Privacy Concerns- How customers perceive different privacy policies?

Master Thesis submitted in fulfillment of the Degree

Master of Science

in MSc in Management

Submitted to Marion Garaus

Haidi Alla

1823501

Vienna, 28th January 2022

AFFIDAVIT

I hereby affirm that this Master's Thesis represents my own written work and that I have used no sources and aids other than those indicated. All passages quoted from publications or paraphrased from these sources are properly cited and attributed.

The thesis was not submitted in the same or in a substantially similar version, not even partially, to another examination board and was not published elsewhere.

ABSTRACT

Technology has made it easier for online services to develop marketing strategies based on customers´ personal data. The information is gathered through privacy policies and is used for personalized products and services, discounts, prioritization, and other benefits. However, data usage has caused a rise in customers´ privacy concerns. The reason behind this is that most of the customers do not read or understand the privacy policies because of the length, visibility, or language used. This implies that consumers are not aware of how the information is gathered, how it is used, and for what purposes. Furthermore, other factors may affect data sharing, such as trust, perceived benefits, control over the data, and sensitivity of information required.

This study aims to investigate how customers perceive privacy policies and understand what factors affect the customers´ privacy concerns and information disclosure. The paper uses a quantitative approach to provide answers to two research questions raised in this master thesis about the customers´ perception of privacy policies as well as the factors that affect privacy concerns and the disclosure of customers' data. A descriptive online survey is employed to gather the data regarding the constructs analyzed in this research, including privacy policy comprehension, customers´ perception, trust, website satisfaction, control, information disclosure, benefits, and privacy concerns. The results showed that, in general, most of the customers do not read and understand privacy policies. Moreover, it indicated that higher trust and benefits would lead to higher information disclosure. On the other hand, higher trust and control would lower privacy concerns. Overall, customers need more control over their data and require benefits in order to share their data.

Keywords: customer data, privacy policy, privacy concerns, information disclosure

ACKNOWLEDGEMENTS

My gratitude goes to my supervisor, Marion Garaus, for being an extraordinary supervisor during my master thesis. I am thankful for her support and for sharing valuable and sincere guidance throughout this collaboration. She has been dedicated and pushed me forward with her advises. Secondly, I want to thank Doraldo for being a supportive partner who has always motivated and encouraged me during the whole thesis duration. Last but not least, thank you to my family, without whom I would not have been who I am today. Thank you for everything, for believing in me, and for supporting me to follow my dreams. Sincere thanks go to everyone who has been by my side during this process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

B2B - Business-to-business

B2C - Business-to-consumer

EC - Electronic Commerce

FTC - Federal Trade Commission

GDPR - General Data Protection Regulation

GIPC - Global Information Privacy Concern

IT - Information Technology

PCAST - President's Council of Advisors on Science and Technology

OSD online self-disclosure

KPI - Key Performance Indicators

P3P - The Platform for Privacy Preferences project

P2U - Purpose-to-Use

SC - Social Contract theory

TRA - Theory of Reasoned Action

TPB - Theory of Planned Behavior

W3C - World Wide Consortium

1 INTRODUCTION

Customers ´ personal information that firms gather during business operations is a useful marketing source. Data collection from existing and potential customers is essential for improving customers´ experience (Plangger and Watson, 2015). Nowadays, marketing uses new technologies that include surveillance practices, so managers need to see how these practices affect their customers (Moe and Ratchford,2018). These practices include gathering, using, and storing customers' data (Plangger and Watson, 2015). Companies use customers´ surveillance to gain loyalty, satisfaction, and customer relationships and, in this way, to gain a competitive advantage (Jaworski and Kohli,1993). On the other hand, many customers share their data in exchange for profits, including discounts, personalized products, and services (Rainie and Duggan, 2016). However, this surveillance may also have adverse outcomes, including privacy concerns (Inman and Nikolova, 2017). Therefore the development of technology has brought the problem of protecting personal data.

Apparently, privacy is vital and precious today because customers are no longer protected, and personal data are misused and shared with third parties without their approval (Aimeur, Lawani, and Kimiz, 2015). In 2014, was surveyed 600 companies, and the results showed that 42% of companies collect data from data-sharing partnerships, which is higher than the 33% of companies that collect data from third parties (Cooper and LaSalle). Data sharing has mainly been used for innovative products, new customer markets, and better customer service. This usage is explained by the collaboration that IKEA had with Facebook. In 2016, Cassidy, Poynter, Duckworth, and Burnett did an experiment to study this collaboration, and they found that IKEA was able to bring existing and new customers to its stores, increased by 1% its overall lift, increased by 31% its lift to the 22-25-year-old customer segment, and gained a return to profit of 6:1 of the expenditures on the paid media.

Most of the time, customers face tradeoffs between safeguarding their data and the profits they get from the companies using their data (e.g., customized products, discounts, etc.). Therefore, customers´ attitude toward surveillance is determined by personal concerns (Baumfartner, 2002) regarding customers´ privacy (Malhotra, Agarwal and Kim, 2004;

Milberg, Smith and Burke, 1996) and customers´ value (Neslin, Ailawadi, and Gedenk, 2001). According to Malhotra, Agarwal, and Kim (2004), the customers´ trust in online services is low, which is seen as a problem for the development of digital marketing. The value-based approach considers privacy as a human right (Neslin, Ailawadi, and Gedenk, 2001). Moreover, the study done by Milberg, Smith, and Burke (1996) showed that Americans are concerned about companies' information privacy practices. These attitudes affect the response to the surveillance actions and include changes in behavior, consumption, and other attitudes (Pflangger and Montecchi, 2020). To understand the customers' attitude toward the surveillance, it was proposed privacy calculus, which explains how customers equilibrate the profits and the costs they get by sharing the personal data (Culnan and Armstrong, 1999). According to Smith et al. (2011), customers share their private information against expected benefits like customization, financial rewards, and social adjustment profits. This means "customers trade away information for a more valued incentive," stated Caudill and Murphy (2000, p.8). For example, when a customer buys online, he sacrifices his data to profit personalized products, discounts, and other benefits.

Currently, the Internet is used by more than three billion people worldwide, where two billion are active users on social accounts (Aimeur, Lawani, and Dalkir, 2015). Even though technological innovation is generally good for society because it helps people interact with each other, this development has been a matter for the privacy of individuals (Stewart, 2017). However, technology is part of daily life, and it allows the community to access information and everything they need online (Allen,2019). Moreover, it has helped people communicate with each other worldwide through different electronic devices. According to a study done by the Pew Research Center, 52% of US adults claim that the technological innovations have had positive effects, whether 38% say that it has had equally positive and negative impacts and 8% claims that it has had significant adverse effects (Funk, Kennedy, and Sciupac, 2016). Even though technology improves people's lives and makes it easier, the downside of its innovation is the difficulties of protecting privacy since the rates of privacy concerns are increasing (Loubier, 2021).

The concept of privacy has been recognized for a long time now, but still, different sectors, including marketing, political science, law, and economics, define it differently (Moor,1990). Some of the most common definitions are: Westin (1967) defined privacy

as “a state where the information of customers is limited”; Altman (1975) stated that “privacy is the control chosen to be accessed by the self”; Nissenbaum (2009) defined privacy as “claiming relevant personal information to society.”

Regarding privacy, a person who participated in a survey of Pew Research Center said: “I share the data every time I leave the house, whether I want to or not. The data isn’t really the problem. It is who gets to see and use that data that creates problems. It is too late to put that genie back in the bottle (Rainie and Duggan 2016, p.9).” Miltgen et al. (2016) claimed that customers’ privacy concerns make them not accept technology innovations, while Jozani et al. (2020) argued that this behavior could bring less engagement from their side. Moreover, Oghazi et al. stated that the increase of information regarding privacy increases concerns and the indisposition to share personal information (2020). As it seems, privacy is multidimensional and progresses with technology development, and it can be determined according to two perspectives value-based or cognate-based (Smith et al., 2011). The first perspective is related to human rights as part of the moral value system. On the other hand, the second perspective is related more to human perception than to value. It is about the ability of the customer to control how, when and what information can be used, and it is according to the EU General Data Protection Regulation (GDPR) (Belanger and Crossler, 2011; Ioannou et al., 2020).

Companies use privacy policies as a channel to disclose the data collected from their customers (Aimeur, Lawani, and Dalkir, 2015). However, even though customers have many concerns about sharing their data, just a few of them take the time to read them because of the length and the difficulties in understanding them (Ermakova, Baumann, Fabian, and Krasnova, 2014). Therefore, to have fewer customers´ privacy concerns and satisfied customers, companies need to provide a friendly format that is easy to read and not force customers to accept the policy if they want to use the website. Therefore, customers face a dilemma because they have only two options: accepting the privacy policy and losing their privacy or not accepting them and not accessing the service they want. One of the most used solutions to the privacy concerns problem is gaining users’ trust through online services (Ermakova et al., 2014). Gaining customers´ trust, companies get more personal information, and customers get personalized products, discounts, recommendations, etc., resulting in a win-win situation.

The development of technology has significantly changed the concept of marketing and has made it easier for companies to reach potential customers with personalized messages (Krafft, Arden, and Verhoef, 2017). One method of marketing used to adapt to these technological advancements is permission marketing based on getting customers' approval to send them marketing messages (Marketing Terms.com, 2004). According to Gordin, permission marketing allows companies to interact with customers without having such matters (1999). Permission marketing is about direct marketing activities that require customers' approval to take action. Permission does not have only advantages to interactive marketing activities, but also it is used as a legal requirement (Tsang Ho and Liang 2004). According to Kumar, Zhang, and Luo, permission marketing is the best solution to gain customers and deal with legal issues and privacy concerns (2014).

1.1 Research aims and objectives

This research gives an overview of previous studies on privacy policies, the challenges of customers´ privacy protection in digital marketing, models and theories related to privacy concerns and information disclosure, how customers perceive different privacy policies, and what factors influence the exposure of the personal data and the concerns related to the customers´ privacy. The main purpose of this study is first to investigate how customers perceive different privacy policies and second to understand what factors affect the customers´ privacy concerns and information disclosure. Therefore, this study will focus on both companies and customers, how and what companies do to protect customers' data and gain their trust, how customers perceive privacy policies, and what affects privacy concerns and data disclosure. The research questions of this master thesis are as follows:

RQ1: How do customers perceive privacy policies?

RQ2: What factors affect the customers´ privacy concerns and information disclosure?

This study uses a quantitative approach to provide an understanding of how customers perceive different privacy policies and what factors affect their information disclosure and privacy concerns, and for this, it is employed a descriptive online survey. The descriptive survey design examines multiple variables explained in the literature review. The data collected will be analyzed using the SPSS.

1.2 Structure of thesis

This study consists of five main chapters. After the introduction of the research background, the research aims, and objectives of the thesis, the literature review chapter will provide an overview of privacy policies providing factors enhancing privacy, the attitude of customers toward personal information disclosure and differentiation between EU and USA; continuing with the conceptualization of customer privacy concerns, the impact of technological development on privacy concerns, and provided solutions for the concerns; the third subchapter talked about companies' strategies toward privacy; followed by privacy ethics, and permission marketing. The next chapter is the methodology representing the study design and the research model. This part describes the study design and the participants, the online survey structure, and explains how the data gathered from all the respondents are being collected and analyzed. In the following chapter, the results will be represented. This section examines the scale reliabilities between each item and tests the arisen hypothesis using linear regression. The next chapter discusses the results from the analysis and shows the limitation, areas for future research related to this research, areas for future research related to this topic, and implications for relevant stakeholders

2 LITERATURE REVIEW

2.1 Privacy policies

2.1.1 Conceptualization of privacy

Traditionally, privacy is seen as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others," (Westin 1967, p. 7) but for many researchers, it is complex as a concept to define (Martin and Murphy, 2017; Smith, Dinev and Xu, 2011). According to Neetling et al. (1996), privacy can be defined as "an individual condition of life characterized by exclusion from the publicity" (p. 36). "The concept of privacy follows from the right to be left alone" (Stair, 1992, p. 635; Shank, 1986, p. 12). Privacy as a notion has been studied for many years in nearly every area of the social sciences and yet is not fully developed (Smith, Dinev, and Xu, 2011). Solove stated privacy, as a conception, "is in disarray [and n]obody can articulate what it means" (Solove 2006, p. 477). Privacy is a fundamental right since it is necessary for other rights such as liberty and autonomy. Hence, there is a connection between privacy, independence, and dignity. Respecting a person's privacy entails recognizing that person's right to be free and his autonomy as a human being (Britz, 1996).

In democratic countries, the right to privacy is protected by the constitution. Since the 20th century, this constitutional right has been expressed in a variety of legislative forms, such as: "The Privacy Act" (1974) in the United States of America, the proposed "Open Democracy Act in South Africa" (1996), and "Data Protection Act" in the UK (1984). Australia likewise adopted a "Privacy Charter" in 1994, which contains 18 principles defining a citizen's right to personal privacy as "effected by the handling of information by the state" (Collier, 1994, p. 44-45).

Privacy policies are the technique of how websites inform the users how they gather and use the data. Online tracking has made it easier for companies to get customers´ data. For example, Netflix collects customers´ personal information to personalize its service and develop new content (Marman, 2019). However, only 4% of users read the privacy policies, while 55% had never read them (dos Santos Brito, Garcia, Durao, de Lemos, Meira,

2013). Reading the privacy policies costs the customer 72 working days for all the websites visited within a year. Moreover, customers are overwhelmed with the complexity of policies (Stewart, 2017). Therefore, time and effort spent reading and understanding the privacy policies is a cost. For this reason, most consumers do not read these policies and do not know what data are collected or how they are used (Richards and King, 2014). A study conducted on the changes in customers' attitudes toward privacy policy over a decade showed that nothing has changed in their attitude because for customers, privacy policies are still long and difficult to read and work only for companies' benefits (Williams, Agaewal, and Wigand, 2015).

The trust of customers that read and understand the policies depends on the content of privacy policies. In 2012 a study examined how the content of the privacy policies is related to the customers´ trust and privacy concerns (Wu, Huang, Yen, and Popova). A significant relationship was found between the content of privacy policies and customers´ trust and privacy concerns. Another study recommends that online service needs to use some characteristics of privacy policies better to encourage customers to read privacy policies (Capistrano and Chen,2015). This study considered length, visibility, and specificity as features to measure their effectiveness in information responsiveness and the importance of privacy policies on the determination to give private data. This experiment presented a short or lengthy privacy policy; the privacy policy was placed on the top of the website (high visibility) or on the bottom (low visibility); standard terms or technical language were used for the specificity. The results showed that the specificity of the privacy policy is the variable that has the most significant effect on customer perception. This means that customers are not used to technical language, and if companies use a daily use language, it will help the consumer read and understand the privacy policies. Moreover, visibility was another significant variable. To show the importance of privacy policies for customers, policies need to be easily seen (Capistrano and Chen,2015).

Even though privacy policies are essential for both the company and the customer, it is questionable if consumers understand the content of privacy policies. Therefore, a study was done to examine the difference of understanding between specialists and ordinary users (Reidenberg et al., 2014). The researchers showed different privacy policies to experts and everyday users to do this experiment. The outcomes demonstrated that regular users had difficulties understanding the content, mainly the information regarding the data

sharing. This misunderstanding leads to sharing of the data by customers that they do not want to share.

According to a study, not many companies are transparent with their customers regarding the data collection, and they do not give the customers a chance to discuss the data gathered about them (Cranor, Hoke, Leon, and Au,2014). For this reason, in 2014, PCAST (President's Council of Advisors on Science and Technology) recommended users' sign-up for one of many "privacy preferences profiles." Moreover, customers will be able to opt-out of a particular use of data (Richard and King, 2014).

Nowadays, several tools are available to support customers in protecting their data, such as eTrust, which aims to convince users that their data are protected. Having this certification on the company´s website will inform the customer of any data collected and why it is collected and, in this way, it creates trust between two parties. eTrust gives the customers the information they need to know about companies' practices, and at the time, it helps companies understand the customers´ concerns. Another tool is PrivacyFix which allows customers to manage their privacy settings. It shows the customer what information is collected and viewed by the companies and enables them to change or delete any data. These tools are a way for customers to know what information is collected and how they are used. They are beneficial for customers and companies that want to keep the existing customers and gain new ones. In this way, companies achieve the customers' expectations for trust and transparency, gain a competitive advantage since it is shown that privacy regulations lead to economic profits, higher quality of data, better marketing, and improved customer experience, which lead to loyal customers (Data Privacy Manager, 2021).

2.1.2 Attitude toward disclosing personal data online

According to Fishbein and Ajzen (1975, p. 6), an attitude is "a learned predisposition to respond in a consistently favorable or unfavorable manner with respect to a given object." Furthermore, Rokeach (1968, p. 112) defined attitude as "a relatively enduring organization of beliefs around an object or situation predisposing one to respond in some preferential manner." However, the attitude structure can be understood as a "psychological inclination manifested by a favorable or unfavorable judgment of a certain entity" (Eagly and Chaiken, 1993, pg.1).

