instagram or Facebook, so I'm just like: how is this connected, I didn't search for it. And apparently this is what they do with those frequencies in a way that we don't hear it as a consumer. So this is also how they collect our phones and mobile devices with these speakers. I think this is one of the most scariest things what I don't like at all (2D).

Additionally, Phone listening seemed to be the most popular explanation for covert information collection:

But have you noticed that phones are listening to you? Because sometimes you see ads from companies you have not googled, so it can't be based on something I have searched online (1D).

I also think keywords are important (when speaking of targeting) or like a big thing, because I have heard of, that if you sit in a room phone next to you and you talk about dog food with your friends for a while, then the phone kind of picks up like what you are talking about, and those are the keywords I guess that are gathered and add even never searching online (2E).

Yack listening is the worst! You has the experience with the recording right? (3B).

The advertisement exchange and network running behind the personalization can be challenging to observe for a regular consumer, since many of their functions are intangible. Therefore, their participation in the personalization process may become as a surprise for the consumer, or as found out from the focus groups, the missing link is between the seen personalized advertisement and the information that the commercial is perceived been based on is explained with conspiracy theories about surveillance. Thus, this is major consequence of the both intentional and unplanned secrecy that the system behind the personalization is shrouded with.

In general, how much your movements are followed (3F)?

I think I'm more concerned, like I don't mind this whole: "what is she searching for, what web stores I go into, if I'm a member", that doesn't concern me that much. The thing I'm more scared of is the camera and the microphone in my devices, how they are used and entered without me knowing (2E).
Things that you can't control (2C).

It can be argued, that looking from the perspective of information asymmetry on how the respondents perceived data collection and personalization, the imbalance between consumers and companies had major consequences: mistrust, lack of control in how information about you has been collected and used, the feeling of being under surveillance, confusion regarding of the advertisement system, and discomfort when facing a situation where you are unaware of what and who have data about you. The information asymmetry can create and maintain major power imbalance between consumers, companies and third party data intermediates (Stevenson 2016).

As the respondent described, they cannot really influence whether or not information is collected from them. The unbalance was seen unfair, but transparency towards personalization and more openness for data collection and use was seen as a solution:

> *Maybe it would be nice if they would be obvious like: "we collect your data because we want to help you support in your search", and then it would feel so much more genuine, and think: "ok they know about me and this is why it fits so perfectly" (2D).*

6.2. Enhancing of privacy - and the lack of it

The participants' thoughts about the policies through which companies inform consumers about the data collection were solid – everyone agreed that they are time-consuming, inconvenient, and possess language that is challenging to fully comprehend, leaving room for misunderstanding and interpretations:

> *So when you read terms and conditions and stuff, they are always talking about this third party, but it is not always clear what this third party actually is, it's complicated, and not really easy for a regular people to know how much information they collect about us, and I think they will get just anything they get (4D).*

> *I don't know exactly how it is, but many companies the text is so long. I don't know if they have it purposefully or are they formal due for the regulation, but because they are so long, as a consumer, you don't really read everything (2B).*

Thus, if consumers do not understand the information regarding of data collection and usage, or that content do not reach them due to other reasons, the personalized advertisement system can be even more trickier to picture than it already is. Whether the poorly-acknowledged consumers are to be blamed because of the companies or the consumers themselves, incomplete information can affect to the decision making about disclosing information (Barth and de Jones 2017).

After GDPR has been enforced, that companies must inform the user about the data collection and use when users enter their websites, as well as gain their consent for it. But as it was mentioned many times in the focus groups, accepting the cookies that collect the user data or agreeing with the privacy policies has become a habit – or a forced one in the absent of clear playing rules. Giving a consent may be arbitrary, as in some cases the user is forced to accept the cookies or the content in the website is not accessible, or they do not have the control to deny them due to other reasons. Therefore, the permission to collect the and use data may remain as vague, as in reality the consumer may not be aware where they actually have signed up to:

> *But the language is usually really formal. So you read through and ugh…but of course I understand if it's on purpose, because they know that consumers want to save time and just go through and click (2C).*

But the problem is that we never as consumers read those things, only after those things have happened, after that you start reading about your rights, that's the issue. Briefly, we know a little what it is but in practice and detail we don't - we just click around and accept and that's it (4B).

