Vilnius University

FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

SHREY BHATIA

FACTORS THAT INFLUENCE UNWILLINGNESS TO SHARE PERSONAL DATA IN ONLINE COMMERCE

Master Thesis

Allowed to defend_____

Master Student_____

Academic Supervisor
MINDAUGAS DEGUTIS

Work submission date _____

Registration Nr. _____

2020

Table of Contents

List of Tables

List of Figures

INTRODUCTION

Personal data protection became a global trend and a subject of introducing new law regulations in the EU in May 2018. Consumers are becoming increasingly aware of the threats hidden behind cookies, terms and conditions, loyalty cards, subscriptions, etc. Everyone wants to protect their privacy. What privacy actually means is not that easy to define as it may seem at first glance. (Lin & Loui, 1998) have described privacy as a few theoretical aspects:

- Privacy is non-intrusion - meaning a right to "be let alone" (Warren & Brandeis, 1890).
- Privacy as a right to control one's information- meaning that if we were able to determine how much and to whom we release the information, we could prevent privacy violations
- Privacy as undocumented personal knowledge- meaning the facts that people wish not to reveal about themselves or feel sensitive about should remain never documented or published (Parent, 1983).
- Privacy as restricted access to personal information- seems the most complex definition, meaning privacy, anonymity, and solitude (Gavison, 1980).
- (Posner, 1977) simply puts privacy as withholding or concealment of information.

With such a variety of definitions and possible approaches to the subject, it is equally challenging to protect privacy as well as provide adequate regulations by law. The question arises, can we even remain private in the modern online world? The rapid growth of technology and the shifting of business on the internet boost the interest of customers in privacy as companies now have new ways to collect and record the customers' data. Customers can now control their privacy and their information usage in a better way (Beales III & Muris, 2008).

Unfortunately, most people are not even aware of how much of their privacy is being shared every day. Customers' information is shared through their daily life activities, such as during a hospital visit, through smartphone applications, online browsing history, and online social networks (Schudy & Utikal, 2017). For that, if we are unaware, we can't really control what we share, and where the information goes to, how it is being processed. Galkin (1996) states:

“Much of the information that people would like to keep secret is already lawfully in possession of some company or government entity.” People basically every day agree to terms and conditions or cookies without being bothered to read them prior to accepting (Sipior et al., 2011).

General Data Protection Act (2018) was introduced to bring more comfort for the consumers by putting more responsibility on every commercial entity collecting, storing, and processing the personal data of its customers/users. Its main task is to prevent unauthorized data exchange and share. Despite all the efforts from the legal perspective and growing awareness among consumers being concerned about data misuse, sharing of personal data on social network sites and on online business websites is not stopped. According to many empirical and theoretical types of research, customers have not enough information and abilities to make decisions about privacy-sensitive measures. Customers often exchange and compromise their privacy for short term benefits (Acquisti & Grossklags, 2005).

This phenomenon leads to the privacy paradox described by (S.B. Barnes, 2006) as well as (Norberg et al., 2007). Privacy paradox surveys revealed that citizens prioritize privacy concerns in the digital era. But at the same time, they exchange their personal information for little rewards (Kokolakis, 2017). For example, in 2012 (Beresford et al., 2012) have conducted an experiment ” unwillingness to pay for privacy” where customers were given an option to buy a DVD in two identical online shops- the only difference was that one of the shops required more subtle personal data but offered DVD cheaper by 1 euro. In this case, nearly all the buyers chose the store at a lower price. While in the second treatment, results surprised the researchers. Participants equally bought from both shops when the price was identical. Concluding- the general statement about consumer privacy concerns are uncorrelated with their choices and behaviors.

Moreover, researchers (Earp & Baumer, 2003; Pastore, 1999; White, 2004) indicate the consumers willingly perceive their data as a currency that can be traded to obtain “free” information, personalized content, prizes, loyalty program memberships, discounts, or some other form of “fair” exchange and that outweighs the “cost” of disclosing personal information such as undesirable e-mails, phone calls or other unsolicited marketing activity (Jai and King, 2005).

Considering excessive literature (Benndorf & Normann, 2018; Jai & King, 2016; Schudy & Utikal, 2017; Ziefle et al., 2016) showing that the perceived benefits are stimulating the

willingness to share/sell personal data, we know relatively little about other factors that possibly encourage consumers to share. Also, communication privacy management theory is used to explain an individual's unwillingness to share personal data. The basic concept behind communication privacy management theory is that how people communicate their personal information. CPM theory deals the privacy management in the context of communicative and social behavior aspects of individuals. The understanding of CMP theory is comprehensive that provides an insight into individual interaction with others. Hence, we can say that communication privacy management theory deals with interpersonal interactions (Baxter & Braithwaite, 2008; Petronio, 2002). Although communication privacy management theory deals with the interactional process, it is not confined to only two people interaction; instead, it presents the part of other people in privacy management. We can say that CPM is communicative in nature. CPM theory takes into account three aspects of private information management, i.e., creating shared privacy boundaries, coordinating privacy boundaries and also this theory cope with privacy turbulence's consequences (Baxter & Braithwaite, 2008).

CPM theory explains privacy regulations as a dialectical process and states that both social and autonomous needs are necessary for an individual. The way people handle their personal data and the choices they make to share their personal information is not at all illogical or paradoxical, as explained by some news media that privacy concerns are paradoxical (Petronio, 2015). More privacy regulations aspects under CPM theory stated that private information could be explained to those information pieces that carry potential vulnerabilities. Further, people believe that they have control over their private information even after they share this information with others and that they have the right to control the information flow. However, people's expectations and privacy management functions do not work in line with each other (Petronio, 2015).

Research problem

The research problem for this study is that what are the factors that influence the customer's willingness to share personal data and lead them to unwillingness?

Research aim

Following the research problem, this study aims to explore the factor which leads the customers to unwillingness about personal data sharing during online transactions,

specifically during online shopping. These factors are explored in the context of the customer's perceived risks, privacy concerns, perceived ownership, and anxiety.

Research objectives

Research Objectives and research question for the present study are hereunder;

- To provide a comprehensive overview of the literature about customers' privacy rights and privacy protection laws and to present an overview of the factors influencing the unwillingness of customers to share their personal data on online business websites.
- To identify the types of factors, i.e., perceived risks, perceived ownership, anxiety, and privacy concerns that hinder the customers from information disclosure.
- To present an overview of the literature on perceived risks and privacy concerns of the customers regarding personal data sharing
- To describe the drivers and causes of businesses website data collection
- To formulate research hypotheses and to build theoretical framework
- To collect primary data with the help of questionnaire for empirical analysis
- To test collected data for hypotheses acceptance or rejection
- To present final conclusion and recommendations for businesses and future researchers

Structure of paper

Initially, a short brief of the study background, research problem, aims, and objectives are discussed. Chapter 1 discusses the theoretical background of this study in light of existing literature. In chapter 2, in light of research objectives and literature overview, hypotheses are developed for this study. The sampling technique is sample size detail is also discussed in chapter 3. A detailed analysis and interpretation analysis is presented in chapter 3. Lastly, a short conclusion is written by the author of this paper.

1. THEORETICAL ANALYSIS OF PERSONAL DATA SHARING

1.1. What is data and personal data

Companies run several programs and surveys to collect the data. Different departments such as marketing, sales, customer support need customers' data to improve their services and support. Companies save the customer's data from getting an idea about their target customers, and the sales team uses this data to identify their target market (Sehat & Paves Flores, 2012). We live in an era of big data, technological advancements, and excessive use of the internet to change the way of decisions making of both individuals and organizations. Old data handling applications are not enough to handle and organize such big data of consumers. Much new software is emerged to manage and analyze such big data, i.e., ICTs. This software also allows for better communication and information flow (Chen et al., 2012). Systematic collection and proper processing of consumers' data lead to the understanding of consumer's attitudes and preferences toward a specific organization's products and services and hence paved the way to sustainable competitive advantage (Erevelles et al., 2016). Data is defined as "unrecognized and raw facts and figures" that are required to be organized as per the need of any working organization. These facts and figures can include raw numbers, statements, and characters. Humans and machines can process and organize this data to be used for further operations. Different organizations and businesses get the customers' data when they interact or visit their websites. In this technological era, customer data is also retrieved from mobile applications, social media, different market campaigns, and surveys. Personal data is a type of customers' data.

According to the EU's GDPR, any information which can be related to a natural individual is regarded as personal data. Personal data includes names, personal residential addresses, contact details, IP addresses, the location of an individual, and e-mail addresses (Irwin, 2020). The information commissioner office of the UK states that this is not only our name but also the minuscule information, i.e., even the log-in timing through which we are

recognizable for others is known as personal data (*Personal Data Sharing—Are We Really in Control?*, 2019).

1.2. Types of personal data

Personal data can be categorized into two kinds; personally identifiable information and non-personally identifiable information.

In personally identifiable information, two types of information are included. One is known as "linked information," and the other is "linkable information." Linked information does not need any supplementary information to recognize a person, such as his name and e-mail address. Linkable information, such as gender or location, required another piece of information to determine a person's identity.

In non-personally identifiable information such as cookies and IP addresses, we can't recognize a person and his real identity (MarTech Advisor, 2019).

1.3. What is privacy

Privacy concerns and their severity alter from individual to individual, which makes it a complicated concept (Larose & Rifon, 2007). Online consumers are more reluctant to reveal their personal details due to privacy concerns (Li et al., 2011). Privacy is a vital tool to protect the individual's opinions from illegal leaks. Government access to the personal data of consumers might restrict their honest opinions (Newell, 2014). According to (Westin, 1967), a person's ability and understanding of information dissemination, i.e., when, where, how, and why it is known as privacy. Irrespective of the easiness of electronic transactions, consumers fear the information leak and loss of control on their personal details in online transactions, such as when consumers visit some online shopping stores or banking sites (Metzger, 2007).

Customers' data is a must thing for business growth, and companies always strive to reach out to the maximum customers. However, with the extensive use of customers' data privacy issue remains the foremost factor to be solved by the organizations. The organizations use this data as a source of value-driven activity, i.e., economic value (Janssen & van den Hoven, 2015). When consumers interact with the websites of companies, it captures activities log through these companies to assess the interests of consumers. Consumers are now more cautious about the privacy issues and use of their data (Janssen & Kuk, 2016). Online information leaks and activities log highlights the information risk. Now companies are

required to be more vigilant in using customers' data and should have more tools to control data leak risks. Ignoring the privacy issue may impair the companies' reputation and economic value (Culnan, 1993; Drinkwater, 2016).

