UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

The social media and e-commerce information trade:

Is privacy protection a losing game?

_

A master thesis written by Miranda Okello.

Graduate School - Knowledge-based Entrepreneurship
Spring semester, 2022
Supervisor: Marouane Bousfiha

Abstract

Background: As technology progresses and more information is gathered to meet the increasing demands of consumers, - businesses on social media and e-commerce sites are working on becoming increasingly practical and effective in delivering their services (e-services). However, users are becoming increasingly concerned about online privacy and the possibilities of organizations' exploiting personal, private information, - the benefits of partaking in these e-services are being increasingly questioned. This thesis validates a model that analyses organizational privacy assurances and policies, - on users' privacy concerns, risk perceptions, trusting beliefs, and non-self-disclosure behaviour.

Purpose: The purpose of this study is to explain how organizational privacy assurances can be related to users' privacy concerns, risk perceptions, trusting beliefs, and self-disclosure behaviour.

Methodology: A quantitative research approach was used with an online self-completion questionnaire as a data collection method distributed via Facebook. In total, there were 100 valid responses.

Findings and conclusions: 14 hypotheses were tested and part of the research model. Three out of the 14 hypotheses were rejected under the null hypothesis. The findings suggest that social media and e-commerce users are aware of the potential risks of agreeing to disclose personal information. The result indicates that trusting beliefs are negatively affected in situations where risk perceptions are heightened. It is also in situations of perceptions of heightened risks, and lower levels of trust, - where users exhibit non-self-disclosure behaviour.

The findings serve to develop a practical- and theoretical understanding of organisational privacy assurances and users' privacy concerns, trusting beliefs, and self-disclosure behaviour. The findings suggest that organisations can better generate positive perceptions by developing privacy policies and self-self-regulations in a way that assures users of their devotion to user privacy and their high commitments to users' safety.

Table of Contents

1. Introduction

The following chapter will provide a background and a discussion concerning the chosen literature topic, which will lead to the purpose of this study.

1.1. Background to the study

As technology progresses and more information is gathered to meet the increasing demands of consumers, - businesses on social media and e-commerce sites are working on becoming increasingly practical and effective to deliver these services, also known as e-services. There are a multitude of different e-services that exist today, they may for example be or privately- or governmentally owned e-services, both of which are part of discussions of information privacy and the possibilities of information exploitation, as companies have collected, stored, processed, and exploited users' privacy in the past (CIGI & Ipsos, 2018; Hong and Thong, 2013; Mutimukwe, Kolowska & Grönlunda, 2020; Durnell et al., 2020; Farshadkhah, Van Slyke & Fuller, 2021; Sharma, Singh & Pratt, 2021).

Along with the increasing demands, the online experience is constantly developed and improved for users, - acting to benefit both the service providers and the service users. However, as users are becoming increasingly concerned about online privacy and the exploitation of personal, private information, - the benefits of partaking in these e-services are being questioned. A study covering over 25 different economies with over 25,000 participants conducted by the Centre for International Governance Innovation, - showed that 78 % of respondents are concerned about their online privacy, which is an increase of 53 % since the year prior (CIGI & Ipsos, 2018; Hong and Thong, 2013; Mutimukwe, Kolowska & Grönlunda, 2020; Durnell et al., 2020; Farshadkhah, Van Slyke & Fuller, 2021; Sharma, Singh & Pratt, 2021).

As a result of the increasing concerns, studies have analysed different factors that play into increased privacy concerns. Factors that affect privacy concerns relate to

users having unauthorized access, - making users feel vulnerable and not in control of their own personal information according to Dinev and Hart (2004) and Mutimukwe, Kolowska & Grönlunda (2020). With the user being secondary in the use of his or her own personal information, perceptions of privacy risks may increase to a point where the perceptions could lead to users hesitating to disclose information or potentially discontinuing relationships with entire organizations due to lack of trust. In order for organizations to have a basis of trust amongst users and encourage users to continue to share information, - organizations must seek to understand how potential risks relating to privacy are perceived amongst users (Sharma, Singh & Pratt, 2021; Mutimukwe, Kolowska & Grönlunda, 2020; Libaque-Saenz et al., 2016; Abri, Mcgill, & dixon, 2009; Libaque-Saenz, Chang, Kim, Park, & Rho, 2016; Malhotra, Kim & Agarwal, 2004; Chang et al, 2018).

Studies attempting to close this research gap often consider the organization's privacy assurance mechanisms, but fail to relate the mechanisms to what the individual user finds important, while other studies explore organizational privacy assurance mechanisms relating to trust without factoring in the antecedents to privacy perceptions and concerns of users (Sharma, Singh & Pratt, 2021; Mutimukwe, Kolowska & Grönlunda, 2020; Libaque-Saenz et al., 2016; Abri, Mcgill, & dixon, 2009; Libaque-Saenz, Chang, Kim, Park, & Rho, 2016; Malhotra, Kim & Agarwal, 2004; Chang et al., 2018).

Furthermore, issues relating to privacy are often dependent on context and situation, meaning that studies addressing privacy on social media differ from those addressing privacy and the healthcare industry. For example, Kantarcioglu & Ferrari (2019), Wu (2014), and Jansen & Van Den Hoven (2015) argues that governmental organizations handle more sensitive data in a less restricted manner than organizations in the commercial sector due to governmental organizations being able to enforce mandatory disclosure of personal information by law. All privacy constructs are not only psychological constructs, but they are also affected by regulatory environments, culture, and security technology (Ebert, Ackermann,

Heinrich, 2020; Barth & Jong, 2017; Kolotylo-Kulkarni, Xia & Dhillon, 2021; Gómez-Barroso, 2021; Nam et al., 2006; Van Dyke, Midha and Nemati, 2007).

In the context of e-retailers, studies have shown that consumers may exit sites and leave their shopped items due to privacy concerns. Users' have also shown to enter false information as a means of remaining anonymous (Farooq & Qureshi, 2020; Ranganathan & Gordon, 2002; Hoffman et al., 1999). Organizations' collection and use of data may be limited due to consumers' privacy concerns, as there is an apparent trade-off between choosing to disclose personal data and choosing to not disclose personal data and not being able to use services in full. The consumer privacy calculus consists of weighing the benefits against the potential risks. If there are additional benefits to the shopping experience such as different personalization features, - it is more likely that the consumer continues shopping (Kanwal, Anjum & Khan, 2021; Dinev & Hart, 2006; Beke, Eggers, Verhoef & Verhoef, 2018; Wieringa & Jaap; 2021). Murray & Häubl (2009) argue that organizations can use tools to contribute to a more enjoyable experience and contribute to the likelihood of the consumer adopting the service.

Dinev and Hart (2004) and Mutimukwe, Kolowska & Grönlunda (2020) suggests that privacy concerns of users is an antecedent to perceived privacy risk and that perceptions of privacy risks can potentially affect users' trust and disclosure behaviour towards the organization in question. It may therefore be important for organizations to understand what these factors imply and how they are formed, - for organizations to ensure that there is a level of trust and disclosure behaviour amongst their users. Therefore, this research will be built on a research model provided by Mutimukwe, Kolowska & Grönlunda (2020) in order to provide suggestions for organizations who wish to have effective privacy assurance mechanisms or privacy policies.

1.2. Purpose

The purpose of this study is to explain how organizational privacy assurances can be related to users' privacy concerns, risk perceptions, trusting beliefs, and self-disclosure behaviour.