Evaluating an individual's attitude toward an activity, like sharing data, is a valid indicator of their disposition to act, even if it falls short of assessing behavioral intent (Fishbein and Ajzen, 1975). Attitude effects have been studied in terms of attitudes regarding online self-disclosure (OSD), which is explained as "the degree to which an individual feels more secure while revealing private information in online contexts" (Ledbetter, Broeckelman-Post, and Krawsczyn 2011, p.226). Similarly, Mothersbaugh, Foxx, Beatty, and Wang (2012), described online self-disclosure as "an individual's willingness to reveal personal information to a firm online" (p.2). Ledbetter (2009) created an instrument to assess attitudes regarding online communication to validate this notion. The instrument used five dimensions to assess both cognitive and affective beliefs about online communication: self-disclosure, apprehension (of communicating online), miscommunication (digital communication inhibits mutual understanding), social connection (online communication facilitates contact with a person's network), and ease (appreciation of the pleasure and utility offered by web communication).

The hypothesis that attitude toward online self-disclosure can influence communication was supported by Caplan (2007), who connected negative attitude toward online self-disclosure with low communication ability. Self-disclosure was negatively correlated with relational closeness, Facebook communication (Ledbetter et al., 2011a), and the quantity of everyday communication over the telephone and face to face (Ledbetter et al., 2011b). A similar research showed that online communication attitudes, especially those of OSD and social contact, significantly affect compulsive and excessive Internet usage (Mazer and Ledbetter, 2012). Moreover, users with a positive attitude toward OSD utilize online communication more often (Ledbetter and Kuznekoff, 2012) but could ignore particular sorts of social media communication (Shoenberger and Tandoc, 2014).

2.1.3 Factors enhancing customer´s privacy

1. Trust

The most determining factor which affects the relationship between two parties is trust. Hunt and Morgan (1994) developed the commitment-trust theory, which argued the importance of commitment and trust in advancing relationship marketing. Trust is attributed to "one´s willingness to rely on an exchange partner in whom one has confidence,"

(Moorman, Zaltman, and Deshpande, 1992, p.315) and "positive expectations about another´s intentions or behaviors" (Rousseau, Sitkin, Burt, and Camerer, 1998). Many researchers have studied the importance of trust in customer-company relationships (Martin and Murphy, 2016; Pavlou et al., 2007; Bleier and Eisenbeiss, 2015). In terms of privacy, the trust supports data disclosing, purchase, and approval of advertising, bringing fewer privacy concerns (Martin and Murphy, 2016). In addition, belief in companies can diminish privacy concerns if the customized marketing messages are according to the customer´s interests (Bleier and Eisenbeiss, 2015). Moreover, trust makes customers more disposable to disclose their data, bringing customers to use customized services (Chepalla and Sin, 2005), causing economic benefits to the companies (Kalaignanam, Kushwaha, and Rajavi, 2018). On the other hand, according to Pavlou et al. (2007), privacy concerns come from customers' convictions that a company is incapable or reluctant to protect customers´ data. Correspondingly, using "privacy-compromising" technologies like cookies harms trust and reduces purchases (Miyazaki, 2008). On the other hand, belief can diminish privacy concerns if the customized marketing messages are according to the customer´s interests (Bleier and Eisenbeiss, 2015). Moreover, trust makes customers more disposable to disclose their data, bringing customers to use customized services (Chepalla and Sin, 2005), bringing economic benefits to the companies (Kalaignanam, Kushwaha, and Rajavi, 2018). Even though technological innovations have made it difficult for customers to believe in companies, trust can be achieved by transparency, which will also decrease negative word-of-mouth and negative customer behavior (Martin et al., 2016). Additionally, trust has been considered as crucial to consumers' interaction in e-commerce (Lin and Wang, 2006) and social networks (Parra-López et al., 2011), as well as information disclosure (Dinev and Hart, 2006), mainly when disclosure is linked with a company's higher disclosed aims (e.g., mission, values) (Anderson and Agarwal, 2011). Consumers' desire to provide their data to companies rises when firms are seen as trustworthy (Dinev and Hart, 2006). Therefore, the following hypothesis was developed.

H1: The higher the trust, the higher the probability of disclosing their personal data.
H2: The higher the trust, the lower the privacy concerns.

2. Information required

The sensitivity of personal data required plays an important role in customers´ perceptions. Data sensitivity has been characterized in terms of intimacy, where more intimacy is being associated with information that is thought to be riskier to expose due to the susceptibility of loss (Lwin, Wirtz, and Williams 2007; Moon, 2000). Psychological (e.g., loss of self-esteem as a result of shame), physical (e.g., loss of life or health), and monetary (e.g., loss of cash) damages may occur as a result of the exposure of personal data (Moon, 2000). Mothersbaugh, Foxx, Beatty, and Wang (2012) describe data sensitivity as "the potential loss associated with the disclosure of that information" (p.2). This approach reflects that sensitive data are viewed as riskier and more difficult to disclose, but it focuses on data sensitivity and the data loss resulting from disclosure (Cranor, Reagle, and Ackerman, 1999).

Customers´ reaction to the privacy policies is related to the information required by the companies (Phelps et al., 2000). From a customer perspective, sharing more sensitive information, such as financial and medical information, is recognized as more risky (Milne and Gordon, 1993). On the other hand, lifestyle information is perceived as less risky, and customers are more willing to share this information. Moreover, users may have more losses if their data are more sensitive, so they avoid sharing these kinds of information (Bansal, Zahedi, and Gefen, 2016). As a result, the type of information required will affect customers' attitudes toward the privacy policy (Malhotra, Agarwal, and Kim, 2004). Based on the findings, the hypothesis is developed as follows:

H3: The higher the level of sensitivity, the lower the probability that customers will disclose their personal data.

3. Transparency

One of the reasons why privacy concerns arise is that companies do not use customers´ data for the purpose that was stated on privacy policies (Bleier, Goldfarb, and Tucker, 2020). In addition, transparency is often related to control (Foxman and Kilcoyne, 1993). This means that if companies inform customers about the data practices and give them control over their private information, customers are willing to share their personal information. Therefore, providing the right and complete information about how the company uses the customers´ data is crucial in diminishing privacy concerns (Bleier, Goldfarb, and Tucker, 2020). According to Clarke (2001), the threat to privacy faced by data sharing

can be described in two ways: (1) the category of the data disclosed, and (2) the form of harm caused by the abuse of disclosed information. Furthermore, Xu et al. (2011) demonstrated a positive correlation between privacy risk and disclosure's perceived value.

4. Comprehension

When talking about privacy policies, the question that often arises is: "Do customers really understand the content of privacy policies, even though they are still the most important source of information for users to know how companies collect, use and share their data?" (Aimeur, Lawani, Dalkir, 2015, p.372). They examined the understanding and remembering of the policy that are dependent on the style of writing, the clarity, and the length of the privacy policy. The results showed that readability is related to comprehension. Moreover, understanding affects benevolence, so they feel that the company cares about customers´ interests when they understand the policy. This means that it is more critical for the privacy policies to be more understandable than to serve as protection for the companies (William et al., 2015). Moreover, Vail, Earp, Anton (2008) examined the consumer perceptions and comprehension of privacy policies. The findings showed that users believe that policies presented in a standard, paragraph-style language are the most comprehensive. Moreover, they found that customers do not feel confident in their understanding of privacy policy when represented in an unusual, less user-friendly way than standard language. The respondents did not understand the policy very well, but once privacy statements were emphasized, understanding of the policy rose. In addition, most of the participants did not read the whole privacy, but even when they did, nearly half of the understanding questions were adequately completed. A study in 2014 showed a lack of understanding of the language of privacy policy language, especially related to data sharing (Reidenberg et al.). This lack of knowledge may lead to making decisions that are not profitable for users. The customers have the right to know how their personal information is used, and for this reason, a good clarification needs to be given before they share their data (Rotenberg and Jacob, 2013). Moreover, when privacy policies are understandable, it implies more trust to customers (Ermakova et al., 2014). A study examined if privacy policy format influences comprehension (Sumeeth, Singh, and Miller, 2012). The results showed that customers did not understand privacy policies in any of the formats given, and approximately 20% of privacy policies comprehension required a

post-graduate level of education. For this reason, most of the customers that do not understand the privacy policies do not disclose their personal data or provide wrong information. As a result, the following hypothesis was formulated:

H4: The higher the comprehension of the privacy policies, the lower the probability that the customers will disclose their data.

5. Control

Customers' data control is one of the factors that affect the customers' decisions. According to the theory of planned behavior (TPB), personal behavior intention influences actual behavior, impacted by attitude, and perceived control (Ajzen, 1991). This implies that when a customer has a positive attitude and perceived control, he is more willing to share his personal data. Moreover, customers want to have control over their data when disclosing them, and one of the reasons they choose not to share their data is the loss of control (Son and Kim, 2008). A study showed "that online consumers consider it most important to (1) be aware of and (2) have direct control over personal information stored in marketers´ databases" (Malhotra, Kim, and Agarwal, 2004, p.350). According to Phelps, Nowak, and Ferrell (2000), a high level of control influence positively purchase decisions. Meanwhile, if they have increased control over their data, they are willing to share more data (Mothersbaugh et al., 2012). Furthermore, if customers have control of their data, the probability of clicking on a customized ad will be higher (Tucker, 2014). Tucker stated "that publicly giving users control of their private information can benefit advertising-supported media and advertisers on social networking sites" (p.557). Moreover, Tucker explained the effects of Facebook allowing its users to control their data (2014). The results showed that controlling their data made customized ads more effective. However, the loss of control leads to customers´ privacy concerns (Malhotra et al., 2004). In addition, Dinev and Hart (2004) showed that controlling their data would reduce privacy concerns. On the other hand, according to Nissenbaum and Solove (2011), given the complexity of companies´ data collection and practices, there are concerns that customers cannot self-manage their data. For this reason, companies should not give customers complete control but let them vulnerable to share and control their data, leading to more information shared (Brandimarte, Acquisti, and Loewenstein, 2012). Regarding the control as a factor of privacy, were formulated hypotheses as follows:

H5: The higher the perceived control over their data, the higher the probability customers will disclosure their personal information.

H6: The higher the perceived control over their data, the lower the privacy concerns.

6. Benefits

Marketing can be described as "an exchange process involving transactions where, among other things, two parties believe it is appropriate or desirable to deal with one another" (Robinson, 2018, p.8). Kotler (1988) defines exchange as "the art of obtaining a desired product from someone by offering something in return" (p. 6). Generally, companies supply goods or services for the customer's profit, who in exchange provides consideration, which may include sharing information to enable the process and benefit the company.

Personal information is frequently exchanged for profits or rewards in digital marketing. By sharing their data, customers' benefits motivate them to share more private information (Acquisti et al., 2013; Chorppath and Alpcan, 2013). Before disclosing their personal data, users analyze the risks and the profits (monetary or not) they get by doing it (Acquisti et al., 2013). In other words, customer privacy views and actions are frequently analyzed using the privacy calculus model (Laufer and Wolfe, 1977). It is a metric that illustrates how users choose whether to share or not their data depending on the outcome involving disclosure demands and privacy concerns in a particular context of data disclosure (Xu, Teo, Tan, and Agarwal, 2009). Before selecting what and how much data to expose to others, customers´ assumption of positive and negative results is considered (Li, 2012). This theory was developed by Culnan and Armstrong (1999), and describes how customers evaluate perceived benefits and privacy concerns during the disclosure of information. It is composed of privacy concerns, perceived benefits, and disclosure behavior. According to this theory, privacy concerns decrease data disclosure while perceived benefits increase information disclosure (Sun, Fang, and Hwang, 2019). Customers are attracted by incentives and react favorably to disclosing personal data in return for potential advantages, such as information, amusement, or financial incentives (Aydogan, Ozturk, and Razeghi, 2017). Furthermore, customers can offer personal data in order to receive personalized treatment from firms (Graeff and Harmon 2002). This is often used as a way for the companies to get customers' data (Krafft, Arden, and Verhoef, 2017). Moreover, monetary incentives raise customer willingness to approve

the use of their data (Hui, Teo, and Lee, 2007), and they are more willing to accept ads via mobile messages (Tsang, Ho, and Liang, 2004). In addition, personalization profits based on user-dependent value are likely the most effective form of data disclosure reward (Xu et al., 2009). Personalization offers customers marketing messages, recommendations, and individualization regarding different products and services they are interested in (Martin and Murphy, 2016). However, this implies sharing their data, leading to less privacy, meaning that personalization effectiveness is influenced by privacy concerns and the limited trust that customers have for the company (Bleier and Eisenbeiss, 2015). As a result, the following hypothesis was formed:

H7: The higher the perceived benefits, the higher the probability customers will disclose their personal information.

7. Behavioral intentions

One theory that has been widely used to determine behavioral intentions or behaviors is the theory of reasoned action (TRA) (Albarracin, Johnson, Fishbein, Muellerleile, 2001). According to this theory, behavioral intentions are precursors to a person's particular acts. More precisely, when a customer perceives that specific behavior leads to a particular result, his attitude will impact his actions, subjective norms, and societal pressures to do or abstain from performing a specific activity affect behavioral intentions, decided by a person's favorable or unfavorable behavior (Liu, Marchewkab, Luc, and Yu, 2005). For instance, a user´s attitudes toward privacy and trust should shape his attitude regarding online transactions, affecting behavioral intents to engage online. Moreover, Liu, Marchewkab, Luc, and Yu's (2005) findings showed that trust would influence the visit to the website again, whether they will have pleasant comments about the website and whether they would suggest it to others. As a result of these observations, the following hypothesis was formulated.

H8. The higher the level of trust, the higher the probability customers will reuse the website and recommend it to others.

2.1.4 Differentiation to similar construct

Privacy is multidimensional and dynamic because it changes with life experiences, but not every concept related to it is privacy (Laufer and Wolfe, 1977). According to Margulis

(2003), concepts like anonymity, secrecy, confidentiality, and security have confused what privacy is.

1. Anonymity

According to Qian and Scott (2007), anonymity is the capability to disguise an individual's identity, which is crucial for analytical data collection. In another context, in information technology (IT), this concept is often adjusted by the privacy-enhancing technologies´ features (Smith, Dinev, and Xu, 2011). For example, "incognito mode" allow users to browse websites with anonymity since cookies cannot be used and the IP addresses cannot be tracked (Waldo et al., 2007). Therefore users can choose whether to be anonymous or identified. It has been discussed what role has anonymity plays in privacy, but even though these notions are linked, anonymity is not privacy (Camp, 1999). Furthermore, anonymity happens when the user browses in a way that is not identified, and no information can be gathered for him. Therefore since no data can be linked to the user, it can enable privacy control (Smith, Dinev, and Xu, 2011).

2. Secrecy

Secrecy is explained as concealing of facts on purpose, and it frequently indicates a reluctance to share possibly inaccurate information (Ywick and Dholakia, 2004). Secrecy and privacy are frequently confounded with each other (McLean 1994). Related to this confusion, Bok (1989, p.11) stated: "Privacy need not hide, and secrecy hides far more than what is private." Moreover, Warren and Laslett (1977) claimed that secrecy is related to something used negatively by the excluded audience, and privacy defends actions valued by society and is morally neutral. According to Tefft (1980), secrecy allows users to manipulate and control environments by not sharing personal information.

3. Confidentiality

Camp (1999) and Rindfleisch (1997) discuss the changes between confidentiality and privacy. According to them, confidentiality is defined as a controlling share of personal data to an arrangement that limits the use or shares of data to other parties. On the other hand, privacy corresponds to the need of an individual to control the disclosed personal data.

4. Security

According to some researchers, security is related to the concerns about the protection of personal data with three objectives: (1) integrity which guarantee that personal data are not changed during transit; (2) authentication that verifies the users' data and approves the use of data; (3) confidentiality that guarantee that authorized people use data for authorized purposes (Belanger et al., 2002; Chellappa, 2008). Belanger et al. (2002) argued that the connection between security and privacy is not clear. However, Ackerman (2004, p. 432) argued that "security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of disclosure, or to reassure users." Related to this statement, Culman and Williams (2009) claimed that companies can successfully secure the customers´ data but can make bad decisions to use these data, leading to data privacy problems.

2.1.5 Differences between US and EU privacy policy regulations

Privacy has been a discussion for decades now, and privacy concerns are a problem worldwide. In 2000, Norman Mineta, former US Secretary of Commerce, stated that privacy is one of the critical issues in the development of the economy. In addition, a study found that 94.5% of Americans are concerned about their privacy when they buy online (University of California-Los Angeles Center for Communication Policy, 2001, p. 44).