Marketing scholars and practitioners are now more interested in exploring the online privacy of customers regarding their personal data due to the growing importance of relationship and data-driven marketing (Castaldo & Grosso, 2014; Dinev & Hart, 2005). According to (Xu et al., 2008), privacy matters can be explored at three different levels named; individual, organizational, and social levels. A number of researchers focused on these three levels, i.e., (Ginosar & Ariel, 2017; Lwin et al., 2007; Smith et al., 2011).

Individual-level privacy domain or customer level domain has been the foremost focus of the researchers. In this domain, researchers explore the customers' privacy concerns, perceived risk of customers regarding online privacy risks, attitudes, and behaviors such as privacy protection and information disclosure behavior (Smith et al., 2011).

Public policies and regulations and ethical and legal perspectives of online privacy are researched under the head of the public domain. Further, the organizational level domain of privacy matters includes "the corporate responsibilities concerning online privacy," i.e., information management practices at the industry or organizational level (Lwin et al., 2007). According to (Smith et al., 2011), individual-level privacy matters are more researched in the marketing discipline. In line with this trend, this research also focuses on the individual privacy domain, i.e., customer level.

1.3.1. Online Privacy

The concept of boundaries and limitations is not applicable in the internet world. Privacy concern is now emerging as a plague in electronic world transactions. In online transactions, consumers perceive the risk of misuse of their personal information (Milne & Culnan, 2004). Online businesses are in need of acquiring consumer's trust for their success (McKnight & Chervany, 2001). Uncertainty and sensitive information leak risk are prevalent in online businesses (Nissenbaum, 2001). By sharing the personal information on the internet, consumers feel a loss of control on their personal data which restrict them from a further online transaction. However, human nature wants interaction with others; therefore, they can't control themselves from sharing personal data (Dinev & Hart, 2006).

As time passed and with the advancement of technology, individuals are more concerned about information privacy in the internet world (Joinson et al., 2012; Miltgen & Smith, 2015). An extensive literature is available about online privacy and the fast dispersion of the internet around the world (Smith et al., 2011). Online privacy issue draws the attention of many researchers to explore the privacy issue related to personal data management not only in the field of law and public policy but also in economics, social sciences, computing, and information management system, marketing, and consumer research (Acquisti et al., 2013; Bansal et al., 2016a; Chellappa & Sin, 2005; H. Akhter, 2014; Heirman et al., 2013; Malhotra et al., 2004; Miltgen & Smith, 2015; Schoenbachler & Gordon, 2002; Walrave & Heirman, 2012).

1.4. Usage of personal data in business

Technological advancement makes it possible for businesses to recognize you through your tiniest information. Many online transaction websites can access consumer's log-in history and browsing history. Companies collect the consumers' data and use it as their power. Data is knowledge, and it is regarded as power; companies utilize this power, which ultimately provides them with economic benefit. For example, Amazon grows its business through this technique by selling products at discounts and, at the same time, collects consumer data to acquire knowledge about its target market. The use of consumer's personal data works as a lifeline for businesses. According to the results of the Accenture survey, which was conducted on 600 global companies, around 79% of participants reveal that companies collect data of visitors from their online websites. Businesses argue that this data collection is beneficial for their growth and also for customers, i.e., they can get the best innovative products and services (Cooper & LaSalle, 2015).

Businesses are blind in their target market without customer's data. Companies use consumers' personal data for their future marketing strategies. Product and service improvements are mainly based on the analysis of customer's personal data. As business websites record the log-in detail of customers, later, they sent an e-mail to their frequent and loyal customers to know their preferences (Lawrence, 2018).

Other causes to collect personal data are also stated by (Minkara, 2014) such as businesses use the personal data of consumers to set their marketing direction according to customer preferences, for better communication with customers, and to provide services in convenient ways. Businesses segment their target customers' market depending on the data and can offer

the right product or service at the right time. Last but not least, personal data use for marketing purposes also boos the revenue f businesses as it gives them the right direction (Minkara, 2014).

1.5. Legal perspective- what are the rights of customers?

An extensive overview of the literature reveals that privacy concern negatively affects the consumer's willingness to share personal data (Dinev & Hart, 2006; Malhotra et al., 2004; Stewart & Segars, 2002). Consumers might share their personal data and accurate information if they are certain about the benefits which they will acquire in exchange for their personal information (Godin, 1999). (Hinde, 1998) states a survey result in which it was observed that data protection and privacy is the priority of consumers, and consumers want assurance that their data will remain private and would not be used for illegal purposes.

To ensure the consumer's privacy protection, US congress developed the Privacy Act in 1970. This act includes the principles of Fair Information Practice (FIPPS), such as use limitation, security, transparency, data quality, and access and correction. In 1980, OECD (Organization for Economic Cooperation and Development) was developed to ensure the privacy protection of the flow of personal data. OECD principles were flexible for real-world privacy concerns, but data processors faced difficulties in their implantation. At that time, eight principles were included in OECD guidelines named; data quality, collection limitation, security safeguard, use limitation, purpose specification, individual participation, openness, and the principle of accountability (Wu et al., 2012).

Moreover, many other privacy policies and laws are developed to build customer trust and to protect their privacy rights. Almost privacy protection laws developed around five foremost factors. These five factors, i.e., notice, choice, access, security, and enforcement, are the origin of fair data protection policies and assembled around the US Federal Trade Commission (FTC) in 1998. The notice principle required that a prior notice should be given to the consumer to collect his personal details. The second principle stresses that each consumer should be given a choice to decide the use of his personal data. Access principle required from data collection websites to provide data access to the consumer to his own data. In this way, he can check his own data precision and completeness. The fourth factor stresses data integrity and security. Collector organization is required to be vigilant in providing data access to consumers, its conversion into an anonymous form, and timely deletion of data to ensure its security. Last principle enforcement is only effective when there is a systematic privacy protection mechanism to enforce this (Wu et al., 2012).

In 1962, President Kennedy introduced the concept of consumer right to safety, information, choice, and redress. Privacy, as a consumer right, causes a change in content privacy rights perception. Not only phone privacy, but also the emphasis was put on personal information privacy. In 1974, after the Privacy Act, privacy concerns emerged as the most important issue. In a survey conducted by Sentry Insurance, 61%of participants agreed that there must be regulations for privacy controls. They demand control over the type of information that an organization collects (Goodwin, 1991).

In the US, a federal law was passed to protect customers' privacy. Later after 1970, this law was amended, and the legal rights of customers were added in the context of unauthorized access and recording of personal information through websites and other electronic applications (Caudill & Murphy, 2000). EU companies have more concerned about customer's privacy rights as compared to US companies. They have policies related to customers' data collection and its usage (Harbert, 1998). Privacy regulation makes it a must for the businesses to explain the purpose of the information recording clearly, and this purpose must be explained to the concerned individuals. After collecting personal information, companies are bound to use that information only for the permitted purpose. By adopting these privacy rights regulations, businesses can collect data along with the privacy protection of customers (Caudill & Murphy, 2000).

Further, transparency should be maintained during the data collection of customers. Customers must have easy access to the privacy policy of a specific business's website. A privacy policy should be written in understandable language. It should contain the detail of the type of information which a website is going to record. Customers have the right to know the purpose of information collection (Flaiz, 2017).

1.6. Factors influencing unwillingness to share personal data

Nowadays, consumers are more concerned about their privacy and are vigilant about what type of information companies are collecting about them. Data privacy and security have become a growing issue for companies who collect the personal data of visitors from their websites (Flaiz, 2017). Most of the time, consumers are reluctant to provide their personal information as they have a concern about data usage (Swant, 2019).

By sharing personal information, consumers feel a loss of control of their personal information. The age of customers also matters in sharing information with companies. Young customers are more concerned about their privacy as compared to old age customers

and take extra measures for privacy protection on their electronic devices. It is also stated that consumers are more willing to share data if they are assured about some value in return (Pingitore et al., 2017). Consumers want fast delivery and at spot solutions to their problems. While providing their personal details, customers expect that companies will provide long-lasting solutions along with financial benefits, i.e., discounts (Carufel, 2017). Data sharing drives also varied from industry to industry, i.e., financial industry customers are more willing to share personal data. Personalized information that is delivered to target customers is the crucial psychological motivation factor for personal data sharing as customers feel more relevant to the organization. Personalized information about a product gives a feeling of control, and hence customers get motivated to share personal data (J. Phelps et al., 2000; Wolff, 2017).

This study aims to cover the research gap by examining the factor influencing the customer's 'unwillingness' to share personal data. Although customers can share their personal data in exchange for some expectation and benefits, there are still some factors which hinder the customers from personal data sharing. A literature overview of perceived privacy risk and privacy concerns is given hereunder.

1.6.1. Perceived Privacy Risk

Consumer behavior toward online privacy and perceived risk are closely related (Mitchell, 1999). Incredible technological advancements provoke the need for a study on the perceived privacy risk of consumers' behavior (Milne & Culnan, 2004; J. E. Phelps et al., 2001; Schoenbachler & Gordon, 2002). According to FTC 1998, 'perceived privacy risk' is related to the perception of customers when businesses try to collect and use the customer's personal data for their own benefits (Myerscough et al., 2006). In the internet world, online perceived privacy risk can be explained through a range of privacy concerns such as illegal and unauthorized use of customer's personal data, recording of customers' online activities, and unwanted contact of businesses with the customers through e-mails (Myerscough et al., 2006).

According to Katz and Tassone (1990), due to excessive privacy infringements by companies' websites, consumers form their own resistance strategies to eliminate the adverse impact of privacy breaches. If consumers perceived that providing personal data would be risky and it will breach their privacy rights, in some situations, consumers refused to deliver accurate information. In some other circumstances, consumers ignore the requested information (Katz

& Tassone, 1990). Other studies by Nowak and Phelps (1992) and Sheehan and Hoy (1999) also supported the research findings (Katz & Tassone, 1990). They stated that before providing information, consumers assess their necessity; if consumers think that giving a piece of specific information is unnecessary, they would not provide that particular information despite f the fact that information is necessary for the marketing context.