1.2.1. Delimitations

In relation to the chosen research model part of this thesis (*see chapter 3*), Mutimukwue, Kolowska, and Grönlund (2020) applied the same model in the context of e-services in Rwanda, - specifically in the contexts of social networking, social media, and e-government sites in Rwanda. This research does not apply the concepts to the same context. Instead, this research focuses on measuring the concepts in the contexts of social media and e-commerce sites. The decision to exclude e-government sites was made partly because of where this study was conducted, which is in Sweden. As suspected before the study was conducted, a lot of participants in this study were Swedish (*see table 5. Demographics)*. Swedish people are often suggested as being rather compliant with their government and their governments' decisions, even through difficult times such as during the height of the covid-19 pandemic (Nielsen and Lindvall, 2021; Harring, 2018). Furthermore, all Swedish "SOM studies" published every year from the "SOM- institution" at the University of Gothenburg, - show that there is a positive relationship of trust in the context of the Swedish government and its governmental organizations. Therefore, the e-governmental context will not be researched further in this study, and it is removed from the original research model. This delimitation is also discussed further in subchapter *8.3 Recommendations*.

1.3. Thesis structure

The thesis is organized into different chapters that each goes through the research process from start to finish. As the introduction and background to the literature topics have now been introduced, - the thesis will explain the research concepts at length in chapter *2 Literature Review*, - to then delve into the research model and all its

constructs in chapter *3 The Conceptual Model*. The thesis will then move onto *chapter 4 methodology* where all information regarding how the thesis was conducted is explained, as well as with what means the thesis was conducted. The thesis then continues with explanations and descriptions of the collected data in *chapter 5 analysis and results*, to then be discussed in relation to theory in chapter *6 discussion*. The thesis is concluded with chapter *7 contributions and conclusions* where both practical and theoretical aspects of the findings are addressed. Finally, *chapter 8 limitations, implications, and recommendations* delve into what limited the research and what could have been done differently, which opens future possibilities for other researchers.

2. Literature review

The following chapter will explain the established literature in the research area as well as explain the different research backgrounds to this thesis.

2.1. Privacy and Privacy Concerns

Numerous studies seek to understand how relationships between users and service providers can be built on a stronger basis of trust, through researching individual user characteristics. These user characteristics often consist of variables relating to privacy concerns, privacy perceptions, information disclosure, and trust, without connection to the service provider. As the service provider builds the privacy systems or mechanisms to assure a sense of privacy through privacy management, - the individual users' perceptions and actions should be more prioritized in privacy management research. Privacy management should be thought of as a transaction between two parties, meaning that no party in the transaction should be singled out. It is not only the individual in question who can exercise certain behaviour to help ensure a sense of trust, but also organizational structures and practices that contribute to privacy management (Xu, Dinev, Smith, and Hart, 2011; Mutimukwe, Kolowska & Grönlunda, 2020, Farshadkhah, Van Slyke & Fuller, 2021).

Privacy is according to Westin (1968) *"the desire of people to have the freedom of choice under whatever circumstances and to whatever extent they expose their attitude and behaviour to others"*. Studies contributing to privacy research have mostly related to the individual's ability to manage their personal information (Stone et al., 1983; Bélanger, Hiller, and Smith, 2002). There are however discussions approaching the matter of privacy from a transactional standpoint. Margulis (1977), concepts of privacy related to the ability to manage transactions between individuals and others to *"enhance autonomy and/or minimize vulnerability"* on those involved in the transaction. Later, Dinev and Hart (2004) also sought inspiration from Margulis (1977) when researching privacy by studying it as a transaction between two parties.

Scientific literature relating to privacy is often coupled with privacy concerns (Dinev and Hart, 2004; Mutimukwe, Kolowska & Grönlunda, 2020). Privacy concerns are according to Xu et al., (2011, 2012) ones worry about possible loss of privacy because of having disclosed information to a certain external player, such as an organization. Therefore, issues relating to privacy concerns are under the assumption that the transaction of information has already occurred.

Both concepts of privacy and privacy concerns intervene with other research concepts that reveal other established literature topics such as trust and self-disclosure behaviour, which are often linked to topics such as privacy or information privacy, which is also why those topics will be explored at length in this thesis (Malhotra et al., 2004; Dinev and Hart, 2004; Dinev and Hart, 2006; Hong and Thong, 2013; Xu et al., 2011; Derlega et al., 1993; Rains, Brunner, and Oman, 2016).

2.2. Privacy in the e-service context

Information privacy is as mentioned a concept that may be explored in different contexts and environments. In the case of information privacy in e-services, the information exchange often occurs between you and an organization. If this information exchange is considered to be worrisome, one might become concerned about one's *actual* level of power of one's own personal information. However, individuals have different desired levels of safe privacy management and different trusting beliefs of how the information will be handled and whether the organization will possess the right abilities to protect you, - users essentially possess different levels of risk tolerance (Xu et al., 2012; Xu et al., 2011, Chang et al., 2018; Mutimukwue, Kolowska, and Grönlund, 2020).

The context of e-services and the privacy transaction is interrelated with trust and concerns as mentioned, but one must not forget that it is a transaction between two parties. The individual or user in the transaction does have the right to withdraw from the transaction and move on if the desired level of privacy management is not

up to one's standards. This concept of non-self-disclosure behaviour is used to note the behaviour of not complying with the presented offer of handling your information (Solve, 2006; Xu et al., 2012; Xu et al., 2011, Chang et al., 2018; Mutimukwue, Kolowska, and Grönlund, 2020).

From the standpoint of the second party in the transaction, the service provider or the organization should arguably be attentive and compliant to their consumers and be able to protect them to their desired levels. As the research connected to privacy was defined as being in a scenario where a transaction occurs, research within this topic should stress both parties' behaviour and thoughts on the matter (Solve, 2006; Mutimukwue, Kolowska, and Grönlund, 2020).

2.3. Organizational privacy assurances

From the organizational standpoint, it is important to deliver the service offer in a manner that leads to a successful interaction with its users. As mentioned, Solve (2006) and Mutimukwue, Kolowska, and Grönlund (2020) stressed that the way organizations handle their users' privacy is linked to research concerning information-disclosure behaviour and concerns, - leading to research concepts as trust being important. A level of trust must be established between both parties in order to form an association, and possibly a transaction. By encouraging trusting beliefs through encouraging communication, the organization may be able to alleviate potential privacy concerns or issues amongst their consumers (Mutimukwue, Kolowska, and Grönlund, 2020; Solve, 2006).

These privacy assurance mechanisms are used for the sole purpose of ensuring their users of their commitments to protecting their privacy, and that it will be held and protected safely by the organization as a custodian (Bansal, Zahedi, and Gefen, 2015; Mutimukwue, Kolowska, and Grönlund, 2020).

2.4. Types of privacy assurance mechanisms

The different types of privacy assurance mechanisms may differ depending on the e-service. However, some of the most commonly used types of privacy assurance mechanisms are often privacy policy statements which are statements that are informative in the way the organization handles their user's information. These types of privacy statements are often made apparent to the user when entering the site or app, along with having the possibility to not comply or disclose any information. There are also examples of privacy assurance mechanisms that make use of a third-party assurance system that assesses each service-provider and provides them with privacy seals of approval if they comply with a set of conditions. Other privacy assurance systems reveal self-policing activities they use to detect, prevent, and/or address possible violations made to their users (Sharma and Kaushik, 2017; Xu et al., 2011; Bansal, Zahedi, and Gefen, 2008; Hui et al., 2007; Culnan and Bies, 2003).