According to Caudill and Murphy, in the US from 1970 until 1993, thirteen privacy regulations were established by Congress (2000). In 1990, the Children's Online Privacy Protection Act and the Gramm-Leach-Bliley Act asked institutions to explain the data sharing to the customers. The EU Data Protection Directive renewed in 2015 includes a broader consumer information privacy protection than any US privacy regulation. In the rules of data protection in the EU Directive, companies are responsible for the privacy behaviors to authority, and there is a section "right to be forgotten" that allows the customer to request the elimination of links that are not accurate for them. After the affection of the EU Directive and some negotiations, the EU-US Privacy Shield was concluded: "The new arrangement will provide stronger obligations on companies in the US to protect the personal data of Europeans and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission, including through increased cooperation with European Data Protection Authorities (European Commission, 2016)."

2.2 Customer privacy concerns

2.2.1 Conceptualization of privacy concerns

There are growing concerns about personal data privacy (Cole, 2001). According to Turow (2003), 64% of adults claim never obtaining advice on how to secure their data online, and 40% indicate understanding little on how to stop websites from gathering their data. Moreover, three-fourths of nonusers view online services as a risk to their privacy, implying that violations of confidentiality also dissuade potential online shoppers (Cole, 2001). Privacy concerns may discourage engagement in online activities, especially among new users and women, restricting online commerce's development (Pew Research, 2000). Furthermore, the Federal Trade Commission (FTC) reported that just 20% of leading e-commerce sites adhered to the agency's guidelines for protecting user privacy (FTC, 2000).

Business-to-consumer (B2C), intra-organizational applications, and business-to-business (B2B) are classed as electronic commerce (EC) applications (Liu, Marchewkab, Luc, and Yu, 2005). Concerns about privacy have become a significant issue in B2C e-commerce as a result of the direct engagement of customers and the company's possible capacity to collect, archive, and distribution of customers' data. Intra-organizational applications emphasize the use of web technologies to convey information within the company. Intranets are becoming a requirement for company data systems due to their effectiveness as a framework for deploying web-based workflow and groupware (Turban, Lee, King, and Chung, 2000). As a result, increased availability of information and increased internal secondary information usage are suggested to enhance internal coordination. Nevertheless, administrative and technical measures against data loss, abuse, modification, unauthorized access, and integrity continue to be necessary (Choate, 2000). According to Liu, Marchewkab, Luc, and Yu (2005), the measures may include "cross-referencing data against multiple sources, authorization, authentication to confirm identity, non-repudiation to provide proof of origin/delivery, audit mechanisms to provide records for independent review, confidentiality to protect unauthorized disclosure, and integrity to detect unauthorized modifications" (p.290). EC has contributed to the development of a variety

of online commercial interactions, such as those between businesses and suppliers, strategic partnerships, company and clients, and business-to-end-consumer (Speier, Harvey, and Palmer, 1998). Until now, privacy has been a concern in the B2C sector and B2B transactions. Moreover, B2B raises significant concerns about data sharing to third parties and external secondary usage of users' private data without their permission: numerous individuals assert a right to be informed what data firms reveal to third parties. Throughout many sectors, information sharing is a crucial marketing strategy. Accenture reported in 2014 a survey of 600 firms worldwide that 42% of them collected users´ information using data-sharing agreements, surpassing the 33% of firms that collected personal information through third-party data providers (Cooper and LaSalle, 2016). Additionally, the collection of information via data sharing was motivated mainly by the desire to improve customer experiences (77%), expand customer markets (52%), and develop innovative services and products (50 %). Nevertheless, 67% of these organizations reported that their users are constantly protecting their privacy (e.g., changing passwords more often or opting out their information).

By participating in different marketing activities, customers need to share their personal information such as their name, address, etc. (Krishnamurthy, 2001). Depending on how customers perceive the information transmitted, they call it a personal sacrifice that leads to privacy concerns (Son and Kim, 2008). Privacy concerns are seen as individuals' personal perceptions of justice in relation to data privacy (Campbell, 1997). Moreover, privacy concerns are impacted by external conditions such as regulations, industry sectors, and past experiences (Donaldson and Dunfee,1994). This implies different perceptions of what is fair and what is not related to gathering and using data. Moreover, customers´ privacy concerns come from the lack of control over their personal data and from questioning how companies use it in marketing messages (Inman and Nikolova, 2017; Plangger and Montecchi, 2020). In addition, while customers decide to share their data, customers compare the costs and the benefits they get from providing them (Lwin, Stanaland, and Miyazaki, 2008; Planggerand and Montecchi, 2020). When the costs exceed the benefits of sharing personal information, privacy concerns become a severe problem for the customer.

Malhotra, Agarwal, and Kim (2004) stated that customers are concerned about "the collections of their data, the perceived control over their data, and the awareness of how the collected information is used."

1. Data collection

Whether it is fairly done or not, the companies' data gathering is the starting point for customers´ concerns. The collection of data is defined as the degree to which a person is concerned about the personal information others own compared to the amount of profits gained (Malhotra, Agarwal, and Kim, 2004). In 2000, a study showed that 85.6% of customers wanted to limit the information collected by companies (Phelps et al.). This limitation of information that customers want to share was explained as the "privacy threshold" in 1993 by Cespedes and Smith. This actively demonstrates that the collection of information by companies will continue to be a source for customers´ privacy concerns (Rendleman, 2001).

2. Control

Talking about customers, control is crucial because they take risks sharing their data. When users have privacy concerns, they either ask for control over their data or opt-out the data (Caudill and Murphy, 2000). Nowak and Phelps (1995) showed that customers are not worried when they permit companies to use their data or when they have the option to opt-out. Moreover, in 2000, a study results showed that 84% of users wanted to have more control over their data to avoid unwanted ads (Phelps et al.). According to Goodwin (1991), privacy is about control over one's presence and the use of one's information. Consumers' privacy preferences differ, so Goodwin maintains that the user has the right to establish the preferred state of privacy throughout a commercial contact by individual decisions. Nowadays, customers have more control over their data through existing regulations.

3. Awareness

Awareness refers to how much the customer is informed how his data will be used (Culcan, 1995). This factor is based on interactional and informational justice. Interactional justice is related to the transparency shown by the company, and informational justice is associated with the sharing of specific information (Malhotra, Agarwal, and Kim,2004).

Moreover, according to a study, 69% of online users refused to share their data because they were not sure how their personal data would be used (Hoffman et al., 1999). In addition, Phelps et al. (2000) stated that 50% of the users wanted more information and transparency from the companies' side regarding data usage.

Privacy concerns are considered an essential part when talking about privacy. However, measuring privacy concerns is complex and, for this reason, many researchers have developed different measurement approaches which are explained below. A one-dimensional global information privacy concern (GIPC) scale is mainly used (Smith et al.,1996). This scale explains privacy concerns in general. Moreover, Smith et al. (1996) made a series of studies that described privacy concerns as one concept, but with many factors related to each other, such as information's collection, improper access, errors that can happen while gathering them, and unauthorized use, which later are developed more by many researchers.

1. Smith et al. (1996), Stewart, and Segars (2002) stated customers' privacy concerns for the companies' privacy practices as a second-order factor consisting of four first-order factors such as the collection of data, errors in data, secondary use, and unauthorized use.
2. Malhotra et al. (2004) explained customers´ concerns about their data as a second-order factor measured by three first-order factors: control, awareness of privacy actions, and data collection.
3. Buchanan et al. (2007) explained customers concerns about their data as a first-ordered factor explained by 16 factors such as: are the customers concerned by the companies for not being what they claim to be?; are the customers concerned about being asked for too much personal data when using a website?; are the customers concerned about personal information misuse?; etc.
4. Hong and Thong (2013) explained customers' concerns about their data as a third-order factor measured by two second-order factors and six first-order factors. The two second-order factors include interaction and information management, and the six first-order factors include collection, errors, secondary use, unauthorized access, awareness, and control.

Furthermore, customer concerns are determined as anxiety customers face for their personal information in a consumption context (Smith et al., 2011). Nissenbaum (2004) was

a researcher who helped explain why privacy provoked anxiety. He stated (p.155): "The right to privacy is neither right to secrecy nor a right to control but a right to appropriate flow of personal information." Moreover, customers want to keep their data private if it includes identity information (e.g.birthday, address, credit card, their status) or if the relationship between the company and the customer is not close (Marshall,1972). However, there are cases when the relationship between the two parties is close; even though some data requests are private, the customer chooses to share them (Fournier, 1998). Moreover, customers´ concerns lead to the companies not being honest and how companies use and benefit from their data (Phelps et al., 2000). Customers are divided into some categories regarding their concerns: (1) customers who are highly concerned and refuse to share their data; (2) customers who are less concerned and could think of sharing the personal information; (3) customers who have some concerns will make a decision taking into consideration the privacy calculus concept.

Total privacy is difficult to obtain in the digital age. According to Xu et al. (2009), benefits have to exceed the costs to guarantee self-disclosure motivation. Moreover, Wang et al. (2016) found that customers' perceived benefits are positively correlated with information disclosure. Hann et al. (2007) found that economic reward encourages consumers to disclose personal data, and Chellappa and Sin (2005) claimed that many consumers are ready to give up their data in exchange for customized services. According to privacy calculus theory, users aware of the costs when sharing their data online, so the cost-profit analysis is widely used in the digital age (Milne, Rohm, and Bahl, 2004).

Apparently, to decrease customers´ privacy concerns, companies need to focus on providing things in exchange for customers´ data, such as better service and lower privacy (Bleier, Goldfarb, and Tucker, 2020). According to Yun, Lee, and Kim, privacy concerns indicate how customers feel regarding using their data (2019). Smith et al. claimed that customers have concerns about data gathering, unapproved use, failure in protection, and inappropriate access. Privacy concerns are reviewed as a focal outcome (Dinev and Hart 2004) and predictor variable (Milne et al. 2004). As a predictor variable, concerns are related to many expected data privacy outcomes, including willingness to reveal information and get the intention. Companies often do not respect the customers' privacy and use them to offer customized services (Gopal, Hidaji, Patterson, Rolland, and Zhdanov, 2018; Piotrowicz and Cuthbertson, 2014). Companies such as Google, Facebook, and

Amazon track customers' behavior to satisfy customers' needs and wants and create customized products, but this can lead to problems with privacy if too much "marketing push" is employed (Piotrowicz and Cuthbertson, 2014). Sheehan and Hoy (1999) have stated that deeper concerns bring higher negative customer replies; others have found privacy concerns are very contextual and related by many factors that include right judgments (Culnan and Armstrong, 1999), the strengthening of policies (Lwin et al., 2007), and the companies' guarantee (Mothersbaugh et al., 2012).

A research by Goldfarb and Tucker (2012) was done to explain how customers´ concerns have changed from 2001 to 2008, and three million respondents collected by a market research company were used. It was found that the denial to share private information was increased over time, and privacy concerns have increased in the younger and older generations, even though the older generation faces more difficulties in understanding the policies and are less likely to share their data. According to Goldfarb and Tucker (2012), older people do not like to share their personal information, related to the rise of the bad experience with information technology.

Generally, privacy concerns are associated with a lack of control over their information and disbelief in how the companies use the data (Inman and Nikolova, 2017; Plangger and Montecchi, 2020). According to Inman and Nikolova (2017), privacy calculus is not sufficient for the customers because they value more fairness, satisfaction, trust, and control. Moreover, when customers share their data, they analyze the costs of sharing them and their benefit in change, and if the costs surpass the advantages, these concerns become serious (Culnanand and Bies, 2003; Planggerand and Montecchi, 2020). Culnanand and Bies (2003) argued that companies could use `the platform for privacy preferences project (P3P), a protocol designed to provide websites a way to represent privacy policies. This means companies have to use a P3P vocabulary for customers to understand the purpose of gathering the data, how the company is going to use the data, and all the information that the customers need to know. Using P3P, there will be an increase of trust and a decrease of privacy risk perceptions of customers, leading to the reduction of customers´ concerns. According to Planggerand and Montecchi (2020), companies need to examine from where comes these concerns and how they can prevent them. Therefore, privacy concerns may be from a particular website (Eastlick, Lotz, and Warrington, 2006), customized ads (Bleier and Eisenbeiss, 2015), innovative technologies (Inman and Nikolova,

2017), different channels of selling (Zhang et al., 2010), and targeting the children (Lwin et al., 2008). Furthermore, David Stewart (2017) suggests the customers read the privacy policies and have the information of nine-question before sharing their data:

1. What is the benefit of sharing the information?
2. To whom will the information be given?
3. At what level of detail?
4. For what purpose?
5. For what period?
6. How private is the information?
7. Is secondary use of the information permitted?
8. What are secondary uses of the information possible?
9. What are the consequences of secondary use?

Firstly, it is crucial that the customers know what information has been approved to share; the default for the sharing decision should involve an opt-in. Secondly, the decision to opt-in has to be communicated by the appropriate factors that affect sharing the information. Thirdly, considering that contingencies change, the customer has the right to delete the shared data. This theory is more coherent with privacy in the EU than in the United States (Directorate-General for Internal Policies, 2015).

Companies work to satisfy customers and to offer them customized products related to their desires, but this can still cause privacy concerns (Zhang et al., 2010). When companies ask for customers´ personal information and use them, privacy concerns may arise, harming their key performance indicators (KPI), which evaluate the company´s performance (Plangger and Watson, 2015). Moreover, when the company handles sensitive personal information, privacy concerns come into place, and the company is the one that faces the consequences, which include losing their customers and losses in their economic profits. Customers are faced every day with marketing messages, and they learn how to react to them (Wright, 1986). Generally, customers respond with various defensive tools (ex: privacy concerns), which affect how they think and act (Hardesty, Bearden, and Carlson, 2007). Thus, the way they think will affect the evaluation of recognized risk (ex: misuse of their data), affecting their trust. The thought will also bring the action that may

cause, on the one hand, false information or, on the other hand, the refusal to disclose their data and purchase.

2.2.2 The impact of innovations on technology cause privacy concerns

The rapid development of technology has created new ways of getting customers' data. Firms are constantly attempting to increase their consumers' personal information by combining it with users' data obtained from another firm (Schneider, Jagpal, Gupta, Li, and Yu, 2017). Firstly, companies use retargeted ads which are used for particular products and services. In such cases, firms provide customized products for customers who have shown interest in their browsing history (Bleier and Eisenbeiss, 2015; Lambrecht and Tucker, 2013). Reusing the past browsing history in a new context can cause privacy concerns because customers lose trust in the company (Bleier and Eisenbeiss, 2015).

Moreover, connected devices create new types of data which bring privacy concerns. Customers´ data are more visible to the companies when they use many devices that track their location, usage, and other information (Hoffman and Novak, 2018; Porter and Heppelmann, 2014). Smart devices gather data and share them with other devices and can make choices based on the information that they have. Moreover, customers will slowly get used to smart devices and how they can help customers to meet their needs and wants (Hoffman and Novak, 2018). However, these data gathered can be used in a new context and cause privacy concerns. For example, fitness apps get user data regarding their fitness track, progression, and other information that this app can get. If these types of data will be used in a new context and for another purpose, customers´ privacy concerns may arise.

Another example is the iRobot vacuum, a smart home device, which raised privacy concerns since the company had planned to sell to third parties the floor map data (Astor, 2017). In this case, it was intended to misuse data gathered, where these data should be used for improving the device's performance.

In addition, an example is a business that sells tickets for different events, including sports, theaters, music, that have first-data for its customers and their purchasing behavior. To expand the data provider requires access to possible customers. For this reason, the firm contact, for example, a social media provider such as Facebook that has detailed information for its users ((e.g., demographic and media consumption information) and shares its users' email, including each users´ segment categorization. Linking the firms´

data with the social media data provides "second-party data". From the second data, both parties have profits. The firm acquires an improved collection of demographic and media consumption data for its existing clients, providing more customized and effective marketing. The social media provider gains by selling its data in ways other than its advertising strategies (Schneider, Jagpal, Gupta, Li, and Yu, 2017).

The examples above show how new types of data are collected and used in a way that the customers do not approve. It seems that people are not as private as they think from technology innovations. For example, Wang and Kosinski (2018) stated that they could find the individual´s sexual orientation from the Facebook pictures, and Crandall et al. (2010) showed that hidden social relations might be inferred from social media. Consequently, companies can find data and understand customers´ preferences from different sources without asking them and having the risk of privacy concerns.

2.2.3 Solutions for privacy concerns

Even though there has been much research in privacy, privacy concerns are a real problem nowadays. For this reason, some solutions are available in order to decrease these concerns. Firstly, the World Wide Consortium (W3C), the central organization for the World Wide Web, was founded in 1994 and is a community for member companies that develop standards so websites can look and work at the same level on all websites. The mission of W3C is to lead the Web to its potential by setting standards and guidelines (Christensson, 2010). To achieve their fullest potential, companies can adopt the website standards created by the W3C, and software engineers can guarantee that the companies work with the latest technology. Using the W3C standards, many websites can interpret the newest HTML and CSS code version. Moreover, The World Wide Consortium gives directions of privacy and security that companies need to follow. It regulates standardization work to better support online customer privacy and establishes expertise in privacy-by-design for websites. In addition, the W3C monitors privacy concerns that affect the web, examine possible areas for new privacy work, and gives direction and advice for making privacy in standard requirements. To work everything by their standards, the W3C has a staff that deals with users to access the websites and be protected (Jordan, 2013). Therefore, users get better accessibility, security, privacy, and internationalization.