A number of studies explored the determinants of risk perception related to online transactions. All studies found that trust is negatively associated with risk perception (Grazioli & Jarvenpaa, 2000; D. J. Kim et al., 2008; Y. H. Kim & Kim, 2005). Further, many studies investigated the customer's willingness to share personal data (Benndorf & Normann, 2018; Jai & King, 2016; Myerscough et al., 2006; J. Phelps et al., 2000; Schoenbachler & Gordon, 2002). Additionally, according to Walrave and Heirman (2012), teenagers are less willing to disclose their personal contact details as compared to adult individuals. Robinson (2017) explores the willingness of individuals to share personal information in the context of education, nationality, and e-commerce experiences. He also studied the perceived risk of customers during online transactions in a cross-cultural setting. Crespo et al. (2009) examine the influence of perceived risk on the online shopping behaviors' of consumers. Mieres et al. (2006) explore the association between perceived risk and store bran proneness. Faqih (2013) explores the impact of perceived risk and internet self-efficacy on online shopping behaviors in Jordan. Another study by Dunn et al. (1986) found the association between perceived risk and brand preferences of customers.

The relationship between information disclosure and privacy is explained by the communication privacy management (CPM) theory presented by (Petronio, 2002). This theory explains the reason behind the customer's willingness to share information and unwillingness to share personal information on the different relational phenomena. CPM theory stated that disclosure of data includes both risks and benefits. It is the customers who balance the need for disclosure and set their privacy boundaries. Self-expression, relationship development, and social control are some of the benefits which customers expect in return for information disclosure. Petronio (2002) states that information disclosure always comprises some degree of risk. This risk leads the customers to develop boundaries and to set their preferences about personal information sharing. Information sharing boundaries allow the customers to control with whom they are willing to share their personal details (Petronio, 2002).

1.6.2. Privacy Concerns

In most consumer-level privacy research studies, privacy concern is a dominant construct. Further, in empirical privacy research studies, privacy concern is the central variable (Smith et al., 2011). Privacy concern is also used in many research studies as antecedent, mediator, and outcome variables. Moreover, a number of privacy-related decision-making models empirically validate the importance of privacy concerns (Miltgen & Smith, 2015; Xu et al., 2008). Companies often offer personalized content to consumers, and to get these, consumers are required to provide some personal data. Although consumers have concerns over online privacy are reluctant to provide their information to those companies that disturb their privacy. However still, they do not take any preventive measures to protect their private data from companies. The reason behind this is that consumers believe that there is no use in taking preventive measures; they perceive that they will still track by these companies. However, the consumer's perception of in-feed ads is positive, as stated by (Lindblad & Sasivanij, 2017).

The internet boosts privacy concerns among customers. UD department of commerce conducted a study in 1998, and the results revealed that 79% of online customers are concerned about their online privacy (Oberndorf, 1998). According to (Caudill & Murphy, 2000), e-commerce business and customer's concern for online privacy and sharing of personal information both boost at the same pace in the internet world. Consumers are more concerned about their personal data collected by the website of different businesses, such as purchasing behavior, habits, interest, and online activities (Caudill & Murphy, 2000; Milne, 2000). Websites now can easily collect the information for their marketing purposes, and customers are more concerned about their data usage (Thomas & Maurer, 1997).

As stated earlier, consumers are reluctant to provide personal information. Dr. Alan Westin presented the Privacy segment indexes (PSI) to understand the relationship between consumers' behavior and consumers' preferences related to privacy. According to him, there are three groups in the context of privacy concerns named; privacy fundamentalists, privacy pragmatists, and uncensored privacy groups (Jai & King, 2016). Classification of privacy presented by Westin based on three statements; first, all consumers agree that they have no control over the information which they shared with the companies, and also, consumers have no idea how this information will be used by companies. Second, consumers agree that businesses handle their personal detail with great care and keep it confidential. Third,

consumers agree with this statement that their privacy is reasonably protected by the organizations (Kumaraguru & Cranor, 2005).

Several studies explore the privacy concern construct in different contexts. Gupta et al. (2010) explore the privacy concern of customers in two different cultures. They concluded that Indian customers are more willing to share their personal data due to collectivistic culture. Indian customers are more inclined to maintain their e relationship with a specific organization. In contrast, the US customers are not much willing to share their personal information due to individualistic society. A number of studies present a correlation between privacy concerns and the privacy management behavior of individuals (Utz & Krämer, 2009; Wu et al., 2012).

Nam et al. (2006) explore the association between consumer's privacy concern and their willingness to share personal data. He found that consumers with more privacy concerns are not willing to share their personal information with companies' websites. Furthermore, when websites want consumer's personal data for registration purposes and to provide further website content, consumers often provide false information to the website, and this results in sites where inaccurate personal data of consumers data is captured (Dinev & Hart, 2006; Rice et al., 2001). Phelps et al. (2000) explore personal information beliefs related to direct marketing and specific privacy concerns in the context of willingness to provide personal data. Miltgen (2009) assesses the association of privacy concerns and willing to share personal data on the internet in an experimental study conducted on French students.

1.6.3. Perceived ownership

Generally, things used by people in their daily life are possessed by people. When an individual uses a single object much time during his life, it gives him a sense of possession. People often feel a sense of possession or entitlement feelings toward their objects, such as homes, vehicles, and even small objects at home (Dittmar, 1992). It is not necessary that possession feelings are attached only toward physical objects. An individual can feel a sense of belongingness toward nonphysical objects. We can describe nonphysical objects, i.e., ideas, designs, personal concepts, and personal information of an individual. Furthermore, a sense of possession influences individuals to protect their personal information or 'objects' on the internet (Anderson & Agarwal, 2010; Feuchtl & Kamleitner, 2009; Furby, 1978; Pierce et al., 2003). Hence, when individuals interact or make transactions through online sites, they feel a sense of possession of information that they provide during transactions. The

information delivered by consumers is considered by consumers as their ‘own.’ A sense of ownership provides consumers with a positive state of mind and self-identity. According to (Van Dyne & Pierce, 2004), individuals do not want to share their personal information with third parties, and hence while sharing information, individuals feel a sturdy sense of perceived ownership over their personal data and desired to limit unwanted third party access.

A previous research study by (Sharma & Crossler, 2014) on personal information disclosure in the context of the social commerce environment is conducted. Results of (Sharma & Crossler, 2014) showed that perceived ownership has no significant association with personal information disclosure. However, a research study by (Raban & Rafaeli, 2007) on data sharing willingness and information ownership revealed that people are more inclined to share information possessed by them privately and are less prone to share organizational information.

According to (Dittmar, 1992), a sense of possession over objects and personal information provides pleasure. She further stated that possession is an instrumental function. A sense of possession empowers an individual to influence outcomes and get his desired results in a certain environment. A number of research studies stated that when we explain possession as an instrumental function, it includes efficacy and a symbolic expression of ‘self.’ Moreover, self-identity, possession, and individuality are closely related (Pierce et al., 2003).

This research is based on CPM theory to analyze the role of perceived privacy risk encountered by individuals and hinder them from sharing personal information. As per CPM theory, critical risk related to personal data sharing is the “loss of control.” Hence even after the information is disclosed by the customer, they want to retain to maintain their control. Information after disclosure becomes co-owned, and customers feel vulnerable in front of others (Petronio, 2015). Although consumers are not happy with the companies who demand their personal data and compelled them to lose control over their privacy, consumers still understand the situation where they are ready to lose their control over personal data. Consumers also do not hinder to loss of their privacy because they want to become part of modern society (Katz & Tassone, 1990).

In order to understand information control and information ownership management, CPM theory proposed privacy rules. Privacy rules under CPM theory are not rigid and have the potential to be applied as per conditions. Privacy rules are flexible to alter as per people's needs and guides them to manage their personal information according to circumstances

(Petronio, 2015). To understand how people consider their information is private, CPM theory also proposed a privacy boundary metaphor. When people are more willing to share their personal data, this implies that these boundaries are thick, whereas when people are less willing to share their personal data, this means that these boundaries are thin. Moreover, thin privacy boundaries are an indication that there is a high possibility people will disclose their personal information and grant access to others (Petronio, 2015).

Generally, people believe that they have the right to retain their personal data. In order to understand the people's right to control flow and ownership of their information, the CPM theory presents the 'privacy information control' principle. The privacy information control principle explains the 'privacy rules' of information ownership and flow control. We can say that privacy rules are guidelines for individuals to decide whether they should grant access to others or not. CPM theory proposes two criteria for privacy rules that can influence people's decision to use privacy rules to regulate their private information. These two criteria are 'core' and 'catalyst.' Core criteria work in the background, i.e., cultural aspects, to reveal and hide particular information. On the other hand, catalyst criteria guide people to react and to bring changes in their privacy rules as per situations (Petronio, 2013, 2015).

1.6.4. Anxiety

As stated earlier, consumers are concerned about their privacy due to unexpected and high risks associated with personal information sharing. Consumers are always uncertain about personal data sharing, which causes anxiety among consumers while doing transactions on the internet. Consumers who shop in traditional stores are less concerned about their privacy (S. C. Robinson, 2018). According to (Ferri et al., 2010), individuals are more vulnerable to privacy risk during online transactions due to widespread fraud and identity theft on the internet. They further added that individuals often received incorrect orders from online stores that validate their perceived risk related with personal data sharing. (Gilbert et al., 2003) described anxiety as an individual's reaction to a specific situation. However, he stated that this reaction is negative and lasts for a short time.

It is suggested in the literature that anxiety is the opposite of comfort. When we study about data disclosure in literature, the concept of comfort is widely discussed. We can't define comfort in a single discipline. Comfort levels change depending on the situation. Hence, we can say that comfort is a multi-dimensional concept that is different for different people in different contexts (Hamilton, 1989; Siefert, 2002). A number of researches are conducted on

comfort concepts in ergonomics, psychotherapy, and psychology (Branton, 1969; Parloff et al., 1954; Pineau, 1982).

A study by Robinson (2014) is conducted to assess the personal data sharing willingness in a cross-culture context. Results revealed anxiety and personal data disclosure among American's is not much significant. However, Estonian people are more concerned about personal data privacy and thus have a more substantial relationship between anxiety and private data sharing. Another research study on an individual's attitudes toward personal data sharing is conducted by Robinson (2018). The findings of Robinson's (2018) research suggest that consumers should be aware of tactics to protect their data during online transactions. Furthermore, factors such as trust, anxiety, and personality dimensions are analyzed. Results showed that anxiety and personal data sharing willingness are negatively associated. (S. C. Robinson, 2018).