2.5. Related research models

The aforementioned research conducted on information privacy has not addressed the topic in a manner that encompasses all the aforementioned concepts such as privacy concerns or risks in the context of e-services. The studies on this topic conducted by Xu et al., (2008;20011;2012) *does* describe multiple different contexts and their relation to multiple privacy concepts, but there are no connections made between privacy and trust or intentions of trusting in those studies. Instead, the authors urge future researchers to delve deeper into this matter, which authors such as Chang et al., (2018) and Mutimukwe, Kolowska & Grönlunda (2020) did by modelling constructs of privacy policy, perceived privacy, and privacy principles. However, the study conducted by Chang et al., (2018) fails to consider the individual's intentions, feelings, attitudes, and behaviour. While other studies such as studies conducted by Hui et al., (2007), Mousavizaadeh and Kim (2015), Bansal et al., (2008), and Mousavizadeh et al., (2016), fail to delve deep into each concept by choosing to not explore the antecedents to each concept. Similarly, there is little research conducted on the effectiveness of organizations' privacy assurance

mechanisms and little understanding of their effect on users' intentions to trust and use the site's services. However, Bansal et al., (2008) does discuss the topic in brief when discussing how choices regarding design and types of messaging affects the overall company reputation.

Apart from the aforementioned studies, the study conducted by Mutimukwue, Kolowska, and Grönlund (2020) is what could be considered as the foundational starting point for this thesis as mentioned in the introduction. The gap in research is still highly existent, however the research by Mutimukwue, Kolowska, and Grönlund (2020) is still built upon the same set of concepts and the same conceptual model, - but the *contexts* to which the model is applied to is different.

3. The Conceptual Model

The following chapter will explain different theoretical concepts and theoretical dimensions in the research area in order to develop hypotheses. All hypotheses are presented in table 1.

3.1. The building blocks of the model

As mentioned, the model that this research will be based on is the model created by Mutimukwue, Kolowska, and Grönlund (2020) which is an extended version of a model created by Xu et al., (2011). The model gives a visual representation of the concepts that were examined by Mutimukwue, Kolowska, and Grönlund (2020) which will be examined in this thesis but through a different context. All concepts part of the model are privacy concerns, trust beliefs, non-self-disclosure behaviour, privacy risk, perceptions of privacy policy, and perceptions of organizational privacy self-regulations, (*see figure 1*). Not only are the concepts measured alone, but they will be measured against each other in order to detect possible relationships between them, which will be explained in the methodology chapter.

The model is designed to delve into topics concerning how individuals' privacy concerns are linked to individuals' privacy risks. How trust coincides with non-self-disclosure behaviour, or how organizational privacy assurance systems affect individual perceptions of privacy and the potential consequences of not living up to expectations, - leading to measures concerning trust, concerns, and non-self-disclosure behaviour.

In order to find possible relationships or linkages between the aforementioned concepts, - a set of hypotheses was formed, which are all presented in *table 1* below.

Table 1. Hypothesis summary

H1 Perceived privacy risks positively correlates with non-self-disclosure behaviour.
H2 Privacy risks negatively affect one's trusting beliefs.
H3 Perceived effectiveness of privacy policy increases trusting beliefs.
H4 Perceived effectiveness of privacy policy decreases non-self-disclosure behaviour
H5 Perceived effectiveness of privacy policy decreases perceived privacy risks.
H6 Perceptions of effective organizational self-regulation increase trusting beliefs.
H7 Perceptions of effective organizational self-regulation decreases non-self-disclosure behaviour.
H8 Perceptions of effective organizational privacy assurance mechanisms decrease perceptions of privacy risks.
H9 Perceptions of privacy risks raises privacy concerns.

3.2. Hypotheses development

The following sub-chapters will explain the theory behind each hypothesis and explain the reasoning behind each hypothesis.

3.2.1. Perceptions of privacy risks and their impact on us

Equating concepts of risk often occur unconsciously or consciously in situations where there may be uncertainty, - where loss or negative consequences often are a result. Risks are more than not associated with the possibility of having a negative situation at hand (Moon, 2000). However, when put in the set context of e-commerce and social media, the common risk equation relates to topics such as “how will my personal information be used?”, or “can I trust they will handle it with care?”.

Risks in the context of the e-service industry are often linked to issues regarding organizations exploiting personal data which contributes to stories of customers' advocacy for their rights to own what is personally theirs. However, these risk equations also occur at smaller levels, where customers equate whether they want to click the ‘agree’ button, read the privacy assurances, or just exit the site or app. This non-self-disclosure behaviour is what explains the action of stopping the interaction with the site or app, - leading users to not disclosing any information, or perhaps even entering false information (Xu et al., 2011; Abri et al., 2009; Mutimukwue, Kolowska, and Grönlund, 2020).

As risks affect us emotionally, physically, or even materially, - there may be some individuals who possess higher perceptions of risks in a situation. These more ‘suspect’ individuals may exhibit a more self-limiting behaviour and, in some situations, discontinue their relationship with the e-service (Abri et al., 2009; Xu et al., 2011; Mutimukwue, Kolowska, and Grönlund, 2020).

Based on the theory, the following hypothesis is formed:

H1: Perceived privacy risks positively correlates with non-self-disclosure behaviour.

3.2.2. Privacy risks and trust

Trusting beliefs have shown to be linked to concepts of risks according to Dinev and Hart (2006). Trusting beliefs are often equated along with different expectations or feelings of dependability. Malhotra (2004) argues that trusting beliefs in relation to organizations are defined by the degree to which the organization could be dependable in protecting personal data. While Flygeson (2006) argued that there is often a feeling of hope when having trusting beliefs, one still wishes to not be let down in any way. These beliefs are often correlated with expectations on the organization in question and whether the relationship with the organization will be exploitative in any way. Therefore, internet or e-service related risks could be connected to trust mechanisms, meaning that low levels of trust in individuals could

show to be a result of relatively high perceptions of risks (Dinev and Hart, 2004; Mutimukwue, Kolowska, and Grönlund, 2020; Dinev and Hart, 2006; Malhotra, 2004; Liu Marchewka and Lu 2005; Yu, 2005). Therefore, it will be hypothesized that:

H2: Privacy risks negatively affect one's trusting beliefs.

3.2.3. Privacy policies effect on trust, trusting behaviour and perceived privacy risks

There are different ways for e-service- organizations to assure their users of their safety or privacy in order to not have instances of non-self-disclosure behaviour. These mechanisms that are used are often informative of what information will be used and for what purpose their information will be of use, and there may also be choices presented to the individual. These presented choices give the individual the opportunity to read up on the designed safeguards that protect the information against possible information loss, information alterations, or information misuse and how the individual can go about the choice of not disclosing any information or data (Hui et al., 2007; Xu et al., 2011; Mutimukwue, Kolowska, and Grönlund, 2020; Clarke et al., 2000).

Under the assumption that organizations try their best to avoid having to deal with non-self-disclosure behaviour and in a way build up a basis of trust amongst their users, - there are different privacy policy statements that can be used to achieve this effectively. Similarly, Xu et al., (2011) argues that effective information assurance mechanisms are only effective to the extent of which the user in question believes that the privacy assurance mechanisms are *accurate* and *reliable* in their information practices. The research revealed that effective privacy policy is linked to users' perceptions regarding their effectiveness of protecting their privacy. Similarly, other researchers have similar findings in that organizations privacy assurance mechanisms may lead to an increased trust and reduced non-self-disclosure behaviour amongst users (Chang et al., 2018; Shim, Johnson, and Jiang, 2006;

Mutimukwue, Kolowska, and Grönlund, 2020; Culnan and Armstrong, 1999; Culnan and Bies, 2003; Xu et al., 2011; Hui et al., 2007).

Based on the provided information, it will be hypothesized that:

H3: Perceived effectiveness of privacy policy increases trusting beliefs.

H4: Perceived effectiveness of privacy policy decreases non-self-disclosure behaviour.

H5: Perceived effectiveness of privacy policy reduces perceived privacy risks.