Websites that use W3C standards are faster to load, and they can use it without any cost because it can be downloaded for free. This organization has organized different workshops for companies regarding customers´ privacy, such as the workshop on permissions and user content (2018), on privacy and user-centric controls (2014), the next step on trust and permissions on apps (2014), web tracking and user privacy (2011), etc.

Moreover, another solution is The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium. It allows companies to declare the privacy policies in a standard format that the customers can understand, and it gives customers more control over their data. Moreover, P3P specifications allow users to choose whether and under what conditions to share their private information. The P3P is developed to do one thing- to inform customers, simply and automatically, a company´s privacy policies and how they compare with the customers´ privacy preferences. Regarding this platform, The New York Times (2000) wrote: "The World Wide Consortium, the group that designs standards for the Web, is creating a new way (P3P) for websites to transmit to transmit the site´s privacy policy automatically, and allow users to signal only the information they are willing to share."

Furthermore, there are nine topics in total that P3P includes. The first five topics give details about the information tracked by the website, and the last four describe the internal privacy policy.

- Who is gathering the information?
- What information is gathered?
- What is the purpose of this data collection?
- What information is shared with third parties?
- Who are the information recipients?

- Can the customer change how his information is used?
- How are the conflicts solved?
- What is the policy for retaining information?
- Where can be found the detailed policies in "human-readable" form?

Using P3P, websites can convert their privacy policies into a standardized, machine-readable format that a user´s browser can easily interpret. This conversion can be made manually or with automated tools, and when it is done, the server automatically informs the user that the website is using P3P. This implies a platform that will help the customers understand the privacy policies and help companies gain the customers´ trust. Regarding the usage of the P3P, on the day that this platform was launched, the Commissioner for Data Protection and Access to Information, Dr. Dix (2002), stated: "The Platform for Privacy Preferences (P3P) is the most sophisticated proposal that has been made from a technical perspective so far to enhance privacy protection on the Web…(while) it cannot replace a regulatory framework of legislation, contracts, or codes of conduct."

Thirdly, the P2U (Purpose-to-Use) is a structure for privacy-aware user data trading based on the idea of adaption. Using this method, the data can be shared between applications according to the privacy policies set by the customer (Iyilade and Vassileva, 2013). It indicates the type of data gathered, the purpose, the time that the data will be used, and with whom are the data shared. This structure includes four active members: the customer, who shares the personal data, data providers that gather the user data and transfer them to other applications for secondary use; data consumers that are the second user data; and a data broker that guarantee that everything is done according to the customers´ references (Iyilade and Vassileva, 2014). Moreover, P2U is based on the "purpose-relevance-sharing principle," meaning that the data can be shared only if they are relevant to a specific purpose. Therefore, the platform can reuse and share the data after gathering them in order to meet different objectives that are profitable for the customers and the companies. Furthermore, P2U includes eight elements with attributes explained below (Iyilade and Vassileva, 2014).

1. Policy element

Policy element is the key of P2U. It encapsulates the other element in the privacy policy. This structure has at least one element and is developed by a provider for one user with one or more purposes. Moreover, two attributes can be stated in the element: (1) name (mandatory) – P2U policy name; (2) `discurl´ (optional) – position of the human-readable version of the policy.

2. Data provider

This element provides information about the person that has issued the policy. It includes two attributes: (1) name (optional)- the name of the provider; (2) `Provid´ (mandatory)- a specific identifier for the provider.

3. User

This element determines the person for whom the policy is. It contains two attributes: (1) name – the username of the person who uses the website; (2) userid- a specific identifier for the customer.

4. Purpose

The purpose element determines the sharing purpose, the company that gathers the data, the period of time that the data will be used, and the kind of information appropriate for a specific purpose. Furthermore, a P2U privacy policy can have one or more purpose components. This element has two attributes: (1) name (mandatory) – a term that identifies the reason for sharing the data; (2) puid – a specific identifier for the purpose.

5. Data consumer

The third-party company is indicated by the consumer element. Data consumer elements have two attributes: (1) name - indicate the customer name; (2) consid – a specific customer identity.

6. Retention element

The retention element determines the maximum retention period, which is given in days for the given purpose. The attribute´s duration is required. Moreover, another optional attribute specifies if the customers´ retention duration is negotiable or not.

7. Data group

The data-group element specifies the collection of data that may be shared for a specific purpose. Furthermore, the data group may have variations, each with its own set of sharing limitations. By giving various variants, users and data providers can negotiate the data possibilities that best fit the users´ demands while not risking the data provider’s usage

policy. In addition, every variant has a specific *groupid* attribute. The data group contains a Boolean negotiable characteristic that specifies if the data collected within the data group are negotiable or not.

8. Data

This element is used to describe the users´ personal information inside a data group. Moreover, the data element contains additional attributes that limit how each user´s data can be used inside the group. These other attributes include: (1) ref (required) – a specific identifier for the data; (2) expires (optional) – specifies an expiration date for the data.

These solutions offer a regulated market where companies are transparent with customers. Moreover, the customers can share their data without being suspicious of their personal information misuse or transmitting it to third parties without their permission. Nevertheless, the solutions have the challenge of guaranteeing that data consumers stick to the agreement for data sharing. The issue is equivalent to enforcing copyright agreements. Iyilade and Vassileva (2014) claimed that enforcing compliance with privacy policies by data users can be accomplished through the use of trust and reputation mechanisms. Therefore, these mechanisms are applied in different sectors, such as e-commerce and peer-to-peer networks, to manage interactions and reduce misbehaviors.

2.3 Companies´ strategies toward privacy

As firms' accessibility to customers' personal information has increased, protecting their data is becoming more vital. A study was done by Gomez et al. (2009) for the top 50 most visited websites, and the results showed that the companies use the customers´ data for personalized ads, and big companies like Google, Facebook, and Microsoft share customers´ data with associated companies. Therefore the use and the sharing of customers´ personal information will bring customers concerns. In 2007, the Ponemon Institute asked 786 American customers, and 62% of them said that they were notified of their data being lost or stolen, and 84% told that they were concerned due to this misuse of their data (Smith, Dinev, and Xu, 2011). However, companies make data protection based on a tradeoff between profits and privacy (Schneider, Jagpal, Gupta, Li, and Yu, 2017). As previously mentioned, companies that share data with third parties may cause privacy

costs such as loss of customer trust, legal penalties, costly regulations. Therefore, companies need to choose strategies to achieve the tradeoff between profitability and privacy (Rust and Chung, 2006).

Customers´ personal information is crucial for companies to stay competitive, build marketing strategies and business models (Holtrop et al., 2017). In addition, companies use customers´ data to innovate new products and services (Porter and Wagman, 2014) and sell them to target customers (Bleier and Eisenbeiss, 2015). Customers´personal data make it easier for companies to make decisions in management terms and helps them for economic profits (McAfee and Brynjolfsson, 2012). For example, Google uses customers´ data in Gmail, Maps, Calendar, Chrome, Youtube, and Google Search to provide companies with targeting opportunities and innovative new products. Some strategies that companies use to get the customers´ data are: tracking transactions using loyalty programs (Blattberg and Deighton, 1991; Turow, 2008), getting data from digital behavior (Bucklin and Sismeiro, 2009), keep records of customers interactions (Lyon, 2007; Turow, 2008), and employ location technologies (e.g., GPS) to control the customers (Junglas and Watson, 2008).

Considering the customers´ privacy concerns, companies need to work on understanding their customers better on the way they think, feel and behave. Some researchers use the theoretical models to understand customer economics of data privacy (Rust et al. 2002). The researchers assumed a free market where there were no privacy regulations, and they put a fee for customers to protect a particular number of data. The same model was followed by Conitzer et al. (2012), using the current customers´ data to put price discrimination in future purchases. Companies use this strategy to charge customers different prices depending on what the firm can get from the customer. From this model, it was shown that the companies profit more when the buyer is free to be anonymous because price discrimination can be placed in such cases. Thus, it is more profitable for customers to share their data and get discounts and offers regarding the products and services offered. Moreover, some researchers examined the behavior of some companies given the customers' data by using a mathematical model (Casadesus-Masanell and Hervas-Drane 2015). This model studies strategic cooperation generated by customers sharing their data and sharing that information with companies, attempting to find the best option to get more customer information and other revenues compared to their competitors. In the end,

it was found that privacy can weaken the competition when customers are heterogeneous; in this way, companies can change their privacy practices from what is said on the privacy policies. These models show how companies can use privacy as a strategy.

The number of companies failing to protect their customers' information is rising (Ponemon Institute 2015). Many researchers claim that privacy concerns can cause loss of profits in economic terms because of a decrease in sales (Pavlou, Liang, and Xue, 2007), foreclosure of data (Heng, Jiang, and Choi, 2013), and risk of litigation (Son and Kim, 2008). Firstly, privacy concerns negatively affect revenues since the customers choose not to purchase more from these companies because they do not trust anymore (Pavlou et al., 2007). Customers do not buy to a company if they have the fear that the company is going to share their data with third parties. Moreover, privacy concerns make customers not take advantage of customized products and services (Baruh, Secinti, and Cemalcilar, 2017). Furthermore, customers who do not like personalized ads may opt-out from receiving them and may use ad-blocking technology, bringing a lot of losses to advertising-based platforms (Bleier and Eisnbeiss, 2015; Tucker, 2014). Secondly, if the company fails with the strategy and customers have privacy concerns, they will be less likely to share their data (Stutzmann, Acquisti, and Gross, 2013; Jiang et al., 2013) and remove their data to the website (Son and Kim, 2008). Thirdly, customers´ privacy concerns can even lead to legal actions against a company (Son and Kim,2008). For example, in 2018, Vtech, a global supplier of electronic learning products for kids, was fined $650,000 for revealing childrens´ data. This company had gathered information such as children's names, birthdays, and genders without the approval of their parents and put them on their server. This means that a company's probability of litigation risk is higher if the data are from a group with greater privacy protection (e.g., children) (Paul, 2018).

Bowie and Jamal (2006) concluded that this system is not guaranteed in a study on whether US companies should tighten the data protection policies. However, they argue that if privacy policies are well-composed and companies have self-regulation, it is sufficient to protect customers' information. Furthermore, corporate privacy policies are crucial for customers to know the data's collection, use, and protection. According to some researchers, engaging customers on emotional and behavioral levels will bring long-term relationships between them (Patterson, Yu, and de Ruyter, 2006; Brodie et al., 2011). Engaged customers may play an active role in giving recommendations for a particular

item or service and developing new products. Unlike the traditional relation approaches, involving ‘‘participation’’ and ‘‘involvement,’’ engagement relies on the presence of focal active customer interactions with unique engagement objects (e.g., a brand) (Brodie et al., 2011). Moreover, Patterson, Yu, and de Ruyter (2006) proposed four main customers´ engagement components based on organizational behavior research: (a) absorption: a customer's level of concentration on a central engagement object, such as a company, reflecting the cognitive aspect of engagement; (b) dedication: a customer's feeling of connection to the company, reflecting the emotional aspect of engagement;(c) vigor: a customer's level of energy attached to the company; and (d) interaction: two-way communication between the subject and object of a focussed engagement. The vigor and interaction components correspond to the behavioral aspect of the engagement. In addition, Brodie et al. (2011) have argued five themes that serve as a starting point for developing a general description of customer engagement. The first theme supposes that customer engagement represents a customer's individual psychological state due to his unique interactions with a focal engagement item (e.g., a brand). The second theme says that customer engagement happens as part of larger, dynamic processes represented by value co-creation. The first and second elements differentiate engagement from the "participation" and "involvement" notions, as the latter does not adequately capture the concept of interactive experiences. A third theme sees engagement as key to service connections, with other relational ideas serving as specific determinants or effects of engagement. A fourth theme argues that engagement is a "multidimensional—cognitive, emotional, and behavioral—concept," where the specific cognitive, emotional, and behavioral components are expressed differently depending on the stakeholder (e.g., customer). The final theme claims that engagement happens within particular types of context-dependent variables resulting in varying customer engagement levels. Achieving customer engagement requires much investment from the company side to know and understand customers, how they feel, how they think about privacy policies, and their concerns. Companies need to focus more on serving and satisfying present customers´ wants and attracting promising customers rather than collecting customers´ data (Linoff and Berry, 2004). Relationships between two parties are built upon honesty; that is why companies need to decrease the demand for customer surveillance to protect this relationship and gain a competitive advantage (Plangger and Watson, 2015). Moreover, to be successful, companies need to understand their customers' feelings, needs, and behaviors to design a surveillance strategy. Now, companies use cookies to track the customer's movements on their website

and get information from them (Laczniak and Murphy 2006). There are different forms to get their data using customer web tracking, creating customer profiles, and other marketing tools using the information on their profile (Nill and Aalberts, 2014).

According to Culnan and Armstrong (1999), customers are more willing to share their data when the procedures for using the information are fair. Therefore, as privacy is crucial to customers, they gain a competitive advantage by being transparent. In addition, Casadeus-Masanell and Hervas-Drane (2015) stated that companies might gain a competitive advantage by showing that their competitors care less about customers´ privacy, such as when Microsoft accused Google of misusing customers´ personal information. Another practice to achieve a competitive advantage is adopting `privacy-friendly` technology such as Google proposes an optional default search engine, DuckDuckgo, in many countries (Zhou, 2019).

Companies should not see tight privacy policies as a cost but as an opportunity to improve customer experience and bring loyal customers. Martin and Murphy (2016) suggest some strategies that companies should follow for data privacy:

1. Companies should authentically prioritize customer information to get customer trust and long-term relationships with them.
2. Companies should interact transparently with their customer regarding their data privacy.
3. Companies can fulfill privacy-promoting practices that means they can use them in all aspects within the firm to have a good performance.
4. To have a positive performance, companies should focus on what they do right, respecting the privacy policies.
5. Companies should follow privacy practices to have long-term benefits; otherwise, they will fail to attract customers.
6. Finally, companies should follow customers' trust as a strategy. Even it needs time, it will bring the companies a good performance.

   When customers have high privacy concerns, they may ask the help of the law to apply stringent regulations (Milberg, Smith and Burke, 2000). The target of these regulations will be the set of a limit for tracking and using customers´ data. The area which can be more affected by the set of rules is online advertising for three

reasons: (1) by its nature, it is already monitored, and it can be documented (Goldfarb and Tucker, 2011); (2) as it is the area that uses digital data, so it is the first to experience the regulations; (3) it is the sector that uses mainly the data. The primary legislation that explains the usage of data in advertising, the European "E-Privacy Directive" (EC/2002/58), is studied by Goldfab and Tucker (2011). This "E-Privacy Directive" limits the companies to track customers for online behavior, making it challenging to gather and use the customers' personal information. Goldfarb and Tucker (2011) analyzed the responses of 3.3 million people to 9596 advertising campaigns to see what effects the regulations had on online advertising. The results showed that online ads became 65% less effective after the regulations. Moreover, another study done by Goldfarb and Tucker (2011) showed that websites with general content (e.g., news) had a decrease in the effectiveness of the online ads compared to the specific websites (e.g., travel websites) after the E-Privacy Directive. When a customer visits a travel website, he has already put himself in a particular market, so the website does not get data from the past browsing behavior to customize ads. Furthermore, Lambrecht (2017) showed that the Directive had decreased the investment in online news and online advertising in the EU.

Moreover, in 2018, Johnson et al. examined self-regulation, the case of AdChoices. It was introduced in 2010, and it gives the customers the opportunity of the "choice and notice" about the usage of their data. AdChoices is located in the top-right of the ad, and customers can click on it to know how their data is used for customized ads. In addition, customers have the opportunity to opt-out their data and only see general ads in general.

The latest regulatory is announced in 2018, EU General Data Protection Regulation (GDPR). Its purpose is to protect the customers' personal information and give individuals more control over their data. Unlike the regulations before, GDPR includes names and addresses as customers´ data and refers to as personal data also any information that is related in/directly to an individual, such as IP addresses (Bleier, Goldfarb, and Catherine, 2020). The announcement of this regulation affected many companies in the EU because of its stringent rules.

Furthermore, children are also involved in privacy concerns, and for this reason, in 2000, the "Children's Online Privacy Protection Act" (COPPA) was announced. It aimed to protect the children´s privacy rights by asking for approval

from parents before gathering the data. However, a study done in 2013 examined 100 children's websites, and it showed that only half of them respect the COPPA requirements (Cai and Zhao).

The regulations have more negative effects on small companies than big ones (Bleier, Goldfarb, and Turcker, 2020). Big companies can make the regulations in their favor because they have enough resources to engage politically (Rehbein and Schuler, 1997). Moreover, big companies have more experience applying new regulations than small companies (Hillman and Hitt, 1999). Furthermore, new regulations have costs for adopting them, which are higher for small companies. Julie Bernard, chief marketing officer of Verve, a mobile marketer, stated: " The implications and ramifications of GDPR compliance will challenge numerous organizations (…) with resources on scales than, say-and in particular-Facebook and Google" (Bleier, Goldfarb and Tucker, 2020, p.472).