1.6.5. Trust

In the literature, trust is recognized as a key element and studied widely in prior studies. Trust is a crucial element between individual relationships or associations between two organizations and even for the relationship between an organization and an individual. Despite several pieces of research, researchers are not a consensus on a single definition of trust (Ilyoo B. Hong & Cho, 2011). In prior studies, trust is studied in numerous settings, such as in labor-management negotiations, buyer-sell relations, and strategic alliances (Lee & Turban, 2001). A general definition of trust is proposed in the literature as a party's willingness to expose itself to another and making themselves vulnerable to the actions of another party. In trust, the party which exposes itself expects that the other party will do actions in favor of the trustor. Also, the first party makes itself vulnerable without taking any control over another party (Mayer et al., 1995). The same definition of trust was proposed by Morgan and Hunt (1994) in which they stated that belief about the behavior of trustee that he will do favorable actions is considered as trust. Hence, we can say that the trustor is ensured that the trustee will not harm in any way.

In an online shopping context, trust is a crucial element due to the impersonal nature of the internet and exchange relationships between buyer and seller. In an online context, there are more chances that consumers will face privacy issues. Most consumers are concerned about their privacy and security, and this plays a role of barrier to sharing their personal information with online web stores (McKnight et al., 2002). Trust is an essential element to convince

consumer s to share their personal information, such as credit card information, with online stores (Hoffman et al., 1999).

In prior studies, trust is widely studied as an important construct in an online context. A study by Hong and Cha (2013) investigate the role of trust as a mediator in relation to the purchasing intention of consumers from an online store. Hong and Cha (2013) concluded that online vendors are required to make efforts to earn the trust of consumers to increase shopping from their online stores. Another study by Bansal et al. (2016a) examines the role of trust in disclosing personal information. It is stated trust is a key factor in disclosing personal information. Bansal et al. (2016a) found three further components of trust named trustee, trustor, and trust context. Other studies on trust are conducted in the context of self-disclosure (Joinson et al., 2010; Taddei & Contena, 2013). It is proposed by Communication privacy management theory that individuals are reluctant to share their personal data and set boundaries to control their private data (Petronio, 2015); nevertheless, if they trust another party, they are ready to share private information. This reproach proposes to explore trust as a moderator among those factors which hinder consumers from personal information sharing.

2. RESEARCH METHODOLOGY OF THE STUDY

2.1. Research questions, model and research hypotheses

In line with the research objectives of the present study, this research aims to find the answers to the following questions;

- What is the influence of perceived privacy risk, privacy concern, perceived ownership of personal information, and anxiety on customer's unwillingness to share persona data?
- What is the moderating influence of trust on relationships amid perceived privacy risk, privacy concern, perceived ownership of personal information and anxiety (independent variables), and customer's unwillingness to share persona data (dependent variable)?

In line with the above literature overview and based on the communication privacy management theory following model is proposed for this research study to cover the existing research gap in the literature. This research study analyzes the influence of perceived privacy risks, privacy concerns, perceived ownership, and anxiety (independent variables) on the unwillingness of personal data sharing (dependent variable) by consumers along with the moderating role of trust.

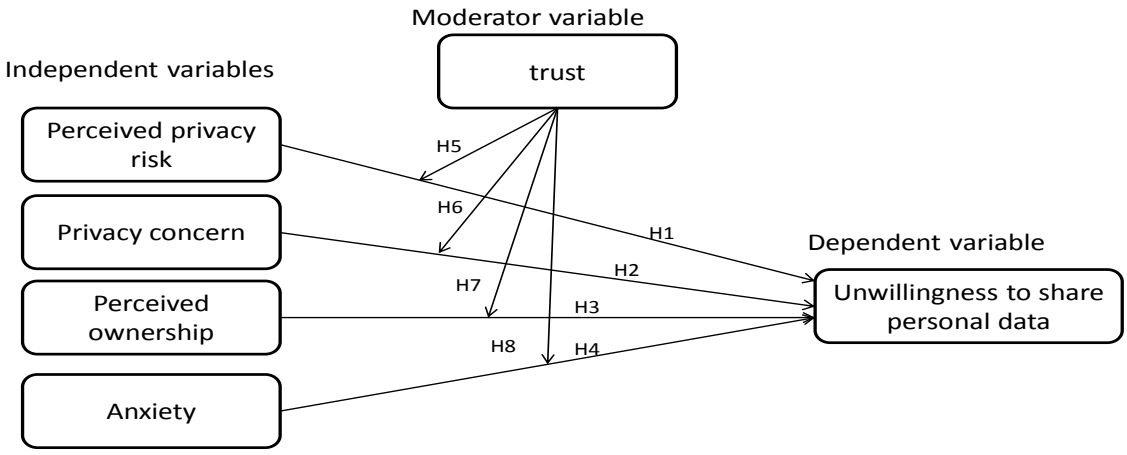


Figure 1. Research Model

Customer's behavior toward the perceived risk of online privacy is increased as more organizations start their business through online transactions (Oberndorf, 1998). Customers are not reluctant to provide demographic information. However, they are specifically unwilling to provide financial and personal information through which they are easily identifiable by third parties (J. Phelps et al., 2000). Therefore, as per the communication privacy management theory, this research thesis hypothesized that following the risk of information disclosure, consumers are reluctant to share their personal data with online vendors. Thus we proposed that;

H1: *Perceived privacy risk has a positive influence on the unwillingness to share personal data.*

As per CPM theory, choices made by the people to share personal data are based on some logic and are underpinned by dialectical tensions that eliminate the paradoxical element of privacy concern matters. We can explain the dialectical process of an individual's choice between a condition where an individual wants to communicate with others, and at the same time, he wants to protect his privacy and wants autonomy (Petronio, 2015). Based on CPM theory, we posit in this research that privacy concerns cause hesitation in individuals to share their private data.

H2: *Privacy concern has a positive influence on the unwillingness to share personal data.*

In line with the already discussed literature, this research explores the role of perceived ownership in the context of individuals' unwillingness to share data as per communication privacy management theory. A notion of private information ownership under CPM theory stated that individuals define their own parameters of private information. It is the right of the original owner to make a decision with whom they want to share their private information. CPM described the original owner as per person who shares his private information with others (Petronio, 2015). Therefore, it is hypothesized that;

H3: *Perceived ownership has a positive influence on the unwillingness to share data*.

This research applies the communication privacy management theory to investigate how anxiety influences individuals' data sharing willingness. According to Child and Westermann (2013), Child and Starcher (2016), and Petronio (2013), CPM theory can be applied to explain everyday problems, i.e., how anxiety affects personal data sharing. In today's world, every individual face anxiety (Basel, 2018), CPM theory is best to study how individuals manage their anxiety while sharing personal data. Therefore, this research thesis posits that;

H4: *Anxiety has a positive influence on the unwillingness to share data.*

Following the extensive literature which supports trust as a significant medium to share personal information and as per communication privacy management theory, this study proposes that trust moderates the association among perceived privacy risk, privacy concerns, perceived ownership of personal information, anxiety, and individuals' unwillingness to share personal data. Heirman et al. (2013) studied the perceived risk and trust factors related to the personal data disclosure behavior of young individuals on a specific website. They concluded that personal data disclosure is significantly influenced by the trust on one particular webpage, perceived level of risk, trust propensity, and familiarity. Therefore, it is hypothesized that trust may increase the chances of personal data sharing with online vendors;

H5: *The higher trust level will lower the positive association between perceived privacy risk and unwillingness to share data.*

H6: *The higher trust level will lower the positive association between privacy concerns and unwillingness to share data.*

H7: *The higher trust level will lower the positive association between perceived ownership and unwillingness to share data.*

H8: *The higher trust level will lower the positive association between anxiety and unwillingness to share data.*

2.2. Measurement scales and data analysis techniques

The research questionnaire for this research study contains two sections. In the first section, participants are required to fill in demographic details. In section two, participants are required to express their opinion on a five-point Likert scale of research variables, i.e., perceived privacy risk, privacy concerns, and unwillingness to share personal data. In order to ensure the reliability and data results validity, all scales are adopted from previous research studies.

Perceived privacy risk

A measurement scale of seven items developed by (Schlosser et al., 2006) and used in a research study by (Fortes & Rita, 2016) is also used in this research to collect data from participants. Cronbach's alpha for this scale is 0.862 (Fortes & Rita, 2016).

Privacy concerns

A scale of four items developed by (Dinev & Hart, 2006) and applied by (Fortes & Rita, 2016) with a Cronbach's alpha of 0.938 is used in this research study.

Perceived ownership

A measurement scale of 5 items previously used in a study by (Sharma & Crossler, 2014) with a Cronbach's alpha of 0.8562 is used in this research.

Anxiety

A scale of 7 items used in a previous research study by (S. C. Robinson, 2018) with a Cronbach's alpha of 0.91 is used in this research.

Unwillingness to share personal data

A measurement scale of 15 items used in a previous research study by Uilenberg (2015) with a Cronbach's alpha >0.71 is used in this research.

Trust

A four items measurement scale for trust is adopted from a prior study of Hong and Cha (2013) with Cronbach's alpha of 0.85.

A detailed research questionnaire is attached in **Appendix A.**

Data collected through an online survey research questionnaire is analyzed by (1) descriptive statistics, (2) regression analysis, (3) correlation analysis, and (4) Moderation analysis.

2.3. Research Type, Target population, Sampling, and Data collection method

Out of research types named; qualitative and quantitative research type, this research study is quantitative research. Quantitative research type is conducted due to its objectivity, reliability, and validity (Creswell, 2014).

The target population is all individuals' or objects that a researcher wants to study in his research. The researcher chooses some units of the target population that form a sample population (Creswell, 2014). The target population for a research study is carefully chosen on the basis of available budget and time (Martínez-Mesa et al., 2016). Hence, based on a limited budget and time for this research study, the researcher prefers to target college-going students in Sweden. An online link to the survey questionnaire was shared with students who filled the research questionnaire voluntarily. Although it is stated by Hong and Cha (2013) that we cannot say college-going students fully represent those individuals who shop online, still it is proved by many researchers that college-going students can substitute online shopper population (Bhatnagar et al., 2000; Featherman & Pavlou, 2003; Jarvenpaa et al., 2000; Lee & Turban, 2001; Pavlou, 2003). Following this argument, this research proposes to target college going students.