3.2.4. Organizational privacy assurances effect on trust, trusting behaviour and risk perceptions

As mentioned, Xu et al., (2011, 2012) goes about the subject of effective organizational privacy assurances through the eyes of the user by measuring it in accordance with users trust and non-self-disclosing behaviour. This behaviour or calculations of potential risks are essentially equated as a result of the organizations abilities to protect their users from any harm and fulfil their promises. As the users are considered the party with most decision-making power, organizations should conform their assurance mechanisms to fit with the expectations of their users (Xu et al., 2011, 2012; Mutimukwue, Kolowska, and Grönlund, 2020).

It should also be noted that this is a self-regulated activity conducted by users, there are no direct rules or laws helping in the process of equating ones' safety. Although it is a heavily discussed subject, regulations at this stage would put restrictions on organizations and their abilities to attend to the issues of privacy and risk perceptions of their users. Perhaps this is also the reason why many organizational assurance mechanisms work to give positive views and enforce positive beliefs about their personal data management. Effective ways of mitigating concerns of trust and not being in power or mitigating possible risk perceptions, - is still a

priority for organizations to maintain their reputation (Xu et al., 2011; Mutimukwue, Kolowska, and Grönlund, 2020; Culnan and Bies, 2003; Culnan and Armstrong, 1999; Graham, 1994).

Based on the provided information, it will be hypothesized that:

H6: Perceptions of effective organizational self-regulation increase trusting beliefs.

H7: Perceptions of effective organizational self-regulation mechanisms decrease non-self-disclosure behaviour.

H8: Perceptions of effective organizational self-regulation decrease perceptions of privacy risks.

3.2.5. Privacy risks on privacy concerns

It has been established that literature concerning privacy is often connected or linked to literature topics concerning risks. Perceived privacy risks or vulnerabilities as described antecedents to privacy and related to concerns according to Dinev and Hart (2004).

A result of the increased internet and social media use are the increasing possibilities or risks of becoming vulnerable or exploited in some way. Personal information may be misused or abused in some way that may make you feel vulnerable. Research shows that threats of having someone unauthorized access your personal information or if your personal information is misused, - concepts such as perceived risks and increased privacy concerns also become involved in the discussion. If an individual is in a situation where they have to agree to sharing personal information and there are perceived risks about it, it will directly influence your perceived privacy concerns as you make a decision (Dinev and Hart, 2004; Dinev and Hart, 2006; Xu et al., 2011; Malhotra, 2004; Solve, 2006; Mutimukwue, Kolowska, and Grönlund,

2020; Hong and Thong, 2013; Smith et al., 1996). Therefore, it will be hypothesized that:

H9: Perceptions of privacy risks raises privacy concerns.

3.3. The conceptual model

The following model is as mentioned built after Mutimukwe, Kolowska, and Grönlunda (2020) model. *Figure 1* is a visual representation of the seven constructs part of the model, consisting of three dependent variables, a partially mediating variable, and two independent variables, - all in the context of e-commerce and social media.

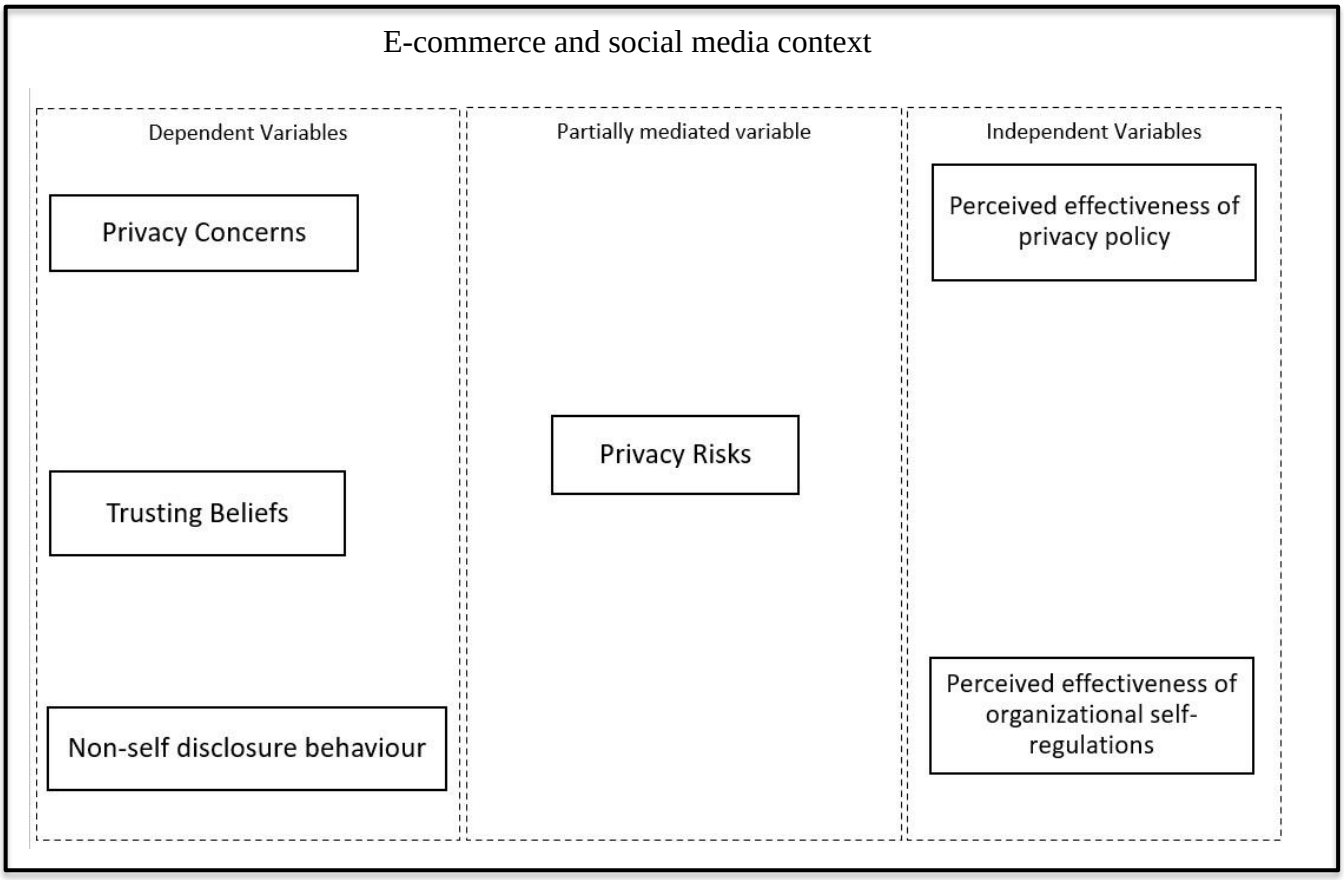


Figure 1. The conceptual model

Furthermore, *Figure 2* below is a visual representation of the variables part of the model, - but with focus on the hypotheses between each construct.