Van Ooijen and Vrabec (2019) express their concern how easily consumers give their consent to websites privacy policies, since the nature of their consent can be imprudent, as it can be easily given whenever they confront a request, without any conscious thinking. Therefore, it may be challenging to enhance one's privacy, especially when there is lack of required information and skills to do so. Moreover, the focus group discussions emphasized, the decision to accept or decline cookies may be arbitrary, and more connected to the current mood, feeling and trust you have towards the visited website or online service - the opposite to the behavioral and economical approach of rational decision-maker (Kokolakis 2017). As many of the modern social and everyday life currently take place online, it is unrealistic to demand the consumer to read cookie policies and terms and conditions each time they enter a new website or online service platform. Van Ooijen and Vrabec state (2019) in their article that in addition to the fact that it takes several hours to read them, many consumers may not possess enough cognitive skills to fully understand them. One study estimated, that reading through once all the privacy policies from the websites they visit would yearly take more than six work-weeks work to execute (Hull 2015). Therefore, they cannot know what they sign up for, although, technically they have accepted the terms by clicking a little consent button on the website. The participants themselves admitted, that usually their decision-making regarding for enhancing their privacy was prone to changes in their mood and feelings:

I think with cookies, I sometimes in certain webpages and certain days be like "Accept!", I just want to see my page (2E).
Hah yes, that's me (2B)!
And then other times with other webpages, if I'm in specific another mood on that day I'll be like "Umm, where is the cancellation button, I don't want to accept this" (2E).
So true (2B)!

And out of convenience for sure. Sometimes you are just way too lazy to read and all this. As you said before, sometimes you are more dedicated to your own safety and your own concerns. But yeah, I think the most of our decisions are based on convenience: so if it's easy to click huge big button of 'accept', so you just go there in stead of searching for the little small exit, disagree button or whatever (2D).

But the thing is, what you 2E said, is that it also depends what kind of website it is, if I'm familiar with this page or if I'm just in a rush, just want to get things over with or if I really want to see something - sometimes you don't even read, you just click. But if it's something unfamiliar, you want to read and be sure what you have signed up for basically. For me that's how it is (2B).

Some participants expressed that their level of knowledge regarding of privacy was not the highest. In fact, many did not know how to protect their own privacy or personal information

systematically. The actions for enhancing privacy or personal information were not completely absent, but the overall tone of voice was confusion:

> *I actually wouldn't know what to do. That's the thing, I think you have something here with transparency, because I have no idea where they find my information, where it's pulled from, how it's stored, do they…so I wouldn't know where to go to combat, for having more privacy, or like the opposite, the breach of my privacy (2E).*

Additionally, the calculus between the privacy risk and gained benefits may be challenged as well. Kokolakis (2017) states, that especially time-wise people tend to value shirt term advantage, such as accessing a website, over possible risk in future, such as disclosing information. Furthermore, as it was present in the talks, the willingness to implement privacy-enhancing strategies may be low, since their effectiveness of such investment may be questionable. Hence, as previously mentioned, the lack of individual privacy protection may be due to the feeling that *they* can do whatever they want, and you cannot really control them:

> *In general I'm not too worried, I'm personally quite sure that my data is used in more general manner, and if someone really want to target me, in Instagram or Facebook, they probably can do it with their resources I really have nothing I can do (4E).*

Interestingly, conspiracy theories and doubting companies motives reached this area of the conversation as well, since it was argued, that companies have misleading privacy policies and arbitrary cookie collection systems by purpose. Inevitably, this influenced to participants attitude towards data collection:

> *The thing is that sometimes they hide it so strategically or attentional, so it' hard for you to see as a viewer, it might be somewhere in the corner perhaps, but you don't see it then (2D).*
> *Even like it do not exist but then you can click the side of the page (2E).*
> *They have their methods for sure (2D).*
> *Yeah, I guess that's also a thing gathering information about you, like private people, that you make it so, that it doesn't seem that you do, you know, so they exploit your un-informativeness. It's like lack of knowledge (2E).*
> *And taking advantage of it (2B).*

7. Discussion

In this section the outcome of the analysis, the consumer reasoning and thoughts behind the information asymmetry and privacy paradox, will be overviewed and discussed in relation with the advertisement exchange network and GDPR.

The mysterious and opaque advertisement network

Being observed at some extent on online environments may not come as a surprise for many. However, the amount and detail of data that can be collected from the individuals, such as: (1)

product and service data of last purchases, future purchases, type of product/service (food, apparel), location of purchase and category of stores; (2) *network, application and decide data*, such as laptop versus smartphone device, wifi versus mobile phone data, web browser, operating system, phone model and installed apps; (3) *activity data*, such as ideology, charity donations and leisure activities; with (4) *additional data features,* such as individual versus household data and modifiers (what has been searched and watched) (Stevenson 2016) surely can be. This information combined with the consumer and non-consumer facing advertisement and data exchange network of data collectors, internet behavior monitors, third party data brokers with the digital marketing supply chain that act together in the complex and hyper-connected personalization production, truly challenge the understanding of average consumer.