The sampling technique for this research study is convenience sampling. The sample size for this research study is 195 college-going students. Sample size calculation is as follows;

Formula for sample size is $\mathbf{=Z(c/100)^2r(100-r),}$ by putting 7% margin of error, 95% confidence level, N=20,000 and r=50%, sample size for this study is 195.

For a research study, data can be collected through primary sources and secondary sources. Data collected through primary sources are specific for particular research and is collected by the researcher itself. While secondary data is available in the form of already published newspapers, books, journals, and articles (Saunders & Lewis, 2012), in this research study,

data is collected through primary sources with the help of an online survey research questionnaire.

3. DATA ANALYSIS AND RESULTS

3.1. Demographics

According to the survey conducted, the percentage of male participants that participated in the survey was 51.8%, which means the remaining 48.2% of participants were female. This survey showed that most of the participants who participated belong from the age group of 20-25 years old, with 47% of participants belonging to this age group. There were 31.8% of participants were between 26-30 years old. The least number of participants were from the age group of 31-35 years, and the percentage of the participants being 9.7%. 11.3% of the participants had more than 35 years of age. We can also get the percentage of the participants according to their education. The percentage of the participants with an Undergraduate degree is 5.2%. Only 5.2% of participants had some kind of undergraduate degree. The highest number of the participants had a Graduate level of education, with it being 43.8% as compared to the rest of the education level of the participants. 38.7% of participants had Some kind of Master's level degree, and 9.8% of participants with M.Phil. Level education. Very few numbers of people with Ph.D. level education participated in the survey. There were only 2.6% of the participants with Ph.D., which puts it on the least number of participants with this Education level. There were 30.8% of participants who had work experience of less than one year, while most of the participants had 1 to 5 years of experience. 44.1% of participants have 1 to 5 years of experience. 19.5% of participants had experience of 5 to 10 years, and only 5.6% of participants have work experience of more than 10 years. The frequency percentages are given in table 1.

Table 1. Demographic Frequencies

Variables	**Percentage**
Gender	
Male	51.8%
Female	48.2%
Age	
20-25 years	47.2%
26-30 years	31.8%
30-35 years	9.7%
Above 35 years	11.3%

Education	
Undergraduate	5.2%
Graduate	43.8%
Master Degree	38.7%
M.Phil.	9.8%
PhD	2.6%
Experience	
Less than 1 years	30.8%
1 to 5 years	44.1%
5 to 10 years	19.5%
More than 10 years	5.6%

Table 2 shows the variables with respect to the Gender of the participants. This table shows that most of the female participants were from the age group of 20-25 years old. Almost 55% of the female participants belong to this age group. 14% of the female participants belong from the age group 26-30 years. 11% of the female participants have age between 31 years and 35 years. 14% of the female participants had age above 35 years. On the other hand, most of the male participants had an age between 26 years and 30 years, with the percentage being 48. 37% of male participants had ages from 20 to 25 years. Only 8% of the participants' age were between 31 years and 35 years, and the rest of the 8% of participants had aged more than 35 years old. 8% of the male participants had an undergraduate degree, and only 2% of the female participants had an undergraduate degree. Whereas 45% of male participants and 40% of the female participants had Graduate degrees. 37% male and 38% of the female participants have Master degree. Whereas for M.Phil. Level education, only 8% of male and 11% of female participants had M.Phil. level education. Only 3% of female participants and 2% of male participants have Ph.D. level education.

Table 2. Demographics

Variables	**Percentage**	
	Male	**Female**
Age		
20-25 years	37%	55%
26-30 years	48%	14%
30-35 years	8%	11%
Above 35 years	8%	14%
Education		
Undergraduate	8%	2%
Graduate	45%	40%
Master Degree	37%	38%
M.Phil.	8%	11%
PhD	2%	3%
Experience		
Less than 1 years	31%	29%
1 to 5 years	43%	43%
5 to 10 years	22%	16%
More than 10 years	5%	6%

3.2. Descriptive statistics

By taking the mean and standard deviation of Gender, we get 1.48 and 0.501, respectively. The mean of age is 1.85, and the Standard deviation of age is 1.002. The mean and standard deviation of education is 2.61 and 0.834, respectively. Experience has a mean of 2.00 and a standard deviation of 0.856. Perceived Privacy risk has a mean of 3.05 and a standard deviation of 0.763. Mean, and standard deviation of Privacy concern is 3.40 and 0.900, respectively. The mean and Standard deviation of Perceived Ownership is 3.49 and 0.807. The mean of anxiety is 3.19, and the Standard deviation of anxiety is 0.618. Trust has a mean of 3.10 and a standard deviation of 0.773. Mean, and Standard Deviation of Unwillingness on sharing Personal Information is 2.31 and 0.816, respectively.

Table 3. Descriptive

Variables	Mean	Standard Deviation
Gender	1.48	0.501
Age	1.85	1.002
Education	2.61	0.834
Experience	2.00	0.856
Perceived Privacy Risk	3.05	0.763
Privacy Concern	3.40	0.900
Perceived Ownership	3.49	0.807
Anxiety	3.19	0.618
Trust	3.10	0.773
Unwillingness on sharing Personal Information	2.31	0.816

3.3. Reliability

Data and questionnaire reliability create a factor of trust and increases the ability of people to depend on it. Through this rise in the factor of reliability, we see that the questionnaires are settled as requirements demand, which includes the needed hypothesis and its variable. Reliable data also shows that responses are consistent with the literature (Fiese & Kline, 1993).

After simple tests and brainstorming, final research was conducted, which included a total of 91 respondents. Through the help of SPSS, we confirmed the consistency of data. Acceptance of results was tested through an evaluation, which led to answers of it being accepted or not. Cronbach's alpha was used to check the reliability and to which excellent results were obtained. The value of alpha is considered good when it is at least 0.7, it is considered better with 0.8, and a figure of 0.9 is considered excellent (Fink & Litwin, 1995).

In the current study, it also calculated both variables separately to test the reliability of each variable, and to a good new for us, it was a great result considering Cronbach's alpha value was 0.823 for good governance and for the dependent variable, which was job satisfaction, Cronbach's alpha value of PPR is 0.848 which is acceptable. The reliability of PC, PO, ANX, TR, PI is 0.866, 0.884, 0.735, 0.781 and 0.947 respectively. All the values are greater than 0.7 means all variables have reliable items. The alpha value is shown in table number 4.

Table 4. Reliability

Variables	Reliability (Cronbach Alpha)
Perceived Privacy Risk	0.848
Privacy Concern	0.866
Perceived Ownership	0.884
Anxiety	0.735
Trust	0.781
Unwillingness on sharing Personal Information	0.947

3.4. Validity and Correlation Analysis

Before moving toward the analysis of our hypothesis, we had to be sure in the aspect of the validity of our questionnaire and data. We are satisfied with the face validity because of it being approved and reviewed by our senior researchers. For the approval of our content validity, we had to compare it with data of previous authors, and through their data, we adopted and improvised our questionnaires. Discriminant validity can be reviewed through the Pearson correlation. Pearson correlation is used to calculate the association between different variables of the relevant model. They can either be positively correlated or negatively correlated. It assures about authenticity and fitness of the framework used in theoretical research. The numbers show a positive correlation of all independent and dependent variables (Hair, Black, Babin, Anderson, & Tatham, 1998). Thus, the validity of the questionnaire is proved. Table number 5 shows the correlation value between all the measured constructs. The correlation between perceived privacy risk and unwillingness to share Personal Information is 0.159, which indicates a positive and lower level of correlation. The correlation between privacy concern and unwillingness to share Personal Information is 0.229 is also an indication of the positive and lower level of correlation. The correlation between perceived ownership and unwillingness on sharing Personal Information is 0.141 is a sign of a positive and lower level of correlation. The correlation between anxiety and unwillingness to share Personal Information is 0.165 is also shows a positive and lower level of correlation. The correlation between trust and unwillingness on sharing Personal Information is 0.237, which also shows a positive and lower level of correlation. However, all correlation results are significant as shown hereunder in the table;

Table 5. Correlation and validity

Correlation	1	2	3	4	5	6
1. Perceived Privacy Risk						
2. Privacy Concern	0.627**					
3. Perceived Ownership	0.536**	0.584**				
4. Anxiety	0.593**	0.559**	0.549**			
5. Trust	0.223**	0.155*	0.343**	0.417**		
6. Unwillingness on sharing Personal Information	0.159*	0.229**	0.141*	0.165*	0.237**	

Note: **P-value≤ 0.01, ***P ≤ 0.001

3.5. Regression Analysis

Regression analysis is used to test the hypothesis. Although the method only analyzes the direct effects of H1, H2, H3 and H4. The regression analysis helps to find out the strength of path between two variables. In regression analysis model fitness and significance of mode is identified through model summary and ANOVA.

Model Fitness

The following table 6 shows the model fitness of the proposed research model. The table provides R, R^2, adjusted $R^{2,}$ and standard error of estimates. The results show that the model is comparatively fit.

Table 6. Model Summary

Model	R	R Square	Adjusted R Square	Standard Error
1	0.330	0.759	0.701	0.578

In table 6, R is considered as the correlation coefficient. R identifies the predictability of the dependent variable; in the current study dependent variable is the unwillingness to share personal information, and its value is 0.330. The R square explains proportion variance explained by the independent variable for the dependent variable. The R square value is

0.759, which means the independent variable in explaining the model by 75.9%. Lawrence (2019) alerts about how to separate between R^2 and changed R^2. You can see from our estimation of .759 that our independent factors clarify 75.9 % of the fluctuation of our dependent variable. As per (Ranganathan, Pramesh, & Aggarwal, 2017), admonitions about R^2 are: little R-squared values are not generally an issue, and high R-squared values are not great.

The standard error 0.578 of a model fit is a proportion of the exactness of the model. It is the standard deviation of the residuals. It shows how the wrong one could be if s/he utilized the relapse model to make forecasts or to estimate the dependent variable or variable of interest. The standard error is utilized to get a certainty span for the anticipated values.

Significance of Model

Table 7 shows that the regression model is a good fit for the data. The F in the ANOVA test indicates the overall fitness of the data. The overall table identifies the predictability of the independent variable over the dependent variable

Table 7. ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	14.113	4	3.528	5.823	000
Residual	115.118	190	0.606		
Total	129.231	194			

The t-value and comparing p-value are in the “t” and “Sig.” In table 8, individually, in this model, the tests reveal to. This implies that the independent variable is helpful in the model when the other two factors are in the model. Like the standard error of model fit examined over, the standard error of the coefficients in relapse yield are additionally wished to be as little as could be expected under the circumstances. It reflects Constant 1.881 is the anticipated incentive for the dependent.