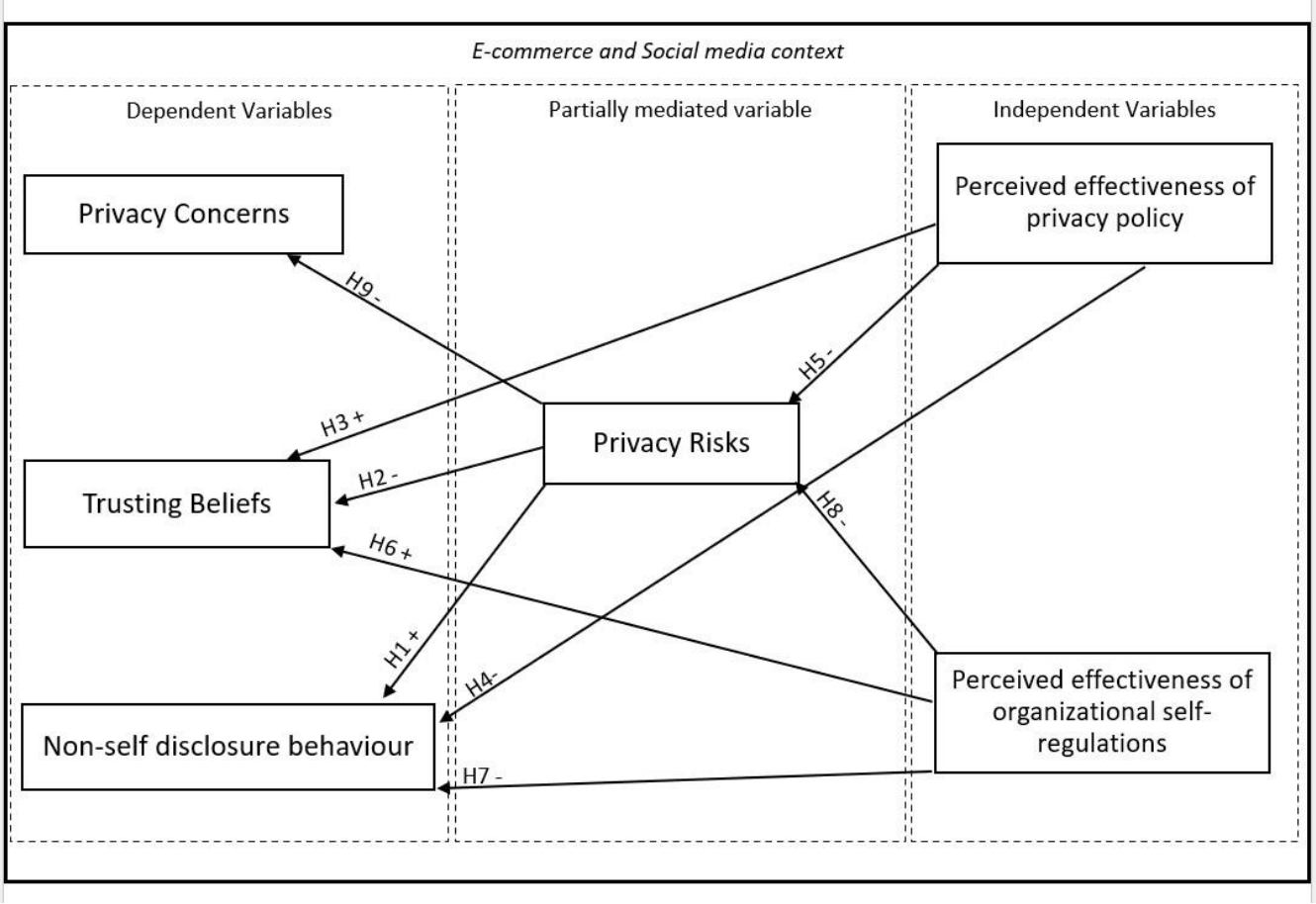


Figure 2. The conceptual model with hypotheses

By first analysing the relationships between risk perceptions and how they may affect users' trust, non-self-disclosure behaviour, and privacy concerns, - the model continues by analysing it in the context of organizational privacy assurance mechanisms and privacy policies. These perceptions, beliefs and attitudes amongst users' is not only examined in the realm or context of organizational privacy assurance mechanisms and privacy policies, - they are also examined to see the direct effects they may have on organizations. The examination of these relationships between both parties allows for *another* examination of the possibility of privacy concerns, non-self-disclosure behaviour, and trusting beliefs being *partially mediated* by perceptions of risk.

4. Methodology

The following chapter of this thesis presents how this research will be conducted throughout the entire research process, and why certain methods were chosen. A brief description of the chosen methods is depicted in Table 2 below.

Research strategy	Quantitative methods
	Deductive approach
Research design	Cross-sectional approach
Data Collection method	Primary data collection
	Self-completion questionnaire
Data analysis method	Multivariate analysis
	Linear regression
	Descriptive Statistics
Quality Criteria	Validity assessments
	Reliability assessments

Table 2. Summary of methods

4.1. Research Strategy

In order to identify effects out of outcomes and to analyse what influences the final outcomes, one may apply a quantitative research method. A quantitative research method may provide a structure where a multitude of ideas become a smaller set ready for testing, such as concepts or variables in hypotheses and research questions. A quantitative approach is often applied to research that aims to test the objective theory that examines the relationship or correlation between variables. By using tools, numbered data could be extracted to be analysed through different statistical features. Also, with having theory tested through different hypotheses, the collected data will ultimately reveal to support or reject the hypotheses. Thus, a quantitative research method will be used (Bryman and Bell, 2015).

Furthermore, according to Bryman and Bell (2015), there are two different strategies one can approach to explain the relationship between theory and reality in research, namely an inductive or a deductive strategy approach. An inductive research approach, which is often also referred to as inductive reasoning, is an approach that involves searching for patterns, from observations to arrive at explanations or theories in the form of hypotheses. Therefore, inductive reasoning is an approach that starts with specific observations to then arrive at more broad generalizations, contrary to deductive reasoning. Deductive reasoning starts off with the researcher having already established theory, to then develop hypotheses from that theory, to lastly commencing in collecting data that will be analysed to test the established hypotheses. In the proposed research, deductive reasoning will be applied as the development of hypotheses, as well as the use of different concepts, as this will be inspired by already existing theories or findings from established literature.

4.2. Research Design

The purpose of choosing a research design is to make sure the study is conducted in a manner that addresses the stated problem. The chosen research design explains how the data will be collected and how it will be analysed in order to draw conclusions to the stated research question (Iacobucci and Churchill, 2015).

Creswell and Creswell (2018) describe two different types of relevant research designs for quantitative studies, cross-sectional and longitudinal research designs. A cross-sectional design includes data from one or more cases, from a single point in time. By taking data from one or more cases into account one may be able to have a substantial amount of quantifiable data, which enables the researcher to look for potential relationships or patterns of association in the data.

A longitudinal design does not take various cases with various variables into account, but only the same set of variables which is studied over a set period of time. This method is often applied to research aiming to understand how a set subject evolves and changes over time in relation to something (Creswell and Creswell, 2018; Bryman and Bell, 2015; Bethlehem, 1999).

Depending on the nature of the stated research question, a research design may be applied in an exploratory, descriptive, or causal framework (or explanatory). A causal research framework supports research that studies cause and effect relationships, and much like the name causal research framework, it helps the researcher in the process of finding supporting evidence to causal relationships. Exploratory, or descriptive research frameworks support research that tests theories against data. In this case, theory is considered as the foundation for the methodology of choice and should be stated in a literature review before conducting any method of collecting data. The exploratory research is therefore dependent on having anticipations or hypotheses of possible significant relationships in the data beforehand, where an independent variable is believed to cause a change in a dependent variable for example (Iacobucci and Churchill, 2015; Saunders et al., 2009).

Both longitudinal and cross-sectional studies can take on these aforementioned research frameworks in order to draw conclusions and make generalizations from the targeted population. However, with this in mind one must consider the previously stated choices of conducting quantitative research with numeric descriptions of attitudes and trends, as well as the choices made regarding *how* the data will be collected, which in this case will be through an online survey. The stated research problem will take numerous dependent- and independent variables into account through the online survey, which will require a cross-sectional research design since multiple cases will be taken into account in order to gather a substantial amount of data. Furthermore Saunders et al., (2009) argues that the cross-sectional design is a favourable choice when conducting research through surveys since the variations in the data and variations between respondents can be more easily examined if the research design allows for more than one case to examine.