The contrast between what the process and participants of the personalization actually is versus what the focus groups participants emphasized in their answers seemed to be great. It was shown in the analysis, that one way of explaining why companies sometimes knew and had the ability to target them so well were conspiracy theories about surveillance. This was interesting and perhaps a natural reaction towards something that you do not fully comprehend. Additionally, many participants were not worried about personalized advertisement per se, but spooked about the outcome of the information and power asymmetry, not knowing who had collected information about them and for which purpose it was going to be used. Thus, the link between these two, receiving targeted advertisements and the widespread data harvesting and utilization, was missing. In order to fill the gaps in the story, and perhaps due to some urban legends, conspiracy theories were used and they had fruitful ground to grow. Among the negative feelings that the structural information and power asymmetry awoke, this was the most major consequence of the opaque advertisement and data exchange network which efforts is incarnated in the targeted commercials. These ads easily become the only data point for the consumer to perceive what information companies have collected about them in the seamless personalization network.

The problem with personalization

As we have seen from the result and analysis, the problem was not personalization itself, but how it was performed. Here lays the paradox - in order to receive relevant content, companies needs to know the consumers, but as it was clearly demonstrated in the focus groups, many was not fully on board with the thought that companies know more about them that they felt comfortable with. Additionally, since the collected information is concretized to the consumers through targeted marketing, the moment when they can see their information in that context that was not expected to be seen, they may experience discomfort as the commercial may be based on misused personal information, and further rase questions of the source of such data.

The process of personalization consist of the stages of data collection, analysis and processing, segmentation, and targeting through various of advertising strategies. All these stages can be go through with third party cooperation, especially at the last phase, where the actual advertisement is performed. Although the use of behavioral data may be obvious for the consumers, but other parts of the personalization may remain as hidden. In addition to not

knowing what information companies have from us, the data analysis and used algorithms are trade secrets, it may be challenging to know in which segment(s) you are placed in, how much the companies do cooperate with third party companies, from which sources companies collect information about you - from which articles you are constituted in their eyes. Therefore, the results from the focus groups were not perhaps surprising. The feeling of surveillance was present as the participant exchanged their thoughts regarding of conspiracy theories and experiences about been 'watched'. Connecting monitoring with economy is not completely a new idea. Zuboff (2015) has in fact introduced a term surveillance capitalism to describe the vast information collection of consumer data run by big corporations in online environments, that is further utilized and monetized exploiting consumers privacy. Thus, the knowledge and power are asymmetrical in the hands of small number of online companies, retailers, and data brokers (Cinnamon 2017).

Since this advertisement network is most of the time invisible and intangible for the consumer and there is lack of transparency about what consumer's information is used for the targeted content they receive. Because consumers are unable to identify how, when, and for which purpose the data has been collected, they may feel that they have been under surveillance, emerging disconfirming emotions among them. One way to tackle the mistrust could be for companies to be more open about the data collection and transparent about their actions.

Why consumers disclose information? Why they do little or do not enhance their privacy?

According to the results, which were aligned the privacy paradox concept, some participants expressed to be highly concerned towards privacy, but they did little actions to enhance it. Another line was not to be concerned regarding of data collection, the abuse of their personal information or frighten towards their own privacy, and the participants who declared this had little attraction to privacy enhancing strategies as well. Although the reasons why the latent group felt unharmed by the data collection could be many, the analysis focused on the view in which the attitudes were effected by privacy paradox- either you feel powerless but do little or careless and enhance privacy as much as the concerned ones, little. Concerns towards one's privacy were usually connected with personal experiences about the abuse of personal information by a third party or unpleasant memories about information asymmetry situations, such as a person using your email for creating an account for online service or a company reaching you out of context.

The participants were united with the view that companies privacy policies are too laborious to read and challenging to fully understand. Additionally, it was admitted that going through privacy and cookie settings when ever entering a new website was nonexistent, since due to convenience, you just want to see the content in that platform, rather than investing time and effort for such activities - as it was mentioned, you easily just click around without any deeper and mindful consideration. Daily, we visit countless of websites and therefore, investing time or energy for investigating each site's privacy policy or how they collect information may be a lot to ask for. It is easier to disclose information for short-time reward and ignore privacy in a long-term. In fact, many participant emphasized that a lot of their privacy enhancing actions were depending on their mood and feeling of the day, making decision-making arbitrary.

Finally, privacy protection may not be active due to the unawareness and lack of related skills, or as individual consumer may have little or nonexistent power to truly control there data over big corporations, the willingness to take actions to protect privacy may be low if the impact of such effort is nonexistent or insignificant. In total, many possible reasons seemed to play a role in why enhancing privacy is either challenging or non-rewarding, explaining the absent of the behavior which would be more align with the concerns and feelings that arise from the discussions as a reaction to information and power asymmetry conditions.