2.4 Privacy and ethical concerns

Technology has a massive effect on the collection, processing, access, and transmission of information, and its vital ethical concerns include accessibility/inaccessibility and information manipulation. It enables more excellent and concurrent access to data. As a result, others gain simple access to a person's data. On the other hand, a user can be prevented from entering information necessary stored in digital using various security techniques such as passwords (Britz, 1996). The employment of technology in the data processing system cannot be seen as ethically neutral. Christians (1999) describes technology adoption as "a value-laden process" (p.7). Kluge (1994, p.337) argues that "technology has changed the ontological status of a document with accompanying ethical implications." He referred to the manipulation of data through the use of technology. Brown (1990, p. 3) expressed that the ethical issues arising by the use of technology do not imply - as he puts it – "...that we should rethink our moral values."

Currently, protecting data privacy is a critical and challenging issue. This protection is essential since the technology-driven and information-intensive environment is so pervasive. Data security becomes a key information security function, assisting in designing and implementing methods to ensure that privacy policies, guidelines, and procedures are correctly expressed, complied with, and implemented effective measures. Lee,

Zankl, Chang (2016) stated that the privacy policies need to be "technically efficient, economically/financially sound, legally justifiable, ethically consistent and socially acceptable since many of the problems commonly found after implementation and contract signing are of a technical and ethical nature, and information security decisions become more complex and difficult" (p.2).

In the evaluation of privacy ethics, Foxman and Kilcoyne (1993, p.106) have cited: "Companies must make an active commitment to ethical behavior in this area if restrictive legislation is to be avoided." Even though nowadays companies have regulations in the collection and the sharing of these data, many researchers claim that there is a need for improvements (Laczniak and Murphy, 2006).

The information required may influence how the customer responds, especially when the data is compassionate (Smith et al., 2011). Bloom et al. (1994, p. 2013) suggested two questions that companies need to take into account:

1. "Should a company be allowed to acquire and store information about individuals without their knowledge or consent?"
2. "Should a company be allowed to disclose information about individuals to other parties without their knowledge and consent?"

In 2020, while companies worldwide have enormous, near-unfiltered availability to users' personal information, companies enter a new type of question (Ritter, 2020): What legal and ethical responsibilities do they have to preserve the data they gather and use?

Regulation such as the General Data Protection Regulation (GDPR) of the European Union is the first phase in pushing organizations to implement ethical data practices. Companies within these countries are required to reveal to a person upon request all data they have acquired on that user, along with a detailed set of third parties that the information was exchanged. Furthermore, whenever the user requests that their information be deleted, an organization complies or faces legal consequences (Ritter, 2020). Legal penalties for information privacy violations can amount to up to 4% of a company's sales, which might be more than the benefits generated by a second-party marketing deal(Gilbert, 2015). Nevertheless, successful security methods one day may become useless the next.

Due to the continuing development of big data gathering, transforming how users are handled from product to partner will help firms achieve their required ethical requirements to utilize the information appropriately and earn their users' trust.

Moreover, a code of conduct is essential when talking about ethics because it serves a range of functions, one of which is to guide companies given a set of guidelines and norms. When properly formulated and stated, a code of conduct may assist in communicating policies and standards effectively. For instance, such regulations can help to prevent future unpleasant behaviors. Despite the code's good intent and formal implementation, it cannot ensure greater ethical behavior on its own. Additional procedures must be in place to properly implement the guidelines and practices (Lee, Zankl, Chang, 2016). Therefore, companies of all kinds have a code of conduct, and they use their distinct policies. Nevertheless, existing codes are typically technical, economic, and legal and are insufficient for ethical, social, and ecological considerations that seem fast-evolving and are rising to the top of corporate and information technology administration agendas. The Hexa-dimension framework is offered as a broad guideline for developing a code of conduct. This structure is composed of two main components: a conceptual Hexa-dimension measurement for assessing legal validity, social perception, environmental balance, ethical acceptability, technological efficiency, and economic viability, and a system for implementing the guideline (Lee, Zankl, Chang, 2016). The implementation process is divided into three critical phases, which include the following:

- Determine the essential aspects that affect the target users. Impact on the environment, for example, is crucial for a factory but may likely be neglected by a data security organization.
- Annual performance evaluations should include an analysis of the ethical integrity of conduct.
- Establish a strategy for measuring each factor in order to evaluate, prioritize, and balance them. The elements will assist in deciding the actions necessary to assess effectiveness.

If written and communicated correctly, the code can aid in spreading policies and principles across the company and beyond, thereby promoting ethical organizational, appropriate behavior.

There are two main reasons why data security professionals require efficient and realistic direction when designing information privacy protection guidelines (Lee, Zankl, Chang, 2016). One is that the information security role is becoming more complex in a technology-driven environment as new risks emerge. Secondly, data protection is becoming a concern for information management as privacy violations continue to happen. Taking an ethical approach to privacy can assist companies in developing and improving their code of conduct, taking into account privacy ethically, and building a code of conduct for protecting sensitive data.

With the increased availability of personal information, it is even more critical to express a sense of trust to customers. Instead of just adhering to privacy policies, evaluate if the personal information gathered is used correctly. Companies need to balance the importance of ethics of the firm against the profits of the data chosen to pick (Brown, 2020).

It is important to mention the Social Contract theory (SC) when discussing privacy ethics. This theory is used to solve ethical issues that may appear and explain the customer-company relationship (Dunfee, Smith, and Ross, 1999). In addition, SC is used to describe the customers' behavior regarding privacy. (Culnan and Bies, 2003). The main principle of Social Contract theory states that "norm-generating microSocial Contracts must be grounded in informed consent, buttressed by rights of exit and voice" (Dunfee et al. 1999, p. 19). It makes companies to be transparent with the customers if their privacy practices are controlled by Social Contracts (Donaldson and Dunfee,1999). Meaning in a long-term relationship, there should be a common understanding of the contractual term and self-control over its duration.

According to the Social Contract theory, customer data sharing should consider the possible risks and harms. The customer believes that companies have fulfilled the privacy contract when they get personalized services and products (Chellappa and Sin, 2005) or are financially compensated (Gabisch and Milne, 2014). According to Caudill and Murphy (2000), if a company joins the Social Contract, they take the responsibility to manage customers´ data fairly. The Social Contract makes companies gather users´ data in an implicit form, meaning not in a legal or economic form which includes undefined responsibilities and asks for users´ trust toward companies (Caudill and Murphy, 2000; Culnan and Bies, 2003). This implies that customers share their private data because they trust that the company will follow the Social Contract. Furthermore, Social Contract theory

claims that *collecting* information is fair only when the customer´s *control* is granted and the customer has the *information* on how his data will be used (Malhotra, Agarwal, and Kim, 2004). The information exchange is done based on the agreed Social Contract; the control allows the customer to share his opinion or to opt-out the data; the information is used to make the customers understand the privacy practices. The data collection is seen as the Social Contract theory´s principle of distributive justice, assigned to "the perceived fairness of outcomes that one receives" (Culnan and Bies 2003, p. 328). Therefore, customers share personal information in exchange for the profit they get for doing so. If customers do not expect a positive outcome, they may refuse to share their data (Cohen, 1987). When it is given control over its data, customers see the use of data as fair (Tyler, 1994). Moreover, based on the Social Contract theory, customers' concerns are lower regarding how the companies use their data.

When talking about SC theory, Corporate Philanthropy, Corporate Social Responsibility, and Corporate Governance play an important role in achieving it (Brandley, 2017). Social Contract theory is important if the company wants to create a relationship with the customers. Corporate Philanthropy lies in meeting customers´ expectations and recognizing the value of giving back. Corporate Social Responsibility is linked with Corporate Philanthropy, but it is focused on sustainable innovation. It satisfies customers´ needs and wants by guaranteeing ethical standards. Last, Corporate Governance is about keeping the company on an ethical path. It includes the principles that the company should operate and the penalty if it fails. Corporate Government is vital to keep Corporate Philanthropy, Corporate Social Responsibility, and the Social Contract Theory as the most crucial part of a business strategy plan. As mentioned above, Social Contract Theory is vital for a company and its customers, but it has its pros and cons (Brandley, 2017). On the one hand, if the company uses this theory, it is protected from legal and reputation risks. On the other hand, if the company fails to treat the customers fairly, it will give the company terrible attention. Secondly, meeting customers´ expectations will create a long-term relationship with them that will be translated into profits for the company. On the other hand, meeting all this theory expectations costs money for the company because it needs to treat the customers fairly. Another issue is that it misleads the companies from their goal that is making money. Spending money and time on Social Contract Theory is money and time not spent in marketing, product development, and other profitable activities.

Despite pros and cons, Social Contract theory brings the customers and the companies closer and is a relationship where both parties profit.

Another theory related to the view of the fairness of the Social Contract theory is Justice theory, which is about establishing procedures to protect the customer's information when it is shared (Culnan and Armstrong, 1999). Many researchers have used this theory to judge customer experience and build relationships between customers and companies (Lin, Wand, and Chang, 2011; Wetsch, 2006; Tax, Brown, and Chandrashekaran, 1998). This theory explains how customers react to a company´s decisions and whether these decisions are fair. If the customers are treated fairly, they are satisfied and loyal to the company (Cropanzana and Bowen, Gilliland, 2007). According to some researchers, it is based on the belief that customers are affected by "fairness of procedures" rather than achieving "the favorable outcome" (McFarlin and Sweeney, 1992). Customers share their information in exchange for their benefits, including customized offers, rewards, and complimentary services. Researches have shown that fair information policies have effectively eased privacy concerns and have given firms the most significant benefit by getting more customers (Wirtz and Lwin,2009). When the customer believes in the fairness of the companies' privacy methods, they are more willing to share the information, which brings neither false information nor negative word of mouth.

2.5 Permission marketing

The marketing method mainly used is permission marketing which can be a solution for privacy concerns, focuses on customers' choices, and interactive collaboration between the company and the customers is permission marketing (Kent and Brandal, 2003). According to Godin, permission marketing is a type of marketing where the company gets the customers' approval before sending marketing messages (1999). This type needs an opt-in process where the customers agree with the terms and conditions. Permission marketing is linked to relationship marketing (Han, Hu, Bal, and Jang, 2005) and one-to-one marketing (Simonson, 2005). Relationship marketing is about the long-term relationship that the company creates with the customer, and one-to-one marketing is creating personalized products or services based on the customer's needs. This method aims to connect with the customer and build trust, making it worthy for all the parties (Kent and Brandal, 2003). In 1999, Godin states: "Consumers are now willing to pay handsomely to save

time, while marketers are eager to pay bundles to get attention... The alternative is permission marketing, which offers the consumer an opportunity to volunteer to be marketed to. By talking only to volunteers, permission marketing guarantees that consumers pay more attention to the marketing message (pp. 42–43)." According to some researchers, permission marketing lowers the confusion and search costs for customers and increases the accuracy of companies (Marinova, Murphy, and Massey, 2002). Nowadays, permission marketing has become very important with the development of mobile marketing and social media marketing. The most used methods by companies is mobile marketing because of omnipresence, location information, and immediacy, allowing customers to get the information anytime and anywhere. (Zhou, 2010). According to MacPherson, permission-based e-mail marketing will be the future of marketing because it is cheap and includes interactive communication between both parties (2001).

Permission marketing has been a term in direct marketing since the 1990s, but it changed personalized marketing messages with technology development (Chung, Rust, and Wedel 2009). Customers allow companies to send them customized messages through different channels. Different from traditional marketing, permission marketing has three particular characteristics (Godin,1999):

1. Customers who allow their names to be on the mail list will receive marketing messages.
2. The company sends personalized marketing messages.
3. The marketing messages will be more appropriate to what the customer wants.

These personalized and relevant messages to the customers are more efficient in keeping and getting new customers than just the random messages they get. According to Godin, there are five levels of permission which include: "Situation" permission which is for a limited time frame, and the customer allows the company to send him marketing messages for a while; "Brand trust" permission is in the phase where the company has gained the trust of the customer; "Personal relationship" is about the special relationship between both parties and selling products to the customer according to his needs; "Points permission" where the customer share their data with the company and is loyal to it; "Intravenous" is the last level of the permission where the customer has trusted the company their buying decisions. Many studies have shown benefits that companies have using personalized messages, such as the increased relevance for customers (Milne and Gordon 1993),

entertainment and informational value (Tezinde, Smith and Murphy 2002), and perceived control (Van Doorn and Hoekstra,2013). In 2001, MacPherson stated that the customers who have permitted the company to receive marketing messages are more loyal and profitable. For these reasons, permission marketing has had rapid growth in usage within different industries.

2.6 Conclusion of literature review and summary of hypotheses

This chapter summarizes the most critical concepts and theories necessary for examining privacy concerns and the customers' perception of privacy policies. Firstly, it was explained privacy and different constructs confused with privacy. Moreover, users' attitude regarding personal information disclosure was described, and the factors affecting privacy included trust, transparency, information required, comprehension, perceived control, and benefits. At the end of the first subchapter, the differences between the EU and US privacy policies were explained. Secondly, were described the privacy concerns and the concerns of customers regarding the collections of their data, the perceived control over their data, and the awareness of how the collected information is used. In addition, the role of technology in privacy concerns was analyzed and if it has made the situation better or worse. The last part of the second subchapter pointed out the current solutions for privacy concerns mentioning “The World Wide Solutions Consortium (W3C)”, “The Platform for Privacy Preferences Project (P3P)”, and “Purpose to Use (P2U)”. Despite the customers' side, companies play an essential role in privacy and privacy concerns. They try to have the customers' trust and to make them feel confident and close to the company. For this reason, companies design many strategies to keep the current customers and attract potential customers, which were explained in the third subchapter of the literature review. In the following part, it was discussed privacy ethics since ethical issues are an essential part when talking about personal data. Regardless of what the companies do for the customers and the strategies they follow, are they ethical in the things they do? In the last part, permission marketing was described as the most useful digital marketing method that could help companies decrease customers´ privacy concerns.

The literature review presented the hypotheses that will be analyzed in the methodology part that are:

H1: The higher the trust, the higher the probability of disclosing their personal data.

H2: The higher the trust, the lower the privacy concerns.

H3: The higher the level of sensitivity, the lower the probability that customers will disclose their personal data.

H4: The higher the comprehension of the privacy policies, the lower the probability that the customers will disclose their data.

H5: The higher the perceived control over their data, the higher the probability customers will disclosure their personal information.

H6: The higher the perceived control over their data, the lower the privacy concerns.

H7: The higher the perceived benefits, the higher the probability customers will disclose their personal information.

H8. The higher the level of trust, the higher the probability customers will reuse the website and recommend it to others.

Based on the hypotheses arising, Figure 1 shows the research framework and the variables that will be measured later in this research.

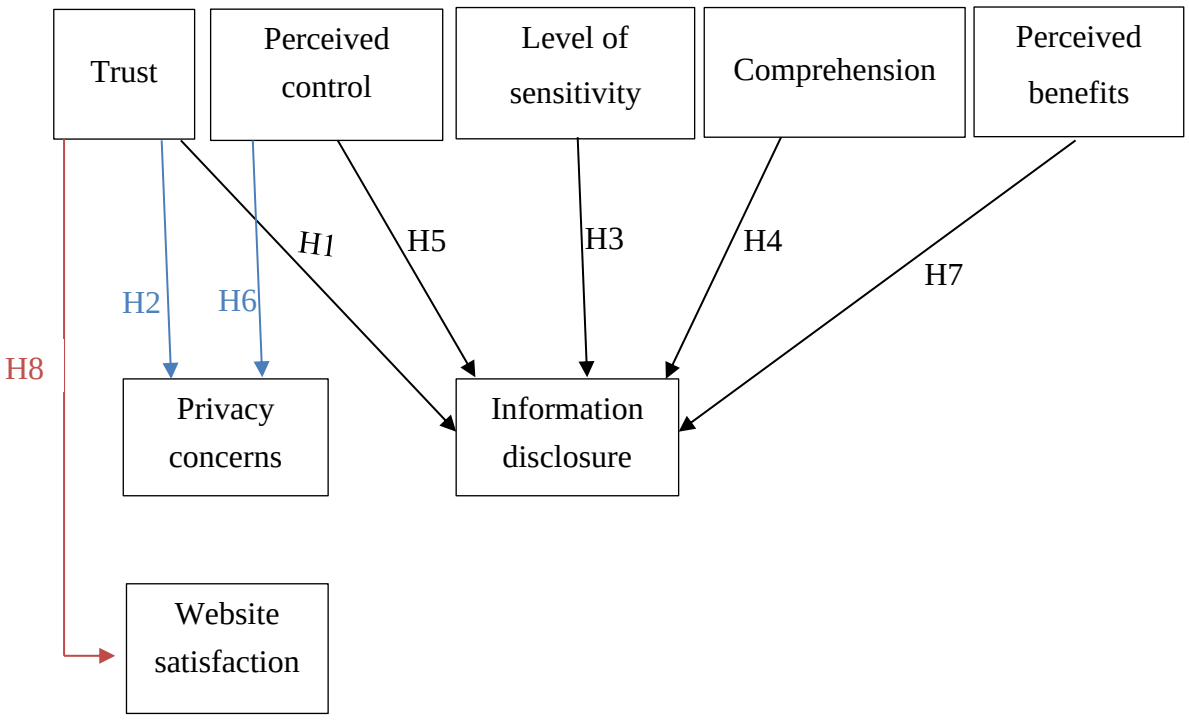


FIGURE 1 THE CONCEPTUAL FRAMEWORK OF THE STUDY

3 METHODOLOGY

This study chapter discusses the research method used to discover consumers' perceptions of privacy policies and the factors influencing privacy concerns and information disclosure. Furthermore, it will give adequate evidence to support the selected method and provide a detailed research design. Moreover, the research sample will be described, as well as the data collection process. Lastly, the data collected will be analyzed, and the analysis methods used will be discussed.