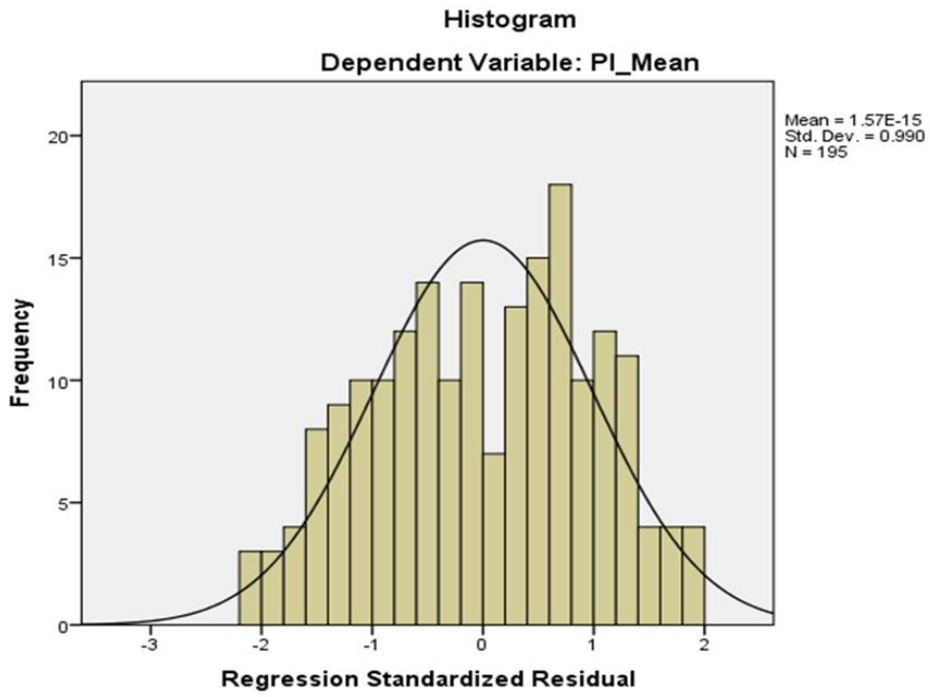
The acceptance or rejection of hypothesis is based beta value of each hypothesis. As H1 measures the impact of personal privacy risk (PPR) on unwillingness to share personal information (PI) and the hypothesis is accepted (β=0.123, p=0.000). the H2 is also accepted measuring the direct effect of privacy concern (PC) on PI and the value is (β=0.338, p=0.001). The relationship of perceived ownership (PO) has positive affect on PI (β=0.291,

p=0.004). The beta value of H4 (β=0.331, p=0.000) is also significant showing the relationship between anxiety (ANX) and PI is positive. The results are given in table 8.

Table 8. Regression Coefficients

Model	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**Correlation**			**Collinearity Statistics**	
(constant)	**B**	**Std. Error**	**Beta**	6.023	0.000	**Zero Order**	**Partial**	**Part**	**Tolerance**	**VIF**
	1.881	0.312								
PPR	0.131	0.103	0.123	1.278	0.000	0.059	0.92	0.088	0.507	1.927
PC	0.306	0.088	0.338	3.489	0.001	0.129	0.245	0.239	0.500	1.999
PO	0.292	0.292	0.291	1.009	0.004	0.041	0.073	0.069	0.571	1.753
AN	0.438	0.122	0.331	3.594	0.000	0.165	0.252	0.246	0.551	1.814

Figure 2. Regression



3.6. Moderation

Using a moderating variable is considered an effective method to increase the research scope regarding a research model. The moderating variable allows generating realistic and accurate results regarding the mechanism of a model by strengthening and identifying the relationship between independent and dependent variables (Namazi & Namazi, 2016). The current study has used the process macro in SPSS for testing moderation, and the macro is developed by (Hayes & Preacher, 2013). The current study has only one moderator and there are four moderating hypothesis H5, H56, H7 and H8. The H4 is supported as the results illustrated by analysis shows estimate of H5 is (E=0.0953, S.E.=0.0964, p=0.001). Hypothesis H6 is also positively significant as the estimate is H2a is (E=0.0062, S.E.=0.0684, p=0.008) is also significant. The H7 is supported as the results illustrated by analysis shows estimate of H4 is (E=0.0603, S.E.=0.0659, p=0.003). Hypothesis H8 is also positively significant as the estimate is H2a is (E=0.1439, S.E.=0.0744, p=0.005) is also significant. The results are shown below in Table 9.

Table 9. Moderation

Hypothesis	**Variables**	**Estimates**	**Standard Error**	**The upper-level confidence interval**	**The lower-level confidence interval**	**Response**
H5	PPR→TR→UPI	0.0953	0.0964	0.0948	0.2855	Supported
H6	PC→TR→UPI	0.0062	0.0684	0.1286	0.1411	Supported
H7	PO→TR→UPI	0.0603	0.0659	0.1902	0.0697	Supported
H8	ANX→TR→UPI	0.1439	0.0744	0.1030	0.2907	Supported

Hypothesis Summary

Table 10. Hypothesis Summary

Hypothesis	**Result**
H1: Perceived privacy risk has a positive influence on the unwillingness to share personal data.	Supported
H2: Privacy concern has a positive influence on the unwillingness to share personal data.	Supported
H3: Perceived ownership has a positive influence on the unwillingness to share data.	Supported
H4: Anxiety has a positive influence on the unwillingness to share data.	Supported
H5: The higher trust level will lower the positive association between perceived privacy risk and unwillingness to share data.	Supported
H6: The higher trust level will lower the positive association between privacy concerns and unwillingness to share data.	Supported
H7: The higher trust level will lower the positive association between perceived ownership and unwillingness to share data.	Supported
H8: The higher trust level will lower the positive association between anxiety and unwillingness to share data.	Supported

3.7. Interpretation of findings

The current study examines the antecedents of an outcome variable. The outcome variable is the unwillingness to share personal information. There are four antecedents that are being a student in the current investigation, and these are personal privacy risk, privacy concern, perceived ownership, and anxiety. These mechanisms in the current research model are enhanced by the addition of a moderator between the privacy attitudes and unwillingness to share information, and the moderator is trust.

The data analysis has shown that people are not willing to share their personal data and information to different sites. Sharing personal data is not related to trust; a lot of people don't want their personal information to sites or people whom they even trust. It's about the comfortability of the customer, and some customers will share their personal data with untrusted websites without blinking an eye. Some will never, even to a trusted site, and our study is in line with the research of (Gerlach, Widjaja, & Buxmann, 2015; Pu & Grossklags, 2017). Our study has shown that a sense of perceived ownership can influence some people to share their personal data but still not everyone, and our results are aligned with the results in the (Yang & Maxwell, 2011). As shown in our study and study conducted by (Robinson, 2017; Wakefield, 2013), Anxious people are less likely to share their personal data due to their anxiety issues.

Our results have shown that for a lot of customers, not all but for the vast majority of the customers, trust can positively affect the relationship between perceived privacy risk and unwillingness to share data and our results are the same as shown in the (Taddei & Contena, 2013). Trust can lower a customer's tension to not share data; if a customer starts trusting the website or store, there is a very high probability that they will trust the store with their personal data, the same can be said for the relationship between perceived ownership and unwillingness to share data, and our results are aligned with the results shown by (Keith, Babb, Lowry, Furner, & Abdullat, 2015). A customer with anxiety issues is mostly anxious about their data getting leaked by some store or website, but if customers with anxiety issues and the store have a positive and trustworthy relationship, even these customers will be willing to share their personal data with the store or website.

CONCLUSION AND RECOMMENDATIONS

Privacy concerns of individuals are increasing day by day with the emergence of modern technologies. The willingness to share data during online shopping is dependent on different factors. Sometimes, individuals will not be willing to share personal data just because they feel anxiety about sharing personal information. Therefore, in the current study, we explore the influence of antecedents that can confine or drive individuals for personal data sharing. The aim of the current thesis was to explore the factor which leads the customers to unwillingness about personal data sharing during online transactions, specifically during online shopping. These factors are explored in the context of the customer's perceived risks, privacy concerns, perceived ownership, and anxiety. Additionally, the role of trust was also explored as a moderator variable. Primary research data was collected from 195 college students of Sweden. The cross-section survey technique was used for data collection, and an online close-ended questionnaire link was sent to college-going students. Questionnaire data is analysed with the help of SPSS v26.

It is evident from theoretical analysis of unwillingness of personal data sharing that consumers feel a sense of ownership of their information which restrict them from sharing. Second, more privacy concerns are linked to more data sharing unwillingness. Third, theoretical analysis shows that online transactions are now mostly full of fraud and identity theft which increases the chances of privacy risk.

The statistical analysis supports all eight proposed hypotheses of this study. First, it is evident from results that a higher level of trust can increase individuals' willingness to share personal data during online shopping. Second, privacy concern is the key antecedent of data sharing unwillingness. Third, the results show that individuals' anxiety of data sharing is not a big reason behind data sharing unwillingness. Forth, the feeling of perceived data ownership changes from individual to individual. Finally, even a higher privacy concern can be changed to lowest stage through trust.

Based on results, first, this study suggested that online vendors should gain consumers' trust to get consumers' data, which is necessary for their marketing purposes. Second, it would be beneficial for vendors if they specifically mention that they will care for consumers' privacy and disclose their third party data access policy. Third, online businesses can get more consumers' information if they introduce a mechanism which ensures consumers about their

data ownership and also give free-hand to consumers' to hide or change their confidential information.

No doubt, the current study contributes to the existing literature of marketing in the context of consumers' willingness to share data; still, there are some limitations. This study only explores antecedents of unwillingness to share data along with a single moderator. Future studies can include other mediators and moderators in the same theoretical framework. Also, studying cultural differences as a mediator would be beneficial for further studies. Furthermore, a longitudinal study by taking individuals from different countries and comparison of antecedents influence would be useful.