Nevertheless the difference between these attitudes, in the advent of big data era, it can truly be challenging, or laborious to control how your data is collected and used, as it has been made impossible to isolate yourself fully from the online platforms and services. Privacy might be increasingly be sacrificed intensionally and unintentionally as interactions on and with online have conquered our lives. However, the question remains: would consumers be more proactive towards their privacy and personal data if they would acknowledge the presence of third party companies, the exchange of information that the advertisement network actively does, and how complex the process of personalization actually is?

Informing consumers about data collection, GDPR and privacy paradox

Finally, we discuss what the empirical findings and analysis mean in relation with GDPR, and further, what challenges the regulation may hold from the consumer perspective. Based on the given focus group answers, it can be argued that still after one year the regulation was enforced, GDPR has remain as a abstract concept for consumers. The participants who were familiar with the regulation in some extent gave the examples of the regulation mainly from a employee perspective, rather than linking GDPR with themselves or to data collection and privacy rights.

Due to GDPR, companies are required to inform website users about data collection and have their consent for it as well. This is performed through cookie policies - users must physically press an ’accept’ button for approving the data collection. Additionally, companies must provide an explanation for how that data is used, which is usually informed either via the cookie pop up or in companies privacy policy section in their websites. However, as it was found from the focus groups, these informative policies are not currently working as they should - informing consumers. Biased or non-existing risk-benefit calculation cannot directly be argued to be existing in how consumers comprehend companies’ data collection through the empirical data, since more structured and quantitative approach may be required for such statements. However, the paper is able to offer, through the focus group discussions, the reasons and insights about why the participants felt challenging to fully picture the extend of the data collection that companies practice.

As earlier discussed and explored, it is difficult for consumers to comprehend the content in the terms and conditions, and due to inconvenience, often do not bother to read them. Firstly focusing in companies terms and conditions for data collection from biased risk-benefit calculation perspective, many focus group respondents argued that these privacy policies are challenging for them to understand – their complex and legal tone of language was considered as arduous to read through. They explained that due to convenience, the website cookies are

easier to accept without further investigation where the collected information is used. Occasionally, as the participants explained, it's not even possible to enter the website without accepting the cookies first or the pop up window for cookies will vanish quickly after entering the site. Since it was to much of an effort to go through the companies policy for data collection and the purpose of it and many accept cookies by default out of convenience, the participants risk-benefit calculation may be biased that may further influence their capability to fully evaluate the risk that may be included in disclosing information. Another important point is consumers' consent, or how easily it is given without fully being aware of what it actually means. Since the given consent may be more formal than factual, consumers may not perceive have given the permission for the data collection in the first place, although from the company and third party perspective they have. This can also have n impact tot he feeling that your personal information has been used without your permission. Privacy self-regulation relies on transparency and control, thus in consent and the ability to be informed (Acquisti et al. 2016). Therefore, since both seems to be hindered due to the previous mentioned reasons and also found in other empirical research, having too much emphasis on consumers' ability for self-regulation may challenging to overcome (ibid.).

Another view is, that the networked system behind the data collection, that includes vast amount of different stakeholders, has remain abstract to average consumer. Even for marketing students taking part of this study the third party role seemed to appear as vague – even after reading terms and conditions, the actual context of that collected data use may remain blurry. Further, although consumers may be able to understand the first hand data usage for personalization, other type of use, storage, selling, sharing, analysis, and processing, either in that company's hand on with other party's, might be too challenging to consumers to picture. Therefore, this information asymmetry, lack of knowledge of the extend data is actually collected and use, may impact to consumers ability to evaluate to possible risks that are present when they allow their data to be collected and used. Hull (2015) argue, that the since the problem in information asymmetry is structural, informing consumers with better privacy policies cannot be seen as a solution, as well as relying on consumer's consent, when at the moment the agreement from the consumer's behalf is given, the use and outcome of data mining is unknowable for both, companies and consumers. Thus, performing a risk assessment is impossible, since the conditions under the decision making are uncertain (ibid.).

Due to GDPR, companies are obligated to handle consumer information according to certain standards and receive a consent for collecting their data. Additionally, consumers have been bestowed with rights over their own data, such as right to be informed its collection and usage, right to access, right to be forgotten, right to object processing, and rights regards of being profiled at. Thus, as we could see from the results, consumers may give their consent without fully understanding what they are consenting for, and this regulation's and companies' emphasis on privacy self-management can therefore be problematic from the consumer perspective. As we also discovered from the results, the regulation is still ambiguous for many. This can also hinder consumer's ability to enhance their privacy, as they are not aware of the rights over their data and privacy.