3.1 Study design and participants

The empirical part of the research examines customers' perceptions of a privacy policy and the factors that lead to privacy concerns and information disclosure. The research analyzes how customers perceive privacy policies using "The Economist" policy. This master thesis used a descriptive research design, a quantitative research methodology that responds to the how, what, when, and where questions rather than the why to the situation studied (Formplus Blog, 2021). To gather the data is used a descriptive online survey. The descriptive survey design examines multiple variables. However, unlike experimental research, the researcher cannot control the variables in this form of study (Voxco, 2021). The variables examined in this study are comprehension of the privacy policy, customer´s perception, trust, utility, perceived control, information disclosure, the sensitivity of information required, benefits, and privacy concerns. The online survey explained the relationship between the selected variables. It used a seven-point Likert scale, and the questions required a response ranging from "Strongly disagree" to "Strongly agree." The survey was conducted with a sample of adults in Europe who uses the internet. Various reasons can be cited to support the decision to perform quantitative research and, more specifically, a descriptive online survey.

Quantitative research is defined as the collection and analysis of numerical data. It is widely used to discover patterns, averages, forecasts, and cause-effect relationships between the variables used in the study (Voxco, 2021). Additionally, it is used to generalize the research outcomes to the population under investigation. In science, including social and scientific sciences, quantitative market research is commonly employed. Moreover, descriptive research enables academics to analyze a research topic's background properly.

A descriptive study methodology is advantageous in various instances, such as identifying and analyzing data trends: the descriptive study technique is used to quantify alterations in variables over time, enabling the identification and analysis of trends; comparing variables: descriptive study is used to evaluate various factors and the responses of various demographics to various variables; identifying subjects' characteristics: it can be applied to assess the subjects' multiple features that can involve qualities such as attitudes, behavior, etc.; and verifying existing terms: it can be an effective approach for verifying the accuracy of an existing state because it requires an in-depth examination of each factor before making conclusions (Voxco, 2021). Employing an online survey is a highly recommended and effective research technique when doing descriptive research. It has many advantages, including the responses are not biased, and the respondent needs a shorter response time.

The main reason this research uses an online survey is related to the topic as participants are anonymous, so their data are protected, and the target population includes people who use the internet. Moreover, in comparison to more traditional methods of selecting participants (in-person or by phone), online participants selection has several distinguishing advantages: greater data collecting efficiency, higher sample sizes, cost savings, and, most importantly, larger size and variety of the populations (Horswill and Coster, 2001). A well-designed online survey has the potential to reach practically everybody with web access and can generate extensive and diverse samples, which can make it easier to test hypotheses that would be difficult in a lab environment (Pollanen, 2014). In addition, online surveys help for the collection of the essential data to make appropriate conclusions regarding the proposed hypothesis. This method allows the researcher to get a large number of respondents from all over the world and relieves him from the interviewer´s job by automating data gathering, as well as providing great statistical power.

Online surveys may be conducted on the devices that participants use on a daily basis. Therefore, they can more appropriately represent both the environmental and technical circumstances encountered in real life than laboratory research. Numerous respondent selection services offer screening and customized limitations and eligibility requirements to ensure precise targeting, providing the researcher heterogeneity in participants (Paolacci, Chandler, and Ipeirotis, 2010). A researcher can collect data from hundreds of volunteers in a couple of hours (Crump, McDonnell, and Gureckis, 2013). However, lab

and online research may experience a decline in voluntary participation as a result of situational demand factors. Nevertheless, anonymity on an online survey can encourage respondents to share their free will, which results in a higher participation rate (Dandurand et al., 2008).

Many recent research has used the online survey research method to analyze the influence of different factors on customers´ privacy concerns and to gather the data. Some of the researchers that can be mentioned using this method are Aimeur, Lawani, and Dalkir (2015), who examined the effect of changing privacy policies on user trust,- Krafft, Arden, and Verhoef (2017) investigated why do customers (not) grant permissions, and Bleier and Eisenbeiss (2015) studied the importance of trust for personalized advertising. For this reason, in this study is chosen to be used an online survey for gathering the data.

This research employed an online survey which was created with soSci survey, a platform that does online surveys. The data collection period was from December 27th, 2021, to January 7th, 2022, providing a sample size of 95 participants. Respondents were acquired by posting the survey on different social media platforms and groups and sharing it with friends and relatives. Moreover, the respondents were asked to share the survey with people who met the criteria. The ratio of females exceeds males by a ratio of 62% to 37%. Adults can be classified into four age categories where the dominant age group is 28-25 years with 61%.

Table 1 shows the sample group divided demographically according to gender, age, and education.

		Number of respondents
Gender	Male	**35**
	Female	**59**
	prefer not to say	**1**
Age	18-25 years	**58**
	26-35 years	**32**
	36-45 years	**2**
	45+ years	**3**
Education	University	**77**
	High School	**16**
	Vocational School	**1**
	Apprenticeship	**1**

Total		**95**

TABLE 1: SAMPLE OF THE SURVEY

Out of 95 people who participated in the online survey, 35 (62 %) respondents were female, 59 (37%) male and 1 (1%) preferred not to say. The division of the respondents according to age were: 58 (61%) participants the age group 18-25 years, 32 (34%) were age group 26-35 years, two (2%) respondents were 36-45 years, and three (3%) respondents were 45+years. According to the education, 77 (81%) people had finished university, 16 (17%) respondents had the highest education high school, and two (2%) respondents had finished vocational school and apprenticeship.

3.2 Survey structure

The target population of the research includes the adults in Europe who use the internet. The non-probability sampling technique was used to collect data from the target population, specifically convenience sampling mixed with snowball sampling. Participants' data were gathered by posting the online survey on social media platforms and sharing it with friends and relatives, and the ones that participated were asked to share it with other people. This was the reason why non-probability sampling is chosen as it is based on the author´s subjective judgment and excludes random selection (Trochim, 2001). Using convenience sampling, the researcher chooses the respondents because they provide "convenient" data sources. In snowball sampling, the researcher asks the respondents to share the survey with people who meet the criteria (Trochim, 2001).

First, the participants saw a privacy policy taken from “The Economist” and needed to read it. The answers were based on their personal judgment, and the survey took about 5 minutes to fill. The online survey employed in this study was divided into three parts: the statements related to “The Economist” privacy policy, general statements regarding privacy policies, and demographic information.

Figure 1 shows the screenshot of “The Economist” privacy policy presented in the online survey.

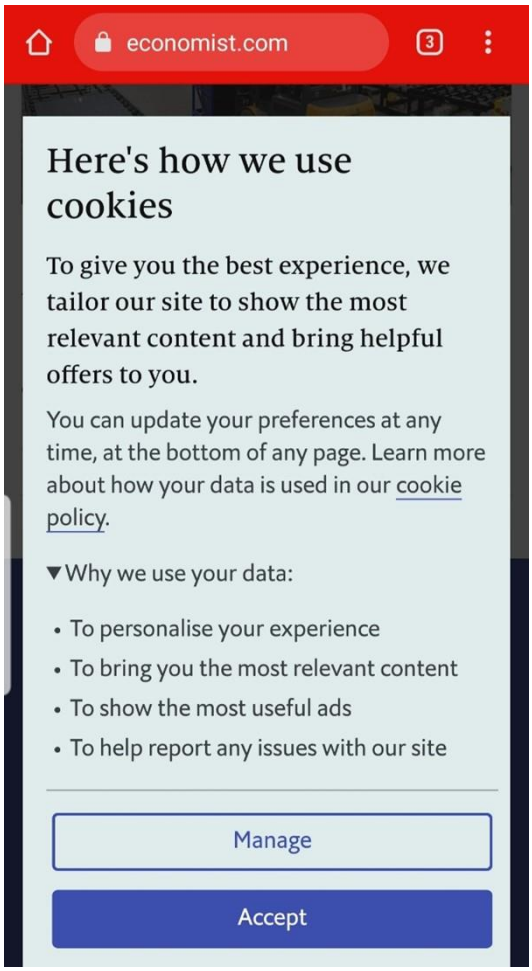


FIGURE 2: SCREENSHOT OF "THE ECONOMIST" PRIVACY POLICY

The questions related to the given privacy policy were to understand the participant's comprehension of the policy, perception of it based on what he read, and trust and satisfaction on this website. The second part focused on the previous experience of the respondents regarding privacy policies, and it was related to the control that the customers want over their data, by what conditions they disclose their personal information, the benefits they want after the disclosure, and the concern they have on privacy. Participants were asked to give their demographic data, gender, age, and education in the last part. They had the opportunity to choose the "prefer not to say" answer since their privacy was respected.

Various variables measured the constructs comprehension, customer perception, trust, utility, control, information disclosure, benefits, and privacy concerns in this survey. The following section elaborates in detail on the scales used in the current survey and why the respective scales have been deemed appropriate for the recent research.

The scale of measurement and questions related to the comprehension of the privacy policy and customers´ perception was adapted from the researches by Aimeur, Lawani, and Dalkir (2015) and Vail, Earp, Anton (2008). The questions were related to what the participants understood about the given website pertaining to the protection of their customers´ data. Furthermore, the questions related to the trust in the website were adapted by Liu, Lu, Marchewka, and Yu (2005) and Rifon, Larose, and Choi (2005). These questions analyzed whether they trust this company, considering the policy and actions that they could take for this website in the future. The following questions related to satisfaction with the website were adapted by Liu, Lu, Marchewka, and Yu (2005) and Schumann, Wangenheim, and Groene (2014). Moreover, the statements related to control that customers want to have over their data were adapted by Aimeur, Lawani, and Dalkir (2015). In addition, by Mothersbaugh et al. (2012) were adapted the questions related to the construct of information disclosure. The respondents were asked what information they were willing to share. The statements related to the construct of benefits were adapted by Morosan and DeFranco (2015) and Wang, Duong, and Chen (2016). In this part, participants were asked for what benefits they disclosed their personal information in exchange. Finally, the participants were asked for the privacy concerns adapted from Schumann, Wangenheim, and Groene (2014). All the items for each construct were measured on a 7 point Likert scale ranging from 1-strongly disagree to 7-strongly disagree.

3.3 Data Analysis

The data collected via an online survey were imported into SPSS for statistical testing of the data. The scale reliability analysis for each variable was conducted as a first step. From this analysis, Cronbach's Alpha showed the reliability of the adapted measurement scales. Secondly, to test the hypotheses proposed, was run the linear regression. After the results were given, it was shown if the hypotheses were accepted or rejected.

4 RESULTS

This chapter summarizes the results of the data gathered from the online survey.

4.1 Scale reliabilities

Each scientific instrument must be both dependable and valid to provide reliable measurements. These measurements are essential for the variables being tested to be easy to interpret. The degree to which a tool evaluates a construct among items and time points is referred to as reliability (MotiveMetrics Research, 2013). Reliability is measured by Cronbach's Alpha. It is a statistical measure of consistency reliability that approximates the actual score to error ratio in “Classical Test Theory”. The value of Cronbach's Alpha should be at least 0.7 and between 0-1. Therefore, a reliability analysis was conducted to guarantee that the measured variables were consistent. Table 2 below shows the reliability analysis's findings for each item.

The analysis findings showed that all concepts are reliable, as the Cronbach's Alpha value for each component is greater than 0.7 and between 0 and 1. Moreover, in this analyse were analyzed the values of "Corrected Item-Total Correlation" and "Cronbach's Alpha if item is Deleted." These data show if a particular factor positively affects the construct or whether it should be removed. "Corrected Item-Total Correlation" needs to be greater than 0.3, and all the variables in this research are greater than 0.3. Furthermore, the values of "Cronbach's Alpha if item is Deleted" should be compared with the value of Cronbach’s Alpha. In the cases that the value of "Cronbach's Alpha if item is Deleted" is smaller than the value of Cronbach’s Alpha, so it means that the item serves to the construct's reliability. If the value of "Cronbach's Alpha if item is Deleted" is greater than Cronbach’s Alpha´s value, the item should be deleted in order to improve the Cronbach´s Alpha. Overall, the items contribute to the reliability of the construct.

Construct & items measuring the construct	**Cronbach's Alpha if item deleted**	**Cronbach's Alpha**
Comprehension (adapted from Vail, Earp, Anton, 2008; Aimeur, Lawani, and Dalkir, 2015)		**0.775**
I read the entire privacy policy of the website.	0.753	
I feel confident in my understanding of what I read in the privacy policy.	0.733	
This privacy policy was too hard to understand.	0.845	
This privacy policy can be read quickly.	0.761	
I have the information for what purpose my data will be used.	0.706	
I have the information if my data will be shared with third parties.	0.720	
I have the right to opt-out my personal information.	0.745	
I have control over my data.	0.705	
Customer´s perception (adapted from Aimeur, Lawani, and Dalkir, 2015; Vail, Earp, and Anton, 2008)		**0.929**
Through this privacy policy, I think the website cares about my concerns.	0.910	
The website keeps customers´ interest in mind.	0.919	
Through this privacy policy, I feel close to the website.	0.912	
I feel secure sharing my personal information with this website.	0.920	
I feel that privacy practices are explained thoroughly in the privacy I read.	0.916	
I feel that this website protects my personal information more than other websites.	0.921	
Trust (adapted from Liu, Lu, Marchewka, and Yu, 2005; Rifon, Larose, and Choi, 2005)		**0.917**
The company is making an effort to keep my personal information out of the hands of unauthorized individuals.	0.896	
The company will not release my personal information about me without my permission.	0.895	
The company will inform me if the data are shared with third parties.	0.905	

The company will use my personal information as stated in the privacy policy.	0.918	
The company will give me control over my data.	0.906	
The company will protect my information from loss, misuse, or alteration.	0.893	
Perceived control (adapted from Aimeur, Lawani, and Dalkir, 2015; Hong and Thong, 2013)		**0.777**
Usually, I read the privacy policies when visiting websites.	0.779	
Usually, I understand the privacy policies.	0.754	
Usually, I am bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared.	0.710	
Usually bothered when I do not have control over the personal information that I provide on the website.	0.737	
Usually, I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction.	0.706	
Information disclosure (adapted from Mothersbaugh et al., 2012)		**0.729**
I am willing to provide personal information for personalized services.	0.637	
I am willing to provide personal information for financial incentives.	0.639	
I am not willing to provide personal information regardless of the benefits.	0.789	
I am willing to disclose personal information that is higher in sensitivity.	0.663	
I am willing to disclose personal information that is lower in sensitivity.	0.652	
Data Sensitivity (adapted from Rifon, Larose, and Choi, 2005)		**0.848**
I will disclose my name	0.835	
I will disclose my e-mail address	0.834	
I will disclose my date of birth	0.820	
I will disclose my family information	0.797	

I will disclose my date of credit card/banking/stock portfolio information	0.838	
I will disclose my medical information	0.808	
Benefits (adapted from Morosan and DeFranco, 2015; Wang, Duong, and Chen, 2016)		**0.931**
I will disclose my personal information if…		
the website can provide me with more relevant promotional information tailored to my preferences or personal interests.	0.913	
the website can provide me with the type of deals/ads that I might like.	0.913	
the website reduces my searching time to access the personalized services, products, or information that I need.	0.922	
the website can provide me with the convenience to instantly access the promotional information that I need.	0.912	
I feel that using the website is beneficial.	0.915	
Privacy concerns (adapted from Schumann, Wangenheim, and Groene, 2014; Bleier and Eisenbeiss, 2015)		**0.877**
I am concerned about my privacy in general.	0.869	
I am concerned about not having control over my personal information.	0.845	
I am concerned that my information could be used in ways, I could not foresee.	0.852	
I am concerned that the company will share my personal information with other parties.	0.842	
I am concerned about the (sensitive) information required.	0.846	

TABLE 2: RELIABILITY ANALYSIS

4.2 Testing of hypotheses

This chapter summarizes the findings of the SPSS hypotheses testing. Several linear regression analyses were run to analyze the hypotheses.