SUMMARY

SHREY BHATIA

FACTORS THAT INFLUENCE UNWILLINGNESS TO SHARE PERSONAL DATA IN ONLINE COMMERCE

Final Master Thesis

Academic supervisor: Prof MINDAUGAS DEGUTIS

Vilnius University, FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

Marketing and Integrated Communication

Vilnius, 2020

Size: 61 pages, 2 figures, 10 tables, 1 appendix

The aim of this study was to explore antecedents that can positively influence individuals' unwillingness to share personal data, specifically in an online shopping context. In addition, it was proposed by the author that trust plays the role of moderator, i.e., the higher level of trust can lower the individuals, privacy concerns, anxiety, perceived privacy risks, and perceived ownership and thus pushed individuals to share personal data. Data was collected through a cross-section online survey technique. All questions about constructs were asked on a Likert scale, i.e., a close-ended questionnaire. Primary data collected for the current study from college-going students and data were analyzed with the help of SPSS and Hayes Process Macro. The statistical techniques used for interpretation of were descriptive, regression analysis, correlation analysis, and moderation analysis. The findings of the current study revealed that all factors privacy concerns, anxiety, perceived privacy risks, and perceived ownership positively influence unwillingness to share personal data. Further, Hayes Process Macro also confirms all hypotheses about the moderation role of trust. Finally, the findings of this study are vital contribution to existing literature of marketing, online vendors can improve trust level of their consumers for data sharing.

References

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

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016a). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Basel, S. R. (2018). *The Confidant's Role in Managing Private Disclosures: An Analysis Using Communication Privacy Management Theory*.

Baxter, L. A., & Braithwaite, D. O. (2008). Relational dialectics theory. *Engaging Theories in Interpersonal Communication: Multiple Perspectives*, 349–361.

Beales III, J. H., & Muris, T. J. (2008). Choice or consequences: Protecting privacy in commercial information. *U. Chi. L. Rev.*, *75*, 109.

Benndorf, V., & Normann, H. (2018). The Willingness to Sell Personal Data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. https://doi.org/10.1111/sjoe.12247

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

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, *43*(11), 98–105.

Branton, P. (1969). Behaviour, Body Mechanics and Discomfort. *Ergonomics*, *12*(2), 316–327. https://doi.org/10.1080/00140136908931055

Carufel, R. (2017, July 26). *Consumers are reluctant to share data—What are the exceptions?* Agility PR Solutions. https://www.agilitypr.com/pr-news/public-relations/consumers-reluctant-share-data-exceptions/

Castaldo, S., & Grosso, M. (2014). Retailer-customers relationships in the online setting: An empirical investigation to overcome privacy concerns and improve information sharing. In *Handbook of research on retailer-consumer relationship development* (pp. 404–425). IGI Global.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, *19*(1), 7–19.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y

Chen, Chiang, & Storey. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, *36*(4), 1165. https://doi.org/10.2307/41703503

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, *54*, 483–490.

Child, J. T., & Westermann, D. A. (2013). Let's Be Facebook Friends: Exploring Parental Facebook Friend Requests from a Communication Privacy Management (CPM) Perspective. *Journal of Family Communication*, *13*(1), 46–59. https://doi.org/10.1080/15267431.2012.742089

Cooper, T., & LaSalle, R. (2015). Guarding and growing personal data value. *Accenture Institute for High Performance*.

Crespo, Á. H., del Bosque, I. R., & de los Salmones Sánchez, M. G. (2009). The influence of perceived risk on Internet shopping behavior: A multidimensional perspective. *Journal of Risk Research*, *12*(2), 259–277.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed). SAGE Publications.

Culnan, M. J. (1993). " How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 341–363.

Dinev, T., & Hart, P. (2005). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dittmar, H. (1992). *The social psychology of material possessions: To have is to be*. Harvester Wheatsheaf and St. Martin's Press.

Drinkwater, D. (2016, January 7). *Does a data breach really affect your firm's reputation? | CSO Online*. https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

Dunn, M. G., Murphy, P. E., & Skelly, G. U. (1986). Research note: The influence of perceived risk on brand preference for supermarket products. *Journal of Retailing*.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, *46*(4), 81–83. https://doi.org/10.1145/641205.641209

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research*, *69*(2), 897–904.

Faqih, K. M. (2013). Exploring the influence of perceived risk and internet self-efficacy on consumer online shopping intentions: Perspective of technology acceptance model. *International Management Review*, *9*(1), 67–77.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Ferri, F., Grifoni, P., & Guzzo, T. (2010). Social aspects of mobile technologies on web tourism trend. In *Social Computing: Concepts, Methodologies, Tools, and Applications* (pp. 896–910). IGI Global.

Feuchtl, S., & Kamleitner, B. (2009). Mental Ownership as Important Imagery Content. *Advances in Consumer Research*, *36*.

Fiese, B. H., & Kline, C. A. (1993). Development of the Family Ritual Questionnaire: Initial reliability and validation studies. *Journal of Family Psychology*, *6*(3), 290–299. https://doi.org/10.1037/0893-3200.6.3.290

Flaiz, W. (2017). *Consumer Privacy Concerns and What Companies Need to Do*. https://www.linkedin.com/pulse/consumer-privacy-concerns-what-companies-need-do-william-flaiz

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002

Furby, L. (1978). Possession in humans: An exploratory study of its meaning and motivation. *Social Behavior and Personality: An International Journal*, *6*(1), 49–65.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421. https://doi.org/10.2307/795891

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), 33–43.

Gilbert, D., Lee-Kelley, L., & Barton, M. (2003). Technophobia, gender influences and consumer decision-making for technology-related products. *European Journal of Innovation Management*, *6*(4), 253–263. https://doi.org/10.1108/14601060310500968

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. https://doi.org/10.1016/j.im.2017.02.004

Godin, S. (1999). *Permission marketing: Turning strangers into friends, and friends into customers*. Simon & Schuster.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, *10*(1), 149–166.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *30*(4), 395–410.

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). *FACILITATING GLOBAL E-COMMERCE: A COMPARISON OF CONSUMERS' WILLINGNESS TO DISCLOSE PERSONAL INFORMATION ONLINE IN THE U*. *11*(1), 13.

H. Akhter, S. (2014). Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, *31*(2), 118–125. https://doi.org/10.1108/JCM-06-2013-0606

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. (2006). *Multivariate data analysis. Uppersaddle River*.

Hamilton, J. (1989). Comfort and the hospitalized chronically ill. *Journal of Gerontological Nursing*, *15*(4), 28–33.

Harbert, T. (1998). *EDN - NONE OF YOUR BUSINESS - Tam Harbert*. https://www.edn.com/none-of-your-business/

Hayes, A. F., & Preacher, K. J. (2013). Conditional process modeling: Using structural equation modeling to examine contingent causal processes. In *Structural equation modeling: A second course, 2nd ed* (pp. 219–266). IAP Information Age Publishing.

Heirman, W., Walrave, M., Ponnet, K., & Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *7*(3). https://doi.org/10.5817/CP2013-3-3

Hinde, S. (1998). Privacy and security—The drivers for growth of E-Commerce. *Computers & Security*, *17*(6), 475–478.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80–85.

Hong, I.B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management*, *33*(6), 927–939.

Hong, Ilyoo B., & Cho, H. (2011). The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. *International Journal of Information Management*, *31*(5), 469–479. https://doi.org/10.1016/j.ijinfomgt.2011.02.001

Irwin, L. (2020, January 1). *The GDPR: What exactly is personal data?* IT Governance Blog En. https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Jai, T.-M. (Catherine), & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, *28*, 296–303. https://doi.org/10.1016/j.jretconser.2015.01.005

Janssen, M., & Kuk, G. (2016). *The challenges and limits of big data algorithms in technocratic governance*.

Janssen, M., & van den Hoven, J. (2015). *Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?*

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, *1*(1), 45–71. https://doi.org/10.1023/A:1019104520776

Joinson, A. N., McKenna, K. Y. A., Postmes, T., & Reips, U.-D. (Eds.). (2012). *Oxford Handbook of Internet Psychology* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199561803.001.0001

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human–Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662

Katz, J. E., & Tassone, A. R. (1990). A report: Public opinion trends: Privacy and information technology. *The Public Opinion Quarterly*, *54*(1), 125–143.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564.

Kim, Y. H., & Kim, D. J. (2005). *A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction*. 170c–170c.

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

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for ….

Larose, R., & Rifon, N. J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, *41*(1), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

Lawrence, J. (2018). *Customer Data Collection is Crucial... Here's Why*. https://www.leightoninteractive.com/blog/why-collecting-customer-data-is-crucial

Lawrence, K. D. (2019). *Robust regression: Analysis and applications*. Routledge.

Lee, M. K. O., & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, *6*(1), 75–91. https://doi.org/10.1080/10864415.2001.11044227

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. https://doi.org/10.1016/j.dss.2011.01.017

Lin, D., & Loui, M. C. (1998). Taking the byte out of cookies: Privacy, consent, and the Web. *ACM SIGCAS Computers and Society*, *28*(2), 39–51. https://doi.org/10.1145/276758.276775

Lindblad, R., & Sasivanij, T. (2017). *Consumer perceptions on the privacy-invasiveness of in-feed advertisements*.

Litwin, M. (1995). *How to Measure Survey Reliability and Validity*. SAGE Publications, Inc. https://doi.org/10.4135/9781483348957

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. https://doi.org/10.1007/s11747-006-0003-3

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.

MarTech Advisor. (2019). *What is Customer Data? Types, Collection and Analysis of Customer Data | MarTech Advisor*. https://www.martechadvisor.com/articles/data-management/customer-data-definition-types-collection-validation-analysis-martech101/

Martínez-Mesa, J., González-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: How to select participants in my research study? *Anais Brasileiros de Dermatologia*, *91*(3), 326–330. https://doi.org/10.1590/abd1806-4841.20165254

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model Of Organizational Trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, *6*(2), 35–59. https://doi.org/10.1080/10864415.2001.11044235

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359.

Metzger, M. J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Mieres, C. G., Martín, A. M. D., & Gutiérrez, J. A. T. (2006). Influence of perceived risk on store brand proneness. *International Journal of Retail & Distribution Management*.

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing*, *19*(1), 1–6.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29.

Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organisations*, *6*(6), 574. https://doi.org/10.1504/IJNVO.2009.027790

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Minkara, O. (2014, December 4). Using Customer Data for Marketing: The Good, Bad & Ugly. *Aberdeen*. https://www.aberdeen.com/cmo-essentials/good-bad-ugly-using-customer-data-for-marketing/

Mitchell, V. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing*, *33*(1/2), 163–195. https://doi.org/10.1108/03090569910249229

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20–38.