As Nissenbaum (2017) argues, current regulations and approaches for controlling and limiting the collection of personal data rather than its usage, has become obsolete and impractical for

the individual perspective. The question remains, how data protection can meet the challenges that emerge from the decision-making itself, that is the outcome of large-scale, complex, and multi-purpose processes of matching and mining enormous amounts of data, as different intermediaries that take part in distributing, sharing, disseminating and disclosing the data as it is bought, exchanged or given (ibid.). Therefore, since GDPR will not intervene in arrangements for data collection and processing that have been agreed upon or granted through consent, it does not protect the individual from *impacts* of the generalized environment of data collection (Couldry and Yu 2018).

Getting the know-how for protect their privacy requires skills, effort and time. Although in some cases one is committed in protecting their own privacy and restrict data collection, when we look the realities in how data collection, processing and use is performed in highly networked and complex structures, the task may appear impossible. Online environments are mostly the playground of big players, such as Google and Facebook, and it may not be realistic to use online platforms or social media services without interacting with these corporations. Thus, individuals are forced to take part in the platforms that exploit their privacy. GDPR has contributed in stronger protection of the data itself; how it is protected by data breaches and third party attacks, and setting policy for how and how long it is stored, which are is huge achievement for setting up common rules for the EU region, giving consumers rights, and improving data security But as discussed earlier, the GDPR's main idea of protecting the data subjects may remain weak.

The fuzz with privacy?

Is the topic of data and online privacy making a hustle out of nothing? Maybe, as many companies are small or they do not yet possess the resources to invest in such technologies and tactics that may be invasive. But as the world continues to develop towards big data, hyper-connectivity and Internet of Things, the questions regarding of consumer rights in relation with data collection, usage and privacy are going to be even more current. Additionally, the leaps in marketing technology raise similar questions, such as if firms start to look at the consumer behavior dataset to identify vulnerabilities for persuasion profiling in order to categorize individuals based on their triggers (Calo 2014).

The clothing view

Personalization is increasingly becoming more used in the clothing industry. Therefore, in order to gain consumers' trust and acceptance for personalization services, the questions regarding of privacy, data collection and its usage should be considered in this sector as well. Firstly, companies should be clear in their communication about personalization, since as it came obvious from the results, if consumers do not know for what the personalization is based on, thus, what information has been used for such adjustment, the negative consequences may overcome the positive ones. Secondly, compared to other fields, fashion is run by exclusivity and branding. As many of the current personalization is focusing on offering products that the consumer has previously searched for, their effectiveness for fashion products could be questioned. In order to keep the magic of fashion, the fun of it as one of the focus group participant mentioned, clothing companies may have to consider other

more exclusive marketing strategies than just relying on offering previously looked items for the consumer. In fact, personalization and individuality could not be more far than that.

8. Conclusions

The research question for this research was:

How consumers view GDPR, data collection and online marketing personalization?

According to the received answers, GDPR has still remained an abstract concept for many, thus, many respondents did not either know much about the regulation, what rights they have as data subjects, nor how the regulation is linked with privacy enhancing strategies. A controversiality between GDPR's, companies' and consumers' view on privacy self-management is evident, as the regulation and companies rely too much on consumer's own responsibility, which they do not take due the reasons that were discovered.

Data collection and utilization emerged variety of contrasting feelings. The main channel for companies to inform consumers about their privacy policy is terms and conditions. However, due to many reasons, the decision making for one's privacy face many hinders, that may influence in how consumers perceive their privacy and how their personal data is collected and used. The given consent may be more formal than factual, thus, consumers do not perceive have given the permission for the data collection in the first place.

Additionally, as an outcome of information asymmetry, on opposite to GDPR principles, many participants experienced challenging to know what, how, by whom and where their information has being collected to, leading to empowerment. It was perceived, that gaining control over their own data was impossible – on the other hand, information asymmetry has lead some to have biased, positive comprehension for that control as well, which may turn out to be unfeasible in the advent of big data and extensive data collection and advertisement exchange network. As using online platforms and services has become a essential part of our everyday life, having their privacy as a commercial good was and was not recognized.

As previous research has observed, consumers do not mind disclosing personal information, if they perceive that they receive personalized or relevant content, which was also aligned with the focus group findings. However, the way in which personalization and data collection was performed by the companies caused the feelings of discomfort among the participants – in fact, the analysis showed that due to the information asymmetry between the companies and consumers, those practices were seen as intrusive. Since the advertisement network appeared to be opaque for the focus group participants, and thus impossible to understand, personalization was connected with conspiracy theories and surveillance.