H1: The higher the trust, the higher the probability of disclosing their personal data.

	R	R^2	F	ß (constant)	ß (trust)	standardized ß
H1 Trust→Information disclosure	0.343	0.118	63.222 $p < 0.001$	2.715	0.362	0.343

TABLE 3 RESULTS OF REGRESSION ANALYSIS

Table 3 shows the results of the linear regression between trust and information disclosure. The value of R is 0.343, which shows a positive influence of trust on information disclosure. Moreover, R^2 value of 0.118 stated that trust accounts 11.8% of the variations in trust. The F-ratio is 63.222 with a significance $p < 0.001$, meaning that there is less than a 0.1% chance that an F-ratio this large would happen if there is no correlation between trust and information disclosure. The ß (constant) value is 2.715, showing that there will be at least a 2.715 level of disclosure of data observed when there is no trust. In addition, the ß value for trust shows that by an increase of 1 degree of trust, the degree of information disclosure will increase by 0.362. Last, the standardized ß is 0.343, which shows that with every increase of one standardized unit in trust, the disclose of the data will rise by 0.343 standardized unit, holding other variables constant. Moreover, the significance value is $p<0.001$, which is less than 0.05, so hypothesis 1 is accepted, meaning the higher the trust, the higher the probability of customers disclosing personal data.

H2: The higher the trust, the lower the privacy concerns.

	R	R^2	F	ß (constant)	ß (trust)	standardized ß
H2 Trust→Privacy concerns	0.135	0.018	8.759 p =0.003	5.097	0.108	0.135

TABLE 4 RESULTS OF REGRESSION ANALYSIS

The result of the linear regression detected a low positive influence of trust on privacy concerns (R = 0.135). R^2 value is 0.018, meaning that trust accounts for 1.8% of the variation in privacy concerns. The value of the F-ratio is 8.759, with a significance level of 0.003. This means there is a 0.3% chance that an F-ratio this large would happen if there is no correlation between the variables. In addition, the values of the coefficients are 5.097 for the constant ß, 0.108 for the ß for trust, and 0.135 for the standardized ß. The constant ß means that there will be at least a 5.097 level of privacy concerns observed when there is no trust. Therefore, if there is no trust, the privacy concerns are high. Moreover, the ß value for trust states that when the trust increases by 1 degree, the degree of customers´ privacy concerns will increase by 0.108 accordingly. In addition, the standardized ß is 0.135, meaning that with every increase of one standardized unit in trust, the privacy concerns will rise by 0.135 standardized units. Moreover, the model is significant since the p =0.003. Based on the values shown in table 4, hypothesis 2 is accepted.

H3: The higher the level of sensitivity, the lower the probability that customers will disclose their personal data.

	R	R^2	F	ß (constant)	ß (sensitivity)	standardized ß
H3Sensitivity→ Information disclosure	0.312	0.097	50.866 p < 0.001	3.138	0.295	0.312

TABLE 5 RESULTS OF REGRESSION ANALYSIS

Table 5 showed a positive influence of the sensitivity of information required on privacy concerns (R = 0.312). The value of R^2 equals 0.097, which tells that level of sensitivity accounts for 9.7% of the variation in data disclosure. Furthermore, the value of the F-ratio reports as 50.886, with a significance lower than 0.001. This means there is less than a 0.1% chance that an F ratio this large would happen if there is no correlation between the variables. The value of ß constant reads 3.138, which states there will be at least a 3.138 level of information disclosure observed when there is no sensitivity to the information required. The ß value for the level of sensitivity is 0.295, meaning that when the level of sensitivity increases by 1 degree, the degree of data disclosure will be increased by 0.295. In addition, the standardized coefficient ß result shows with every increase of one standardized unit in the level of sensitivity, the privacy concerns will rise by 0.312 standardized units (ß = 0.312). Last, the significance level is $p < 0.001$, lower than 0.05, meaning hypothesis 3 is accepted. For this reason, it can be assumed the higher the level of sensitivity, the lower the probability that customers will disclose their personal data.

H4: The higher the comprehension of the privacy policies, the lower the probability that the customers will disclose their data.

	R	**R^2**	**F**	**ß (constant)**	**ß (comprehension)**	**standardized ß**
H4 Comprehension→ Information disclosure	0.235	0.055	27.730 $p < 0.001$	3.327	0.222	0.235

TABLE 6 RESULTS OF REGRESSION ANALYSIS

The linear regression analysis result revealed a positive impact of comprehension of the privacy policy on information disclosure (R = 0.235). The R^2 value of 0.055 states that comprehension of privacy policy accounts for 5.5% of the variation in information disclosure. F-value equals 27.730 ($p < 0.001$), meaning that there is less than a 0.1% chance

that an F-ratio this large would happen if there is no correlation between comprehension and data disclosure. Moreover, the value of the coefficient ß constant is 3.327, determining there will be at least a 3.327 level of information disclosure when there is no comprehension of the privacy policy. The value of ß for the comprehension is 0.222, and it implies when the comprehension of privacy policy increases by 1 degree, the degree of information disclosure will be increased by 0.222. Furthermore, the value of standardized ß is 0.235, meaning with every rise of one standardized unit in the comprehension of the privacy policy, the information disclosure will rise by 0.235 standardized units. The significance is $p < 0.001$, so hypothesis 4 is accepted. Therefore, the higher the comprehension of the privacy policies, the lower the probability that the customers will disclose their data.

H5: The higher the perceived control over their data, the higher the probability customers will disclosure their personal information.

	R	**R^2**	**F**	**ß (constant)**	**ß (control)**	**standardized ß**
H5 Perceived control→ Information disclosure	0.256	0.065	33.089 $p < 0.001$	3.051	0.266	0.256

TABLE 7 RESULTS OF REGRESSION ANALYSIS

Results of table 7 identified a positive influence of perceived control and information disclosure (R =0.256). The value of R^2 is 0.065, implying perceived control can account for 6.5% of the variation in information disclosure. F-value is 33.089, which is significant at $p < .001$. This result shows that there is less than a 0.1% chance that an F-ratio this large would occur if there is no correlation between control and information disclosure. The constant ß value is 3.051, which means there will be at least a 3.051 level of information disclosure when there is no perceived control over the data. The ß value for perceived control is 0.266. It determines when the consumers' perceived control over the data increases by 1 degree, the degree of information disclosure will be increased by 0.266 accordingly. In addition, standardized ß is 0.256, which shows that with every increase

of one standardized unit in perceived control, the disclose of the data will rise by 0.256 standardized units, holding other variables constant. Last, the significance level is p< 0.001, hence hypothesis 5 is accepted.

H6: The higher the perceived control over their data, the lower the privacy concerns.

	R	R^2	**F**	**ß (constant)**	**ß (control)**	**standardized ß**
H6 Perceived control→ Privacy Concerns	0.256	0.066	33.197 p < 0.001	4.598	0.184	0.256

TABLE 8 RESULTS OF REGRESSION ANALYSIS

The analysis of hypothesis 6 found an influence of perceived control on privacy concerns (R =0.256). R^2 is 0.066, hence, perceived control accounts for 6.6 % of the variation in privacy concerns. Moreover, the value of the F-ratio is 33.197, which is significant at p< .001, showing that there is a probability of less than a 0.1% chance that an F-ratio this large would happen if there is no correlation between the variables. The coefficient ß constant equals 4.598, which means there will be at least a 4.598 level of privacy concerns when there is no control over the data. The ß value for perceived control is 0.184, implying when the consumers' perceived control over the data increases by 1 degree, the degree of privacy concerns will be increased by 0.184 accordingly. The standardized ß is 0.256, which shows that with every increase of one standardized unit in perceived control, the privacy concerns will rise by 0.256 standardized units, holding other variables constant. Furthermore, the significance level is p<0.001which is lower than 0.005, so hypothesis 6 is accepted. Therefore, the higher the perceived control over their data, the lower the privacy concerns.

H7: The higher the perceived benefits, the higher the probability customers will disclose their personal information.

	R	R^2	**F**	**ß (constant)**	**ß (benefits)**	**standardized ß**
H7 Benefits→ Information disclosure	0.366	0.134	73.057 $p < 0.001$	2.320	0.419	0.366

TABLE 9 RESULTS OF REGRESSION ANALYSIS

The linear regression shown in table 9 shows a positive influence of perceived benefits on information disclosure (R =0.256). Moreover, the value of R^2 equals 0.134 shows that benefits account for 13.4 % of the variation in information disclosure. The value of the F-ratio is 73.057, significant at $p < .001$, demonstrating that there is a less than 0.1% possibility of an F-ratio this large would happen if there is no correlation between perceived benefits and information disclosure. In addition, the value ß constant, 2.320, implies that there will be at least a 2.320 degree of information disclosure when there are no perceived benefits. The ß value for benefits is 0.419, and it means when the customer perceived benefits increase by 1 degree, the degree of the disclosure of personal data will be increased by 0.419 accordingly. This means that the perceived benefits increase the information disclosure significantly. Last, the value of standardized ß is 0.366, meaning that with every increase of one standardized unit in perceived benefits, the disclosure of personal data will rise by 0.366 standardized units, holding other variables constant. Concerning the findings, the perceived benefits significantly impact the information disclosure ($p<0.001$). Therefore, hypothesis 7 is accepted, so the higher the perceived benefits, the higher the probability customers will disclose their personal information.

H8. The higher the level of trust, the higher the probability customers will reuse the website and recommend it to others.

	R	R^2	**F**	**ß (constant)**	**ß (trust)**	**standardized ß**
H8 Trust→ Website satisfaction	0.404	0.163	73.853 p < 0.001	2.819	0.384	0.404

TABLE 10 RESULTS OF REGRESSION ANALYSIS

The value of R shown in table 10 is 0.404, implying a positive influence of trust on reusing the website and recommending it to others. R^2 value is 0.163, meaning trust accounts for 16.3 % of the variation in website satisfaction. Moreover, the F-value is 73.853, with significance at p < .001. This result implies that there is less than a 0.1% chance that an F-ratio this large would happen if there is no correlation between these variables. Furthermore, talking about the value ß constant, which is 2.819, shows that there will be at least a 2.819 degree of website reusage and recommendation to others when there is no trust. The value of ß for trust is 0.384, meaning when the customer´s trust increases by 1 degree, the degree of the website satisfaction will be increased by 0.384 accordingly. Therefore, trust significantly impact the reuse of a website and recommendation of it to others. Finally, the value of standardized ß is 0.404, showing that with every increase of one standardized unit in trust, the website satisfaction will rise by 0.404 standardized units, holding other variables constant. As the significance level is less than 0.05 (p<0.001), hypothesis 8 is accepted. As a conclusion can be claimed that the higher the level of trust, the higher the probability customers will reuse the website and recommend it to others.

4.3 Overview of the results of the hypotheses tests

Hypothesis	**Results**
H1: The higher the trust, the higher the probability of disclosing their personal data.	Accepted
H2: The higher the trust, the lower the privacy concerns.	Accepted
H3: The higher the level of sensitivity, the lower the probability that customers will disclose their personal data.	Accepted
H4: The higher the comprehension of the privacy policies, the lower the probability that the customers will disclose their data.	Accepted
H5: The higher the perceived control over their data, the higher the probability customers will disclosure their personal information.	Accepted
H6: The higher the perceived control over their data, the lower the privacy concerns	Accepted
H7: The higher the perceived benefits, the higher the probability customers will disclose their personal information.	Accepted
H8. The higher the level of trust, the higher the probability customers will reuse the website and recommend it to others.	Accepted

TABLE 11: THE OVERVIEW OF THE HYPOTHESIS

5 DISCUSSION AND CONCLUSION

Customers perceive various marketing messages as a violation of their privacy. For this reason, customers have concerns about their privacy when it comes to the collection and use of personal data (Dolnicar and Jordaan 2007). Privacy policies are the technique of how websites inform the users how they gather and use the data. The way customers perceive privacy policies may vary throughout customers' life, in different circumstances, based on their cultural values, age, experience, etc. (Brandimarte and Acquisti, 2012). Although customers have concerns about sharing personal data, only a few of them take the time to read them due to their length and difficulty in comprehension (Ermakova, Baumann, Fabian, and Krasnova, 2014). In addition, customers are overwhelmed with the complexity of policies (Stewart, 2017). Therefore, the time and effort required to read and comprehend privacy policies is a cost. As a result, the majority of consumers do not read these policies and are unaware of the data gathered (Richards and King, 2014).

To understand better what leads to privacy concerns and information disclosure, factors such as trust, perceived control, the level of sensitivity of information required, comprehension of privacy policies, and perceived benefits were examined. Many researchers have analyzed the relationships between these factors with privacy concerns and information disclosure. After reviewing the existing studies, these factors were based on some theories, such as the commitment-trust theory that plays a vital role in relationship marketing between customers and companies (Hunt and Morgan, 1994); the theory of planned behavior (TPB), which shows perceived control makes customers more willing to share their personal data (Ajzen, 1991); the privacy calculus theory which describes how customers evaluate perceived benefits and privacy concerns during the disclosure of information (Culnan and Armstrong, 1999); and last the theory of reasoned action (TRA) which says a user´s attitudes toward privacy and trust should shape his attitude regarding online transactions, affecting behavioral intents to engage online. (Albarracin, Johnson, Fishbein, Muellerleile, 2001). Moreover, many researches findings showed that data sensitivity is related to intimacy, where more intimacy is associated with information considered to be riskier to expose due to its tendency to lose (Lwin, Wirtz, and Williams 2007; Moon, 2000). Another factor analyzed was comprehension of privacy policies that

by many researchers was the main factor related to data disclosure (Aimeur, Lawani, Dalkir, 2015; Reidenberg et al., 2014). Based on the theories mentioned and the review of many studies, a conceptual framework for this study was developed.

This master thesis attempts to contribute to existing researches and extend it by investigating the customers´ perception of privacy policies and the factors that influence the privacy concerns and disclosure of customers´ data. Based on what is discussed in this research, two research questions were raised, RQ1, "How do customers perceive privacy policies?" and RQ2, "What factors affect the customers´ privacy concerns and information disclosure?". These research questions try to understand the customers' perception about privacy policies and what factors affect customers' privacy concerns and the disclosure of their personal data with the aim of creating a possible approach to help companies understand customers' behavior. To answer these research questions, an online survey was used to collect data from customers, based on the construct developed in the literature review. The survey included the factors that affect customers' concerns and information disclosure, such as comprehension, trust, benefits, perceived control, etc. The data collection period was 12 days providing a sample size of 95 participants.

As the main aim of this research was to see how customers perceive privacy policies, an evaluation of the participants´ responses was made. Based on the data collected, in general, only 43% of participants agreed that they read the privacy policies on general terms. On the other hand, 49% of respondents agreed about understanding policies. Based on the results, it can be concluded that most people do not read the privacy policies, and those who read them do not understand them. In addition, this causes the problem of not knowing what information is gathered and how it is used.

Taking into consideration " The Economist" privacy policy, 62% of respondents read the whole policy where 30% of them did not feel confident in the understanding, 61% understood it, and 9% were skeptical about their understanding. In addition, 32% found it difficult to understand, while 70% said it could be read quickly. Considering that most of them were highly educated and young people, 81% had a university degree, and 95% were under 35 years old, these statistical findings showed that this group of customers understood what is written in the policy and could read it quickly. 49% of the participants knew for what purpose their data would be used, if the website would share the information with third parties, and if they would have control over their data. Consdidering

these results, it can be assumed that nearly half of customers do not know what happens with their data after disclosing them. Moreover, based on what the respondents read on the privacy policy, 51% of them had a positive thought about the website, like feeling secure sharing their personal information, protected, and close to the website. Based on the results, privacy policies that are short and use everyday language are perceived as understandable and easy to read. Even though many pieces of information were missing, customers felt secure and close to the website.

Furthermore, eight hypotheses were developed based on the factors analyzed in this master thesis to answer the second research question. The hypotheses analyzed the influence of trust, level of sensitivity, comprehension, perceived control, and benefits on information disclosure; the influence of trust and perceived control on privacy concerns; and the influence of trust on website satisfaction. The linear regression analyses´ findings reported a significant p-value less than 0.05, supporting the examined regression models. Based on the results, it can be assumed that a higher level of trust, perceived control, and benefits lead to higher information disclosure. On the other hand, a higher level of comprehension and sensitivity of information required lead to lower disclosure of personal data. In addition, a higher level of trust and perceived control lead to lower privacy concerns. Lastly, a higher level of trust leads to the reuse of the website and recommendations of it to others.

5.1 Implications for relevant stakeholders

This master thesis analyzes a big problem that customers who use online services have. Companies need to look at customers' attitudes toward privacy policies, information required, and customer surveillance to make the right decisions (Plangger and Matteo, 2020). For customers is vital to know how their data are gathered, stored, and used as well as giving them control over their data, benefits for sharing the personal information and assuring about the safety of their data. This research provides an understanding of customers' behavior that is also important for the companies to improve their business strategies to satisfy customers´ needs and wants.