Myerscough, S., Lowe, B., & Alpert, F. (2006). Willingness to Provide Personal Information Online: The Role of Perceived Privacy Risk, Privacy Statements and Brand Strength. *Journal of Website Promotion*, *2*(1–2), 115–140. https://doi.org/10.1080/15533610802104182

Nam, C., Song, C., Park, E. L., & Ik, C. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *ACR North American Advances*.

Namazi, M., & Namazi, N.-R. (2016). Conceptual analysis of moderator and mediator variables in business research. *Procedia Economics and Finance*, *36*(16), 540–554.

Newell, B. C. (2014). Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly*, *31*(3), 421–431. https://doi.org/10.1016/j.giq.2014.04.001

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron. *BUL Rev.*, *81*, 635.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Nowak, G. J., & Phelps, J. E. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing*, *6*(4), 28–39.

Oberndorf, S. (1998). *Users remain wary—Multichannel Merchant*. https://multichannelmerchant.com/news/users-remain-wary/

Parent, W. A. (1983). A new definition of privacy for the law. *Law and Philosophy*, *2*(3), 305–338.

Parloff, M. B., Kelman, H. C., & Frank, J. D. (1954). Comfort, effectiveness, and self-awareness as criteria of improvement in psychotherapy. *American Journal of Psychiatry, 111*(5), 343–352.

Pastore, M. (1999). *Consumers Will Provide Information for Personalization—ClickZ*. https://www.clickz.com/consumers-will-provide-information-for-personalization/57216/

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Personal Data Sharing—Are We Really in Control? (2019, June 11). Data Protection Blog. https://dataprotection.blog/personal-data-sharing-are-we-really-in-control/

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*(1), 6–14.

Petronio, S. (2015). Communication privacy management theory. *The International Encyclopedia of Interpersonal Communication*, 1–9.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, *15*(4), 2–17.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The State of Psychological Ownership: Integrating and Extending a Century of Research. *Review of General Psychology*, *7*(1), 84–107. https://doi.org/10.1037/1089-2680.7.1.84

Pineau, C. (1982). The psychological meaning of comfort. *Applied Psychology*, *31*(2), 271–282. https://doi.org/10.1111/j.1464-0597.1982.tb00097.x

Pingitore, G., Rao, V., Cavallaro, K., & Dwivedi, K. (2017). *What consumers really think about sharing their personal information*. 11.

Posner, R. A. (1977). The right of privacy. *Ga. L. Rev.*, *12*, 393.

Pu, Y., & Grossklags, J. (2017). *Valuating friends' privacy: Does anonymity of sharing personal data matter?* 339–355.

Raban, D. R., & Rafaeli, S. (2007). Investigating ownership and the willingness to share information online. *Computers in Human Behavior*, *23*(5), 2367–2382. https://doi.org/10.1016/j.chb.2006.03.013

Ranganathan, P., Pramesh, C., & Aggarwal, R. (2017). Common pitfalls in statistical analysis: Logistic regression. *Perspectives in Clinical Research*, *8*(3), 148.

Rice, R. E., McCreadie, M., & Chang, S.-J. L. (2001). *Accessing and browsing information and communication*. Mit Press.

Robinson, C. (2017a). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582.

Robinson, C. (2017b). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Robinson, S. C. (2014). *Consumer intent to disclose personal information in ecommerce: A comparison of Estonia and the United States*.

Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214–233. https://doi.org/10.1080/10919392.2018.1482601

Saunders, M. N., & Lewis, P. (2012). *Doing research in business & management: An essential guide to planning your project*. Pearson.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online

Purchase Intentions. *Journal of Marketing*, *70*(2), 133–148. https://doi.org/10.1509/jmkg.70.2.133

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*(3), 2–16. https://doi.org/10.1002/dir.10033

Schudy, S., & Utikal, V. (2017). 'You must not know about me'—On the willingness to share personal data. *Journal of Economic Behavior & Organization*, *141*, 1–13.

Sehat, M., & Paves Flores, R. (2012). *Customer Data Management*.

Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, *13*(5), 305–319.

Sheehan, K. B., & Hoy, M. G. (1999). Using e-mail to survey Internet users in the United States: Methodology and assessment. *Journal of Computer-Mediated Communication*, *4*(3), JCMC435.

Siefert, M. L. (2002). Concept Analysis of Comfort. *Nursing Forum*, *37*(4), 16–23. https://doi.org/10.1111/j.1744-6198.2002.tb01288.x

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce*, *10*(1), 1–16.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

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

Swant, M. (2019). *People Are Becoming More Reluctant To Share Personal Data, Survey Reveals*. Forbes. https://www.forbes.com/sites/martyswant/2019/08/15/people-are-becoming-more-reluctant-to-share-personal-data-survey-reveals/

Taddei, S., & Contena, B. (2013a). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Taddei, S., & Contena, B. (2013b). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Thomas, R. E., & Maurer, V. G. (1997). Database marketing practice: Protecting consumer privacy. *Journal of Public Policy & Marketing*, *16*(1), 147–155.

Uilenberg, A. (2015). *Willingness to disclose personal information when shopping online: A comparison between consumers from the Netherlands, Germany, and Indonesia*.

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2).

Van Dyne, L., & Pierce, J. L. (2004). Psychological ownership and feelings of possession: Three field studies predicting employee attitudes and organizational citizenship behavior: PSYCHOLOGICAL OWNERSHIP. *Journal of Organizational Behavior*, *25*(4), 439–459. https://doi.org/10.1002/job.249

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003

Walrave, M., & Heirman, W. (2012). Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes: Adolescents, Online Marketing and Privacy. *Children & Society*, no-no. https://doi.org/10.1111/j.1099-0860.2011.00423.x

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193. https://doi.org/10.2307/1321160

Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, *7*, 431–453.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, *14*(1 & 2), 41–51.

Wolff, C. (2017, September 7). *Your customers are more willing to share their data than you thought*. Lucky Cart. http://www.luckycart.com/your-customers-are-more-willing-to-share-their-data-than-you-thought/

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. https://doi.org/10.1016/j.chb.2011.12.008

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, 6.

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164–175.

Ziefle, M., Halbey, J., & Kowalewski, S. (2016). *Users' Willingness to Share Data on the Internet: Perceived Benefits and Caveats.* 255–265.

Appendix A

Questionnaire for participants

Section I

Demographics

1. Gender Male☐ Female☐

2. Age (in years) 20 - 30 ☐ 31 – 40 ☐ 41 – 50 ☐ 51 – 60 ☐

3. Level of education PhD ☐ M.Phil. ☐ Master's Degree ☐ Graduation ☐

Other (specify) ……

4. Experience (related to online shopping or any other online transactions)

Less than 1 year ☐ 1-5 ☐ 6-10 ☐ 11 -15 ☐ 16-20 ☐ 21 and above ☐

Section II

I am a Masters researcher from Vilnius University undertaking a research on the topic:*"FACTORS THAT INFLUENCE WILLINGNESS TO SHARE PERSONAL DATA IN ONLINE COMMERCE".* Please read each descriptive statement carefully and indicate your degree of agreement or disagreement by selection appropriate option, that is, best describes how you feel about the statements. Allow yourself to remember that your answer will keep confidential and use only for educational purposes. Your name will not appear anywhere in this document.

1	**2**	**3**	**4**	**5**
Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

Perceived privacy Risk

1.	Online shopping is risky.	1	2	3	4	5
2.	Providing credit card information online is risky.	1	2	3	4	5
3.	Providing personal information (i.e. social security number and mother's maiden name) online is risky.	1	2	3	4	5
4.	Purchasing items online is risky.	1	2	3	4	5

5.	Providing my e-mail address and phone number online is risky.	1	2	3	4	5
6.	Registering online is risky.	1	2	3	4	5
7.	It is riskier to shop online for a product than to shop offline for it.	1	2	3	4	5

Privacy Concern

1.	I am concerned that the information I submit on the internet could be misused.	1	2	3	4	5
2.	I am concerned that a person can find private information about me on the internet.	1	2	3	4	5
3.	I am concerned about submitting information on the internet, because of what others might do with it.	1	2	3	4	5
4.	I am concerned about submitting information on the internet, because it could be used in a way I did not foresee.	1	2	3	4	5

Perceived ownership

1.	Information I share while online purchasing is MY personal information.	1	2	3	4	5
2.	I sense that the information I provide while online purchasing is my own.	1	2	3	4	5
3.	I feel a very high degree of personal ownership for the information I provide during online purchase.	1	2	3	4	5
4.	I sense that the information I provide during online purchase is personal.	1	2	3	4	5

5.	I believe that the information I disclose during online purchase belongs to me.	1	2	3	4	5

Anxiety

1	I felt uncomfortable providing the information during online shopping.	1	2	3	4	5
2	It wasn't stressful at all during online shopping.	1	2	3	4	5
3	I didn't feel intimidated during online shopping.	1	2	3	4	5
4	I was uncertain about providing information during online shopping.	1	2	3	4	5
5	I was anxious about being asked for my information during online shopping.	1	2	3	4	5
6	I would have preferred not to provide all the information during online shopping.	1	2	3	4	5
7	I was relaxed without any worries during online shopping.	1	2	3	4	5

Trust

1	I trust the online stores and would purchase products from online stores.	1	2	3	4	5
2	I believe that the online store is trustworthy.	1	2	3	4	5
3	I believe the online stores will keep their promises and commitments.	1	2	3	4	5

Unwillingness to share personal data

How willing are you to disclose the following personal information to the webpage you visit?

Please encircle the number that describes your opinion.

1	**2**	**3**	**4**	**5**
Not at all willing	**Only a little willing**	**To some extent willing**	**Rather much willing**	**Very willing**

1	Name	1	2	3	4	5
2	Home e-mail address	1	2	3	4	5
3	Home address	1	2	3	4	5
4	Home phone number	1	2	3	4	5
5	Work email address	1	2	3	4	5
6	Work address	1	2	3	4	5
7	Work phone number	1	2	3	4	5
8	Credit card details	1	2	3	4	5
9	Date of birth	1	2	3	4	5
10	Age	1	2	3	4	5
11	Weight	1	2	3	4	5
12	Medical history	1	2	3	4	5
13	Media habits	1	2	3	4	5
14	Financial information (e.g. income, credit history)	1	2	3	4	5
15	Lifestyle data (e.g. number of pets, house owner or rental)	1	2	3	4	5