The fashion industry cannot either dismiss the demand for transparency or consumer's feelings – as companies have the ability to become more closer to the consumer, such as in conversational commerce to reach consumers through their private messaging on Facebook or Instagram, it may be important to proceed according to consumer's terms in order to avoid the

negative consequences that personalization may cause (Lieber 2019A). Moreover, a good question to consider for fashion marketers is to consider different targeting and personalization solutions than other industries are using – in addition that aggressive targeting strategy can be perceived as too pushy, relying too much personalization with behavioral data may lead to fashion's lost in magic and the targeting overload may badly executed in fact hurt the brand more than benefit (Lieber 2019B).

The intrusive nature of the personalization practices made the participants, directly or indirectly, reluctant towards it, as it was highlighted that it is not personalization per se that made the respondents uncomfortable, but *how* it was done. Thus, marketers might have to think new solutions and strategies to reach their audiences, if the negative outcomes are greater than the positive ones. Additionally, the current way of informing consumers regarding of data collection and privacy policies with terms and conditions seems to have hinders – both from the consumer and company sides. Therefore, new ways to increase transparency and openness could be welcomed.

Limitations and future ideas for research

GDPR is a 261 pages long regulation, consisting of 99 directives with additional 173 legal preliminary statements, that address the fundamental changes of the complex, digitally-driven society (Axinte et al. 2018). Therefore, due to the lack of legal acknowledgement, instead of focusing to the legal side of GDPR, this paper will only discuss the regulation in general manner and the consumer view of it. Thus, this study will go through the regulation by its most important aspects from the consumer perspective: in addition to the obligations companies hold and the rights consumers are justified, GDPR's contribution to privacy, transparency, and control will be covered.

Despite the fact that GDPR is a regulation instead of directive, therefore lawful for EU members or any third party company that do business in EU, we still know little how much GDPR has actually influenced companies and online privacy. In paper, the regulation is really ambitious and demanding. But how effective it has actually been will still remain as unknown – although we understand how it should work, but as this thesis has tried to emphasize, there is no evidence how well companies follow it or of its influence to online privacy. Therefore, future research should map how companies have actually implemented the regulation and what how GDPR had influenced to their data collection, usage, processing, third party cooperation or to other activities.

The age of the participants was between 22-32 and majority had a higher education degree, so the results of this study cannot be generalized to present wider population. Additionally, as the majority of the focus group participants were women, the gender division was unbalanced. However, if this part of the society, young and educated, do not know their rights or take actions to enhance their online privacy, how can people in much weaker position and less knowledge to do so?

References

Acquisti, A. and Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, 3(1), pp.26-33.

Acquisti, A., Taylor, C. and Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), pp.442-492.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K. and 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), pp.34-49.

Alemany Oliver, M. and Vayre, J. (2015). Big data and the future of knowledge production in marketing research: Ethics, digital traces, and abductive reasoning. *Journal of Marketing Analytics*, 3(1), pp.5-13.

Ashdown, S. and Loker, S. (2010). Mass-customized Target Market Sizing: Extending the Sizing Paradigm for Improved Apparel Fit. *Fashion Practice*, 2(2), pp.147-173.
Aslam, B. and Karjaluoto, H. (2017). Digital advertising around paid spaces, E-advertising industry's revenue engine: A review and research agenda. *Telematics and Informatics*, 34(8), pp.1650-1662.

Axinte, S-D., Petrica, G. and Bacivarov I. (2018). GDPR Impact on Company Management and Processed Data. *Access to Success,* 19(165), pp. 150-153.

Baek, T. and Morimoto, M. (2012). Stay Away From Me. *Journal of Advertising*, 41(1), pp. 59-76.

Barocas, S. (2014). Data mining and the discourse on discrimination. Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining, New York, NY.

Barth, S. and de Jong, M. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), pp.1038-1058.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, pp. 419-426.

Bryman, A. and Bell, E. (2015). *Business research methods*. 4th ed. Johanneshov: MTM, pp. 512 -517.

BoF Team and McKinsey & Company (2018). *Fashion in 2018 | 04. Getting Personal*. [online] The Business of Fashion. Available at: https://www.businessoffashion.com/articles/intelligence/top-industry-trends-2018-4-getting-personal [Accessed 12 Aug. 2019].

Brito, P., Soares, C., Almeida, S., Monte, A. and Byvoet, M. (2015). Customer segmentation in a large database of an online customized fashion business. *Robotics and Computer-Integrated Manufacturing*, 36, pp.93-100.

Burri, M. and Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 6, pp.479-511.

Calo, R. (2014). Digital Market Manipulation, *George Washington Law Review*. 82(4), 995-1051.

Chen, C. (2018). *How to Tackle Fashion's Tech Deficit? Hire the Right People*. [online] The Business of Fashion. Available at: https://www.businessoffashion.com/articles/professional/how-to-tackle-fashions-tech-deficit-hire-theright- people [Accessed 12 Aug. 2019].