In addition to the cross-sectional research design, a causal framework will be applied to this thesis. As the stated research problem in this thesis requires multiple independent variables to be tested in relation to different dependent variables that collectively focus on detecting attitudes and behaviour, a causal framework is concluded to be the most appropriate framework. Along with the cross-sectional research design allowing this research to detect variations amongst respondents, the causal framework will continue along the same lines and support the process of detecting cause and effect relationships, i.e., explaining *why* respondents may feel a certain way.

4.3. Data sources

The collection of data may be conducted in two different ways, through primary or secondary data collection. When collecting primary data, one refers to the collection of empirical data that has been collected by the researcher alone. This type of data collection method often requires the researcher to conduct interviews or observations in order to gather primary data (Jacobsen, 2002). A secondary data collection method does not require the researcher to gather data alone, secondary data is data that already exists which the researcher may use to conduct a study (Patel and Davidson, 2003). As for this thesis, primary data will be collected in order to answer the research question which aims to measure attitudes or feelings of trust or invasiveness etc. By collecting primary data through a survey, one may be able to collect information about these attitudes and find correlations between certain consumer attitudes and behaviour for example, which will also require a big data sample along with item scales in order to make comparisons. By utilizing an online survey to collect primary data one may also be able to reach a larger population in a relatively short amount of time, which was also regarded as an important factor when choosing the data collection method. Furthermore, reaching out to potential respondents with an online survey (Facebook) may be fitting since the aim for this research is to collect answers from individuals who are active online. This may help ensure that the collected data represents the targeted sample population, which will help ensure that conclusions could be drawn from the analysed data in order to answer the research question (Jacobsen, 2002; Bryman and Bell, 2015).

4.4. Data collection method

Once primary data collection has been defined as the data source of choice, one must define through what means one is planning to collect primary data. This all depends on which data collection is viewed as most beneficial for the research at hand. It may be observations, experiments, interviews, or questionnaires that are deemed to be most appropriate for the stated research purpose and research problem. Research that takes on the quantitative approach is often focused on providing numerical facts to be analysed in a logical and critical manner, to categorize and generalize the targeted population, according to Ghauri and Grønhaug (2010). Furthermore, in quantitative research, observations or questionnaires are often chosen as a means of collecting data, according to Easterby-Smith et al., (2018).

By using a questionnaire as a data collection method, one may be able to collect data in a way that allows for standardization and comparison. However, this requires that the questions asked in the questionnaire are all constant or standardized. The questions asked in the questionnaire need to be representative of the chosen concepts one wishes to study to be able to generalize and correlations in the collected data. If done effectively, a questionnaire could be a data collection tool that assists the researcher in collecting data on attitudes and opinions from a relatively large pool of respondents. Perhaps this is also the reason why questionnaires have become increasingly popular in business related studies (Ghauri and Grønhaug ,2010; Easterby-Smith et al., 2018; Malhotra, 2010).

Based on the aforementioned information, a questionnaire will be the data collection method of choice for this thesis. By applying this data collection method in a structured and standardized manner, one may be able to retrieve information from the target population and generalize and comparisons in turn. However, there are different structures that may be applied to the questionnaire as a data collection tool.

A questionnaire could be highly structured in the way the questions are formulated. A structured questionnaire often has predetermined answers to the questions that gives the respondents a different set of answers to choose from. A more unstructured

questionnaire often contains more open questions that allows the respondents to write in their own words. Furthermore, the questionnaire could be disguised or exposed to respondents, meaning that the purpose of the study could be explained at large to all participants, or disguised so that all participants do not know the purpose behind the asked questions. Structured questionnaires that are disguised have become increasingly popular in business research according to Iacobucci & Churchill (2015) since it may help minimize potential risks of having misunderstandings amongst respondents while also minimizing the risks of not being able to compare the results. It is not only considered a data collection method that could help minimize confusion amongst respondents-, but a method that could allow the researcher to handle and analyse the data easier. By having a structured, disguised questionnaire with predetermined options as answers to each question, researchers may also be able to collect larger amounts of data over a relatively short period of time. Therefore, a structured, disguised questionnaire is the data collection method of choice for this thesis.

4.5. Data Collection instrument

Questionnaires are often sent out to respondents through postal mail, or online if the questionnaire is web-based. Postal questionnaires are considered to be a low-cost method of collecting data and it is also a method that could help researchers reach a lot of respondents due to not having face to face contact with respondents. Albeit one may reach out to a lot of respondents, the actual response rate of postal questionnaires is often considered to be about 20 percent according to Easterby-Smith et al., (2018). Today, web-based questionnaires are becoming increasingly popular due to the fact that increasing amounts of the population is active online to some extent. Web-based questionnaires allow the researcher to reach potential respondents through email, or through social media. This is not only considered to be convenient in today's society, - but it is also considered to be cost effective. By utilizing online tools such as Google Forms, respondents are able to reach the questionnaire through a link to then get help from certain pop-up instructions that guides the participant through the survey with functions such as error checking

which checks that the respondent fills in all questions. This is not only considered to be a tool that helps respondents fill out the questionnaire, but a tool that helps researchers form structured questionnaires, ensuring that all participants go through all stages and all questions. It is also a tool that simplifies the process of exporting the collected data to other programmes such as Microsoft Excel or SPSS. However, a possible downside to online questionnaires is that all respondents need to have access to the internet, but since the purpose of this research is to measure attitudes and opinions about different e-services, this 'issue' is only considered to be beneficial in the process of finding the targeted population sample (Easterby-Smith et al., 2018).

Not only is Google Forms a tool that simplifies the process for both respondents and the researcher, - but it is also a free questionnaire tool that could be designed to be answered through a web browser on the computer, or through a phone. Google Forms also summarizes the answers in different formats through graphs and charts so that the researchers could be updated with a summary of all respondents' answers in real time (Google, n.d).

Based on the aforementioned benefits of using web-based questionnaires through Google Forms, Google Forms will be the only tool used to create and distribute the questionnaire. In addition, this tool may help in the process of making a more personalized questionnaire design, as well as help me conduct a disguised, structured questionnaire where respondents are 'forced' to fill in any missing answers in order to hand in the finished questionnaire.

4.5.1. Questionnaire design

The online questionnaire starts off with an introduction that welcomes each respondent with a small section that explains the overall purpose of the research. It also informs each respondent that they will remain anonymous, which is part of the ethical considerations applied to this research (*see 4.10 ethical considerations*). As the questionnaire is self-administered an introduction may help increase the response

rates as well as minimize confusion throughout the questionnaire. Therefore, respondents will go through different sections (some of which have examples of real privacy assurance mechanisms) with short instructions of how to fill out each question, starting with a set of control questions asking participants to fill out their age, gender, income and occupation as well as where they are from. These answers are designed to be fixed with a set of different options to choose from that fits the respondents best (Saunders et al., 2009).

In order to have a good response rate certain techniques may be applied. For example, in the process of reaching out to potential respondents with the link to the questionnaire one may explain that the survey will only take a few minutes to fill in, in order to not 'scare' potential participants away. Furthermore, it is argued that a well thought out design with an attractive layout may increase the response rate (Dillman, 1983 cited in Bryman and Bell, 2015).

4.5.2. Measurements

As mentioned, designing the questionnaire is an important factor in attracting potential respondents to partake in the study. To help ensure this one may include instructions or information to the questionnaire, such as short statements such as: *"Kindly answer to what extent you agree with the following statements, ranging from 1 (strongly disagree) to 7 (strongly agree)".* Having a scale to measure each question, i.e., a Likert scale will help in the process of receiving consistent answers to that may be standardized and comparable at a later stage in the process of reviewing the collected data. Having closed questions with options using a Likert scale will also help ensure that there is little room for participants to elaborate on answers. The Likert scale is also a tool that may help ensure the choice of having a structured questionnaire. Furthermore, the pre-coded results may help the process of converting and processing the data with more ease (Bryman and Bell, 2015). However, there were also options for the respondents to write freely after each section if they wanted to, it was not mandatory.