Findings from the data collected showed that perceived control is the most vital construct for customers. According to Brandimarte et al. (2012), giving customers greater control

over their personal information will increase the data disclosed. Since information disclosure is central to online services, companies have benefits by providing customers with control over their data. Another crucial construct for customers is the perceived benefits. Here can be included monetary incentives such as discounts and non-monetary incentives such as personalized products. Furthermore, trust is a factor that can be built by the transparency the company is toward the customer. If the customer has the trust that the company cares about him and will inform him of everything, he will disclose the personal data and will not have concerns about privacy. Therefore, providing the customers with control, benefits, and trust will be beneficial for both parties as customers will disclose more information that will help companies improve their marketing strategies and offer the customers what they want.

5.2 Limitations

The chosen research method gives a valuable contribution regarding the customers´ perception of the privacy policies. Nevertheless, some limitations may be considered in this study.

As mentioned above, this research employed an online survey where only one privacy policy was shown, and different factors were measured. The privacy policies differ from each other, from the length, the complexity of the language used, the information provided, the way it is structured, etc. The privacy policy was taken from "The Economist," a known and trustworthy website, and the privacy policy used everyday language and was short and easy to understand. Therefore the respondents may have made less accurate assessments because of the given policy, so the customers´ perception may not be representative of different privacy policies.

Moreover, as mentioned above, the respondents were acquired by posting the survey on different social media platforms and groups and sharing it with friends and relatives. As the researcher decided the selection of respondents, the answers may be biased.

In addition, most of the participants on the online survey were below 30 years and from Albania and Austria. This determines another limitation as privacy concerns and how customers perceive privacy policies vary from cultural values (Krafft, Arden, Verhoef, 2017). Moreover, the older generation faces more difficulties understanding the privacy

policies and is less likely to share their data (Goldfarb and Tucker, 2012). Therefore the study is not representative of Europe and for the whole population as the results may not be accurate for another country and different age groups.

5.3 Future research

Section 5.2 represented the limitations of the study, which serve as a springboard for future study on the topic of privacy concerns and privacy perception.

Firstly, this master thesis uses a privacy policy from a known and trustworthy website that is short and understandable. For this reason, the answers are based on the perception of one policy. The suggestion for future research would be to use different privacy policies that include different languages (technical and everyday language), different lengths (short and long), and different visibility (show the policy on the bottom or the top of the website).

Secondly, the population of this research was young adults, and it was based in two countries. The suggestion would be to focus on an age group and in one country. It would result in more representative findings that would better explain the hypothesis raised.

Furthermore, the suggestion would be to use a different method to gather the data. In such cases would be better to use the experiment or interviews to explain better the customers´ perception regarding different privacy policies and understand the customers´ behavior.

Finally, in this master thesis, the researcher analyzed privacy concerns and customers´perception of privacy policies in normal circumstances. Considering the Covid-19 situation where everything was done online, the privacy of customers was affected. Future research could study customers' privacy in particular circumstances, such as the Covid-19 situation.

6 BIBLIOGRAPHY

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of retailing*, *91*(1), 34-49.

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, *58*, 368-379.

Allen M. (2019). `Technological Influence on Society.´
Available: https://www.bctv.org/2019/11/07/technological-influence-on-society/

Bawack, R. E., Wamba, S. F., & Carillo, K. D. A. (2021). Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, *58*, 102309.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in marketing*, *37*(3), 466-480.

Bradley B. (2017), 'Social Contract Theory.'
Available:https://smallbusiness.chron.com/social-contract-theories-business-59955.html

Brandimarte, L., & Acquisti, A. (2012). The economics of privacy. *The Oxford handbook of the digital economy*, *20*.

Brey, E. T., So, S. I. A., Kim, D. Y., & Morrison, A. M. (2007). Web-based permission marketing: segmentation for the lodging industry. *Tourism Management*, *28*(6), 1408-1416.

Britz, J. J. (1996). Technology as a threat to privacy: ethical challenges to the information profession. *Microcomputers for Information Management*, *13*(3-4), 175-193.

Brodie, R. J., Hollebeek, L. D., Jurić, B., & Ilić, A. (2011). Customer engagement: Conceptual domain, fundamental propositions, and implications for research. *Journal of service research*, *14*(3), 252-271.

Brown, A. (2020). `Digital ethics and privacy: Doing the right thing with data.´

Available:https://rgp.com/human-insight/digital-ethics-privacy-doing-the-right-thing-with-data/

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24-31.

Christensson, P. (2010, May 6). *W3C Definition*.
Available: https://techterms.com

Data Privacy Manager (2021). `Why are companies investing in privacy and GDPR compliance?
Available:https://dataprivacymanager.net/why-do-companies-invest-in-gdpr-compliance-what-are-benefits-of-gdpr-compliance/

Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social Contracts and marketing ethics. *Journal of Marketing*, *63*(3), 14-32.

Epstein L. `A closer look at two survey design styles: within-subjects and between-subjects.`
Available: https://www.surveymonkey.com/curiosity/within-groups-vs-between-groups/

Formplus blog. (2021). `Descriptive Research Design: Types, Examples, and Methods.´
Available: https://www.formpl.us/blog/descriptive-research

Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China. *Data and Information Management*, *5*(1), 195-207.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806.

Funk C., Kennedy B. & Sciupac E. (2016), ` Public sees science and technology as net positives for society.´Pew Research Center.
Available:https://www.pewresearch.org/science/2016/07/26/public-sees-science-and-technology-as-net-positives-for-society/

Gaille, L. (2017), `16 Advantages and Disadvantages of Experimental Research.`

Available:https://vittana.org/16-advantages-and-disadvantages-of-experimental-research

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review*, *102*(3), 349-53.

Hoffman, D. L., & Novak, T. P. (2018). Consumer and object experience in the internet of things: An assemblage theory approach. *Journal of Consumer Research*, *44*(6), 1178-1204.

Howell B. `Online psychology experiments: everything you need to know.`
Available: https://www.psychstudio.com/articles/online-experiments/

Iyilade, J., & Vassileva, J. (2014, May). P2u: A privacy policy specification language for secondary data sharing and usage. In *2014 IEEE Security and Privacy Workshops* (pp. 18-22). IEEE.

Im, H., & Ha, Y. (2013). Enablers and inhibitors of permission-based marketing: A case of mobile coupons. *Journal of Retailing and Consumer Services*, *20*(5), 495-503.

Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, *93*(1), 7-28.

Ivaturi, K., & Bhagwatwar, A. (2020). Mapping sentiments to themes of customer reactions on social media during a security hack: a justice theory perspective. *Information & Management*, *57*(4), 103-218.

Jordan (2013). ´The importance of W3C Standards.´
Available: https://www.bopdesign.com/bop-blog/2013/06/the-importance-of-w3c-standards/

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions?. *Journal of interactive marketing*, *39*, 39-54.

LEE, W. W., ZANKL, W., & CHANG, H. (2016). An ethical approach to data privacy protection. *Isaca Journal*.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304.

Loubier A. (2021), `Is society moving in the right direction with technology rapidly taking over the world?´ Forbes.
Available:https://www.forbes.com/sites/andrealoubier/2021/06/01/is-society-moving-in-the-right-direction-with-technology-rapidly-taking-over-the-world/?sh=14a7ec1c7c09

Lumsden, J. (2019). `So, you want to run an online experiment.` Available: https://ocean.sagepub.com/blog/how-to-run-an-online-experiment

Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: A meta-analytic review. *Journal of Retailing*, *96*(4), 458-473.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Miller, B., `8 Main Advantages and Disadvantages of Experimental Research.`
Available: https://greengarageblog.org/8-main-advantages-and-disadvantages-of-experimental-research

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*, 120-130.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research*, *15*(1), 76-98.

MotiveMetrics Research. (2013). `Psychometrics 101: Scale Reliability and Validity.` Available: http://blog.motivemetrics.com/psychometrics-101-scale-reliability-and-validity

Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., & Bråthen, S. (2021). An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. *Journal of Business Research*, *136*, 63-75.

Piotrowicz, W., & Cuthbertson, R. (2014). Introduction to the special issue information technology in retail: Toward omnichannel retailing. *International Journal of Electronic Commerce*, *18*(4), 5-16.

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32-44.

Pollanen, T. (2014). `The advantages and challenges of web-based experiments in behavioral sciences.`
Available: http://www.web-psychometrics.com/advantages_challenges.html

Rawls, J. (1999). *A theory of justice: Revised edition*. Harvard university press.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of consumer affairs*, *39*(2), 339-362.

Ritter, S. (2020). `The ethical data dilemma: Why ethics will separate data privacy leaders from followers.´
Available: https://www.forbes.com/sites/forbestechcouncil/2020/03/31/the-ethical-data-dilemma-why-ethics-will-separate-data-privacy-leaders-from-followers/?sh=44c4b23914c6

Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214-233.

Ruddell, B. L., Cheng, D., Fournier, E. D., Pincetl, S., Potter, C., & Rushforth, R. (2020). Guidance on the usability-privacy tradeoff for utility customer data aggregation. *Utilities Policy*, *67*, 101106.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, *34*(3), 593-603.

Stewart, D. W. (2017). A comment on privacy. *Journal of the academy of marketing science*, *45*(2), 156-159.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information systems research*, *13*(1), 36-49.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability*, *11*(12), 3311.

Trochim, W. (2001). `Nonprobability sampling`
Available: https://conjointly.com/kb/nonprobability-sampling/

Vail, M. W., Earp, J. B., & Antón, A. I. (2008). An empirical study of consumer perceptions and comprehension of website privacy policies. *IEEE Transactions on Engineering Management*, *55*(3), 442-454.

VOXCO. `Quantitative research: definition, method, and examples.`
Available: https://www.voxco.com/blog/quantitative-research/

VOXCO. (2021). ` Descriptive Research Design.´
Available: https://www.voxco.com/blog/descriptive-research-design/

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management*, *36*(4), 531-542.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, *28*(3), 889-897.

W3C. `W3C privacy activity.`
Available: https://www.w3.org/Privacy/

W3C. `P3P 1.0: A new standard in online privacy.`
Available: https://www.w3.org/P3P/brochure.html

Xu, H., Teo, H. H., & Tan, B. (2005). Predicting the adoption of location-based services: the role of trust and perceived privacy risk.

APPENDICES

Appendix 1: Online Survey

soSci
oFb - der onlineFragebogen

0% completed

Dear participant,

thank you for participating in this survey. We are investigating how customers perceive different privacy policies.

In the following, you will see a privacy policy. Please have a look, and in the following, you will answer some questions related to the policy.

Please note that your answers should be according to your personal judgment. There are no right or wrong answers. Your participation will make a significant contribution to this study at Modul University Vienna. This survey takes about 5-7 minutes.

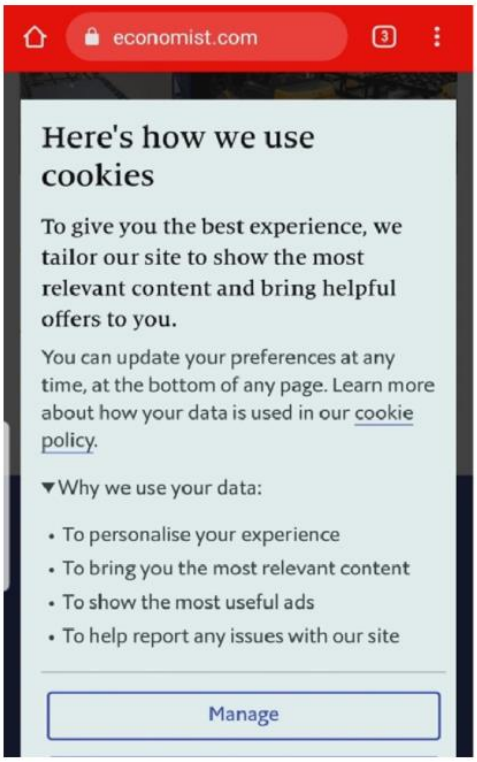
Participation in this survey is voluntary, and you can withdraw from the study at any time without any penalty or consequences. By clicking on the next button, you agree to participate in the research study and grant permission for the data generated from this survey to be used in the researchers´ publications on this topic.

Thank you for your input and participation.

Next

You decided to read an article on a website, but you need to accept the privacy policies to read the article.

Please read the privacy policy and then answer the following questions. Please click on "Next page" after reading the policy.



1. Please think about the privacy policy you read before and give a rating from 1-strongly disagree to 7-strongly agree to the following statements:

	Strongly disagree						Strongly agree
I read the entire privacy policy of the website.	○	○	○	○	○	○	○
I feel confident in my understanding of what I read in the privacy policy.	○	○	○	○	○	○	○
This privacy policy was too hard to understand.	○	○	○	○	○	○	○
This privacy policy can be read quickly.	○	○	○	○	○	○	○
I have the information for what purpose my data will be used.	○	○	○	○	○	○	○
I have the information if my data will be shared with third parties.	○	○	○	○	○	○	○
I have the right to opt-out my personal information.	○	○	○	○	○	○	○
I have control over my data.	○	○	○	○	○	○	○

	Strongly disagree						Strongly agree
Through this privacy policy, I think the website cares about my concerns.	○	○	○	○	○	○	○
The website keeps customers´ interest in mind.	○	○	○	○	○	○	○
Through this privacy policy, I feel close to the website.	○	○	○	○	○	○	○
I feel secure sharing my personal information with this website.	○	○	○	○	○	○	○
I feel that privacy practices are explained thoroughly in the privacy I read.	○	○	○	○	○	○	○
I feel that this website protect my personal information more than other websites.	○	○	○	○	○	○	○

	Strongly disagree						Strongly agree
The company is making an effort to keep my personal information out of the hands of unauthorized individuals.	○	○	○	○	○	○	○
The company will not release my personal information about me without my permission.	○	○	○	○	○	○	○
The company will inform me if the data are shared with third parties.	○	○	○	○	○	○	○
The company will use my personal information as stated in the privacy policy.	○	○	○	○	○	○	○
The company will give me control over my data.	○	○	○	○	○	○	○
The company will protect my information from loss, misuse, or alteration.	○	○	○	○	○	○	○

Next

2. Based on this privacy policy:

	Strongly disagree						Strongly agree
I would visit the website again.	○	○	○	○	○	○	○
I am going to visit the website in the near future.	○	○	○	○	○	○	○
I am not going to visit the website again because I don't feel safe.	○	○	○	○	○	○	○
I would recommend this website to others.	○	○	○	○	○	○	○

3. On a general level, please indicate to what extent you agree to the following statements:

	Strongly disagree						Strongly agree
Usually, I read the privacy policies when visiting websites.	○	○	○	○	○	○	○
Usually, I understand the privacy policies.	○	○	○	○	○	○	○
Usually, I am bothered when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared.	○	○	○	○	○	○	○
Usually bothered when I do not have control over the personal information that I provide on the website.	○	○	○	○	○	○	○
Usually, I am concerned when personal information control is lost or unwillingly reduced as a result of a marketing transaction.	○	○	○	○	○	○	○

	Strongly disagree						Strongly agree
I am willing to provide personal information for personalized services.	○	○	○	○	○	○	○
I am willing to provide personal information for financial incentives.	○	○	○	○	○	○	○
I am not willing to provide personal information regardless of the benefits.	○	○	○	○	○	○	○
I am willing to disclose personal information that is higher in sensitivity.	○	○	○	○	○	○	○
I am willing to disclose personal information that is lower in sensitivity.	○	○	○	○	○	○	○

Next

4. I will disclose my personal information if...

	Strongly disagree						Strongly agree
the website can provide me with more relevant promotional information tailored to my preferences or personal interests.	○	○	○	○	○	○	○
the website can provide me with the type of deals/ads that I might like.	○	○	○	○	○	○	○
the website reduces my searching time to access the personalized services, products, or information that I need.	○	○	○	○	○	○	○
the website can provide me with the convenience to instantly access the promotional information that I need.	○	○	○	○	○	○	○
I feel that using the website is beneficial.	○	○	○	○	○	○	○

5. How likely is it that you will disclose the following information at this site?

	Strongly disagree						Strongly agree
Name	○	○	○	○	○	○	○
E-mail address	○	○	○	○	○	○	○
Date of birth	○	○	○	○	○	○	○
Family information (e.g., children's names/ages, marital status)	○	○	○	○	○	○	○
Credit card/banking/stock portfolio information	○	○	○	○	○	○	○
Medical information	○	○	○	○	○	○	○

6. I am concerned...

	Strongly disagree						Strongly agree
about my privacy in general.	○	○	○	○	○	○	○
about not having control over my personal information.	○	○	○	○	○	○	○
that my information could be used in ways, I could not foresee.	○	○	○	○	○	○	○
that the company will share my personal information with other parties.	○	○	○	○	○	○	○
about the (sensitive) information required.	○	○	○	○	○	○	○

Next

Age

7. Highest completed education

[Please choose]

8. Gender

[Please choose]