Couldry, N. and Yu, J. (2018). Deconstructing datafication's brave new world. *New Media & Society*, 20(12), pp.4473-4491.

Cinnamon, J. (2017). Social Injustice in Surveillance Capitalism. *Surveillance & Society*, 15(5), pp.609-625.

Danna, A. and Gandy, O (2002). All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. *Journal of Business Ethics,* 40, pp. 373–386.

Degeling, M. and Nierhoff, J. (2018). Tracking and Tricking a Profiler. Proceedings of the 2018 Workshop on Privacy in the Electronic Society - WPES'18.

Deuker, A. (2010). Privacy and identity management for life. Berlin: Springer.
Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2), pp.89-101.

Dewar, K. (2017). The value exchange: Generating trust in the digital world. *Business Information Review*, 34(2), pp.96-100.

Dipayan, G. (2018). *How GDPR Will Transform Digital Marketing*. [online] Harvard Business Review. Available at: https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing [Accessed 18 Mar. 2019].

DMA. (2018). *GDPR for marketers: The essentials*. [online] Available at: https://dma.org.uk/uploads/misc/5a8eea20f3566-gdpr-essentials-for-marketers----an-introduction-to-the-gdpr-amendment-v1_5a8eea20f34aa.pdf [Accessed 18 Mar. 2019].

DMA. (2019). Martech 2019: Marketing technology shows no sign of slowing down in Northern Europe | DMA | Research | Martech 2019: Marketing technology shows no sign of

slowing down in Northern Europe. [online] Available at: https://dma.org.uk/research/martech-2019-marketing-technology-shows-no-sign-of-slowing-down-in-northern-europe [Accessed 18 Mar. 2019].

Fitizzy (2019). *About us | Fitizzy*. [online] Fitizzy.com. Available at: https://www.fitizzy.com/en/about-us/ [Accessed 12 Aug. 2019].

Gironda, J. and Korgaonkar, P. (2018). iSpy? Tailored versus Invasive Ads and Consumers' Perceptions of Personalized Advertising. *Electronic Commerce Research and Applications*, 29, pp.64-77.

Gitelman, L. (2013). *Raw data is an oxymoron*. 1st ed. Cambridge: The MIT Press.

Grindrod, P. (2016). Beyond privacy and exposure: ethical issues within citizen-facing analytics. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), p.20160132.

Hill, K. (2012). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*. [online] Forbes. Available at: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#3052e6a36668 [Accessed 28 Aug. 2019].

Hill, R. and Martin, K. (2014). Broadening the Paradigm of Marketing as Exchange: A Public Policy and Marketing Perspective. *Journal of Public Policy & Marketing*, 33(1), pp.17-33.

Hwangbo, H., Kim, Y. and Cha, K. (2018). Recommendation system development for fashion retail e-commerce. *Electronic Commerce Research and Applications*, 28, pp.94-101.

ICO. (2019). *Guide to the General Data Protection Regulation (GDPR)*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed 28 Aug. 2019].

Kannan, P. and Li, H. (2017). Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing*, 34(1), pp.22-45.

Kshetri, N. (2014). Big data′s impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), pp.1134-1145.

Krueger, R. and Casey, M. (2015). *Focus groups*. Thousand Oaks, Calif.: Sage Publications.
Punch, K. (2014). *Introduction to social research*. 3rd ed. pp.: 87, 95-96, 120-122 , 171-177.

Koistinen, A. (2019). *Facebook sai Yhdysvalloissa viiden miljardin dollarin sakot yksityisyyden loukkaamisesta*. [online] Yle Uutiset. Available at: https://yle.fi/uutiset/3-10892365 [Accessed 28 Aug. 2019].

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, pp.122-134.

Koops, B. (2014). The trouble with European data protection law. *International Data Privacy Law*, 4(4), pp.250-261.

Krämer, J. and Wohlfarth, M. (2018). Market power, regulatory convergence, and the role of data in digital markets. *Telecommunications Policy*, 42(2), pp.154-171.

Kurtz, C., Semmann, M., and Böhmann, T. (2018). Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Twenty-fourth Americas Conference on Information Systems, New Orleans.

Leeflang, P., Verhoef, P., Dahlström, P. and Freundt, T. (2014). Challenges and solutions for marketing in a digital era. *European Management Journal*, 32(1), pp.1-12.

Lieber, C. (2019A). *The Golden Age of Instagram Marketing Is Over*. [online] The Business of Fashion. Available at: https://www.businessoffashion.com/articles/professional/social-media-advertising-rising-costs-instagram-facebook [Accessed 12 Aug. 2019].

Lieber, C. (2019B). *Why Brands Are Sliding Into your DMs*. [online] The Business of Fashion. Available at: https://www.businessoffashion.com/articles/intelligence/why-brandsare- sliding-into-your-dms?source=bibblio [Accessed 12 Aug. 2019].