The whole questionnaire with all introductions can be found in the appendix.

Table 3. Likert Scale

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	*Neutral*	Somewhat Agree	Agree	Strongly Agree

4.5.3. Operationalization

The operationalization table with all concepts, items and authors to the measurements can be found in *Appendix A (10.1).*

4.6. Population and sampling method

To be able to carry out this scientific research, a nonprobability sampling method was applied. All persons in the population did therefore not have the same chances of being asked to participate in the study. Conversely, it could also mean that the targeted individuals asked to participate do not possess the true characteristics, thoughts, and attitudes of said population. However, as there were no requirements about selecting participants, and time and finances to carry out the study was almost non-existent, - the nonprobability sampling technique was still deemed to be fitting. Although it should still be noted that it may be limiting to this research in terms of not being able to generalize results due to lack of representation. Therefore, this issue is also discussed in the limitations chapter (Bryman and Bell, 2015; Aaker et al., 2011).

To further specify how this research was conducted, it should also be noted that a convenience sampling method was used. All participants were chosen based on their availability and level of convenience at that time. This could also be a possible limitation to this research as it concurs with the method of not picking participants

with time and care. Therefore, the limitations of using a convenience sampling method will be discussed in the limitations chapter as well (Bryman and Bell, 2015; Aaker et al., 2011).

As the foundation of this research and the formulation of the stated research problem is based on existing research, a snowball sampling method was also used. As mentioned, a key piece of research by Mutimukwue, Kolowska, and Grönlund (2020) was used as a basis of inspiration in the process of formulating the stated research problem. Not only did the research by Mutimukwue, Kolowska, and Grönlund (2020) play a vital role in reading up on the research topic, - it also allowed this research to snowball into other studies which helped build the theoretical foundation of this research (Bryman and Bell, 2015; Aaker et al., 2011).

4.7. Pre-testing

Before the questionnaire was distributed it was sent to three different people to conduct a pre-test. Along with sending the pre-test, each person was asked to provide feedback so that the questionnaire could become as understandable and clear as possible to comply with the ethical considerations of this thesis (*see 4.10*). A pre-test is also often applied to quantitative research to prevent confusion and to avoid errors in the data (Bryman and Bell, 2015). Therefore, the pre-testing was also conducted to make sure that the selected research items measure the intended research concepts and that they were accurate.

4.8. Data analysis method

It is not only questions of how the data will be collected that is of importance, but one must also consider how one should analyse the collected data. Data analysis could for example take one variable into account, which makes it a univariate analysis, whereas analysing two variables is called a bivariate analysis. Taking three or more variables into account is considered as a multivariate analysis (Bryman and Bell, 2015).

When choosing how to handle the collected data one must still have the stated research problem in mind, while also considering the nature of the collected data. The nature of this research issue requires multiple independent- and dependent variables to be analysed and put against each other. Therefore, a multivariate analysis is deemed most useful. To be able to carry out the multivariate analysis the data will be measured through a correlation and regression analysis. This choice of data analysis method will also help in the process of establishing if relationships in the data could be found or not, and if the relationships bear any significance (Bryman and Bell, 2015).

A more in-depth explanation of the chosen data analysis methods will be provided in the coming subchapters.

4.8.1. Cleaning the data

Once the data has been assembled and gathered through Google Forms, it is entered into an analytical statistics software program called SPSS. The data, containing both questions and answers, will then appear in code, where different answers and different questions will be named a number or piece of code. This type of software will not only provide tools to analyse the data but help assist in the process of looking through the data to see if there are any missing values and if there are any irregularities or inconsistencies that are out of range (Malhotra, 2010).

Control variables, namely questions concerning age or gender were handled a bit differently in SPSS in order to include them in the regression analysis. Each nominal variable was changed from string values to specific numeric values. Not only did this provide a more rigid basis of testing these types of variables against each other, but it also assisted in the process of understanding the distribution of the sample (Bryman and Bell, 2015; Malhotra, 2010).

In total there were 100 surveys with complete answers.

4.8.2. Descriptive statistics

Now onto a more in-depth description of the statistics and how the data was handled. Measures relating to the distribution of the data, i.e., the central tendency of the data was applied to the data in order to measure the mean, median and mode. Not only was the distribution of the data of importance, but also the amount of variation in the data. Through the use of standard deviation measurements, one could detect the variations in the data and how it was cantered in relation to the mean value. This was done through calculating the difference between values in the distribution along with the mean, to then divide the total difference by including all values (Bryman and Bell, 2015).

4.8.3. Central tendency and dispersion

To further the explanation of descriptive statistics, the dispersion and central tendency of the data should be addressed. The calculation of the central tendency in the data coincides with the aforementioned method of defining the mean, median and mode in the dataset to again describe the statistics (Malhotra, 2010; Saunders, Lewis, and Thornhill, 2016).

The dispersion of the statistics refers to how the data is dispersed or spread. In order to look at how the data is spread, the aforementioned standard deviation is used, along with all items and scales in the data (Cook and Weisberg, 1982).

The calculated central tendency and dispersion in the data can be found in the analysis and results section.

4.8.4. Skewness and kurtosis measures

To further understand the distribution of the collected data, one may utilize the statistical calculations of the kurtosis values and the skewed distribution. The skewness of the data is determined by the extent to which each value deviates from the mean. This is determined by examining the normal distribution curve and weather the curve leans positively or negatively in one direction. Negative values are shown to lean to the left and have a curve with a long ‘tail’ to the right, while

positive values should be more equally distributed and more symmetrical. To specify even further, this could be determined by looking at the exact skewness measures, which should be within the range of 1 in order to be determined as acceptable (Saunders, Lewis, and Thornhill, 2016; Malhotra, 2010; Hair et al., 2013).

Kurtosis measures relate to the distribution of the data, and it gives the opportunity to examine the flatness and peaks of the curves. Again, this could be determined by exact measures in a range where the value 1 is considered the strongest measure. Values that are -1 or even -2 or 2 are still considered quite acceptable according to George and Mallery (2003). All negative values point to having a flatter curve, while all positive values point to having a curve with a more prominent peak. A normal distribution curve will show to have a kurtosis value of 0 (Malhotra, 2010).

4.8.5. Regression and correlation analysis

Not only is it of importance to determine how the data is distributed to know if values are acceptable or not. It is equally important to determine the strength of each value to know if there could be any association between variables. This is where a correlation analysis will be of use. The correlation analysis is not only assisting in the process of determining relationships between the variables, but it also assists in the process of determining the strength of each variable, through the measure 'r' which may range from -1 to 1. Both values are clear in showing accepted and rejected correlations in the data, where 1 reflects a positive relationship, and -1 reflects a negative relationship. If the 'r' value shows to be 0, there is no relationship to be found between the variables (Malhotra, 2010). However, Pallant (2010) and Cohen (1988) do argue that 'r' values that are close to 1 and -1 should also be deemed as acceptable values, whereas values closer to 0 or values that are lower than 0,5 should be considered as weak correlations and should be treated as such.

To further the understanding of the level of correlations found between variables, the 'p-value' should be taken into account. The p-value furthers the basis of understanding of the values and their relationships with each other. A p-value of

significance where a hypothesis could be accepted is usually a value where $p<0,05$. However, a p-value of $p<0,01$ or $p<0,001$ could also be considered as values with significance. Negative p-values such as $p>0,05$ is an example of a value that lacks statistical significance, and should therefore be rejected (Pallant, 2010).