Lineup. (2019). *10 Digital Ad Trends 2019*. [online] Flipsnack. Available at: https://www.flipsnack.com/lineupsystems/10-digital-ad-trends-2019/full-view.html [Accessed 12 Aug. 2019].

Martin, K. and Murphy, P. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), pp.135-155.

Martínez-Martínez, D. (2018). Unification of personal data protection in the European Union: Challenges and implications. *El Profesional de la Información*, 27(1), p.185.

Molin, A. and Magnusson, N. (2019). *The 29-Year-Old Who Rocked Facebook Has Big Data Plans for H&M*. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2019-01-31/the-29-year-old-who-rocked-facebook-has-big-data-plans-for-h-m [Accessed 12 Aug. 2019].

Montgomery, A. and Smith, M. (2009). Prospects for Personalization on the Internet. *Journal of Interactive Marketing*, 23(2), pp.130-137.

Morisada, M., Miwa, Y. and Dahana, W. (2019). Identifying valuable customer segments in online fashion markets: An implication for customer tier programs. *Electronic Commerce Research and Applications*, 33, p.100822.

Nissenbaum, H. (2010). *Privacy in context*. Stanford, Calif.: Stanford Law Books.

Nissenbaum, H. (2017). Deregulating Collection: Must Privacy Give Way to Use Regulation?. *SSRN Electronic Journal*.

Nurse, J. and Buckley, O. (2017). Behind the scenes: a cross-country study into third-party website referencing and the online advertising ecosystem. *Human-centric Computing and Information Sciences*, 7(1).

O'Connor, T. (2019). *How Luxury Fashion Learned to Love the Blockchain*. [online] The Business of Fashion. Available at: https://www.businessoffashion.com/articles/fashion-tech/how-luxuryfashion- learned-to-love-the-blockchain [Accessed 12 Aug. 2019].

Pantano, E., Giglio, S. and Dennis, C. (2018). Making sense of consumers' tweets. *International Journal of Retail & Distribution Management*, 47(9), pp.915-927.

Richards, N. and King, J. (2013). Three Paradoxes of Big Data. *STANFORD LAW REVIEW ONLINE*, 66(41).

Statista. (2019). *Global big data and business analytics revenue 2015-2022 | Statistic*. [online] Available at: https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/ [Accessed 18 Mar. 2019].

Stevenson, D. (2016). Data, Trust, and Transparency in Personalized Advertising. *ProQuest LLC*.

Stitchfix.com. (2019). *Stitch Fix, Your Personal Stylist*. [online] Available at: https://www.stitchfix.com/about [Accessed 12 Aug. 2019].

Sørensen, J. and Van den Bulck, H. (2018). Public service media online, advertising and the third-party user data business. *Convergence: The International Journal of Research into New Media Technologies*, p.135485651879020.

Tapsell, J., Akram, R. and Markantonakis, K. (2018). Consumer Centric Data Control, Tracking and Transparency – A Position Paper. Retrieved from https://arxiv.org/abs/1805.04747.

Van Ooijen, I. and Vrabec, H. (2018). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, 42(1), pp.91-107.

Yuan, S., Abidin, A. Z., Sloan, M., & Wang, J. (2012). Internet advertising: An interplay among advertisers, online publishers, ad exchanges and web users. Retrieved from https://arxiv.org/abs/1206.1754.

Yu, S., Hudders, L. and Cauberghe, V. (2018). Are fashion consumers like schooling fish? The effectiveness of popularity cues in fashion e-commerce. *Journal of Business Research*, 85, pp. 105-116.

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), pp.75-89.

Zwick, D. and Dholakia, N. (2004). Consumer subjectivity in the Age of Internet: the radical concept of marketing control through customer relationship management. *Information and Organization*, 14(3), pp.211-236.

Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *SSRN Electronic Journal*.

Appendix

Focus groups questions

- What type of data you think companies collect from you and how it is used?
- (Follow up: what thoughts this emerges in you?)
- What do you think about targeted marketing or online and marketing personalization in general?
- (Follow up: how would you describe e-commerce and marketing personalization is performed?)
- Could you explain GDPR in your own words?
- Are you aware what obligations companies and what rights you have due to GDPR?
- What thoughts online privacy emerges in you?
- Do you take actions to enhance your online privacy?
- (Follow up: read companies terms & conditions for privacy and delete cookies?)

THE SWEDISH SCHOOL
OF TEXTILES
UNIVERSITY OF BORÅS

Visiting address: Allégatan 1 · Postal address: 501 90 Borås · Phone: 033-435 40 00 · E-mail: registrator@hb.se · Webb: www.hb.se