As a multivariate analysis is used, a regression analysis is what may help in the process of determining relationships between multiple variables, specifically one dependent variable and one or more independent variables. The regression analysis determines the degree relation of each relationship that is chosen to be measured (Malhotra, 2010). However, there are multiple different methods to conducting a regression analysis and as multiple variables need to be taken into account in this research, a multiple linear regression analysis is deemed most fitting. A multiple linear regression takes multiple variables into the analysis, and it results in modelling a linear association between the analysed variables. In the form of a graph, containing a 'x' and 'y' axis, the data will in the best-case scenario be portrayed in a straight line. If there are deviations in the data, one may more easily detect those as they will appear outside the straight line and appear as outliers (Cook and Weisberg, 1982; Saunders, Lewis, and Thornhill, 2016).

Not only will the multiple linear regression appear in a model, but it will also appear as a statistical metric called R^2 which helps determine the variation in the outcome of each correlation. R^2 can range from 0 to 1 and it is a measure that may explain the variance in each variable, related to the variance in the other variable. An R^2 measure that is higher than 0,5 is for example showing that half of the variance between the variables are explained by the model, but if the measurements are close to 10 % the model is deemed valid (Falk and Miller, 1992; Saunders, Lewis, and Thornhill, 2016; Pallant, 2010).

One can also make use of the measure called 'adjusted R^2', which allows you to exclude certain independent variables that have no explanatory power towards the dependent variable in question. The adjusted R^2 measure essentially provides a more in depth explanation in case the usual R^2 measure overestimates certain

variables depending on the sample size (Hair et al., 2013; Pallant, 2010; Tabachnick and Fidell, 1996).

To ‘test’ the data even further, a standardized regression coefficient is utilized. This coefficient examines the level of increase or increase in standard deviations that appear in a variable when the independent variables are increased by a single standard deviation. When applying this regression coefficient, all other variables are held constant and if applied correctly it may help find what independent variables possess the largest or smallest effect on the selected dependent variable (Cook and Weisberg, 1982; Pedhazue, 1997). With that said, it is not easy to perfect this measure with utmost accuracy due to the fact that the projected results may not coincide with each single data point. It is rather difficult to take note of these small variations in the data, which is why another measurement called ‘E’ will be applied to the data analysis. This measure takes predictions and actual outcomes into account, which may assist in the process of determining if a hypothesis could be rejected or accepted (Malhotra, 2010).

4.9. Quality criteria

To ensure that the collected data is of certain quality, different quality measures will be applied to the data. Measures concerning validity of the data makes sure that what is said to be measured is measured. For example, ‘construct validity’ measures could be applied, which helps ensure that the theoretical basis of a concept coincides with the actual measure (Bryman and Bell, 2015).

Reliability measures, which are used to ensure the consistency and reliability of all measurements will also be applied to the collected data. The stability of the data will be considered, which measures if the data is stable over time and that the collected sample of respondents do not fluctuate, but stay true to the chosen, targeted sample. One may also delve deeper and measure the internal reliability of the data, which measures each answer put in by respondents, and collects them to create an overall score to see if there is a lack of coherence between different indicators (Bryman and Bell, 2015).

4.9.1. Pearson's correlation coefficient

Continuing on the subject of construct validity, Pearson's correlation coefficient will be added as a step in the data analysis. This measure is often used to examine relationships in a manner that takes intervals and ratio variables into account. The Pearson correlation coefficient should appear as a value between 0 (no relationship detected), or 1 (strong relationship detected), (Bryman and Bell, 2015).

4.9.2. Cronbach's alpha

A reliability measure that will be used in the analysis of the collected data is Cronbach's alpha. It measures the internal reliability, which examines whether the collected answers from one observation are related in some way, and if so to what degree. Here, a value that is around 0,7 or 0,8 or higher is reliable according to Bryman and Bell (2015) and Pallant (2010). However, it should be noted that this measure is quite sensitive and that it may not take the entire variance of the dataset into account. Therefore, the composite reliability of the dataset will be analysed. This measure is often around 0,6 or 0,7 in order to be deemed acceptable and it takes the entire variance into account (Sub, 2005; Nully and Bernstein, 1994; Brunner and Sub, 2005)

4.10. Ethical considerations

Ethics in research is an important subject, especially in the context of how the data was collected and with what means it was collected, all collected sources should be considered as 'proper' in order to make use of it in full. When conducting scientific research, one must go to certain measures in order to ensure that the entire research process follows a certain moral standard. For example, one should not try to go against participants' ethical beliefs or morals (Ghauri and Gronhaug, 2005).

In an effort of trying to comply with these ethical and moral considerations, all participants of this study were treated anonymously, with no names, no personal email, and no address. All participants would essentially not be identifiable in any way. Not only were these ethical considerations applied to the data collection method with the participants personal ethics and morals in mind, - but being treated

anonymously could also assist the participants in answering freely and more truthfully, which would increase the reliability of the study (Jacobsen, 2002).

Generally, ethical considerations in scientific business research consist of a set of principles: one should not harm participants, all participants should be informed before they consent to participate, and possibilities of invading on privacy and possible deception should be considered by the researcher. Not only is it important that the researcher acknowledges these principles when conducting ethical research, it should also be specified and clarified to the participants. It should be communicated that the researcher is held responsible for any possibility of inflicting any harm on participants. All contact with participants were therefore informed about their participation in the study, how the study was formed and for what purpose (Bryman and Bell, 2015).

Moving on from ethical issues relating to informed consent, ethical issues of invasion of privacy should also be considered a principle one should follow when conducting scientific research. This (again) coincides with the duty of the researcher to not pursue any form of investigation that may infringe on sensitivities such as personal individual values. Not only would this inflict harm on the participant in question, but it would also reflect negatively on the researcher and the trusted community between respondents and researchers (Bryman and Bell, 2015). Therefore, transparency was a priority during the entire research process, and perhaps even more so in situations where participants were included in the process. Letting participants in on the entire context and purpose of the study, to allow them to make a fully informed decision on whether they wanted to participate in the study or not. There was also a possibility of exiting the survey at any time and discontinuing the survey altogether if wanted.

It should however be noted that the survey was distributed into Facebook communities with other students and researchers that most probably already have experiences of participating in studies. However, all participants were given the

same information before participating and if they were unsure of anything about the study itself or portions in the survey, they could reach me via email.

Not only were the control questions in the survey designed in a manner that would protect each participant's identity, - each statement made in the survey was also made quite general in order to protect the participants identity. For example, there were no statements or questions included in the survey that would reveal who did or did not choose to actively participate in certain social media or e-commerce sites. Instead, general examples and scenarios were utilized to protect each participant's identity.

5. Analysis and results

The following chapter will present the results from the conducted study, as well as presenting the analysis and conclusions of the results.

5.1. Analysis of questionnaire results

There were in total 100 respondents participating in this study (N= 100). As explained, the questionnaire started off with a set of control questions which asked about the participants ages, gender identification, their occupation, and their country of residence. These questions concerning demographics showed that most of the respondents are Swedish and that most of the respondents are female. The parts of the questionnaire where the respondents could write freely is not entered into SPSS as these thoughts and opinions will only be discussed in relation to the analysed results (see the *appendix* for the entire questionnaire and *8.3 recommendations,* to see commentary on these answers).

The results of the control questions also showed that 36 % of the respondents are in the ages between 25 to 34 years old and that 48 % of the respondents are in the ages between 15 to 24 years old. With most of the respondents being in their early twenties to early thirties, the results also showed that most respondents were either employed or students, with 50 % of the respondents being students and 40 % of the respondents being employed.

The remaining questions part of the questionnaire were as mentioned all written as statements where each respondent had the Likert scale to answer from. There were no more control questions part of the survey, hence all 100 completed answers were used and included in the analysis.

All answers were converted to fit into the software program SPSS to clean the data, code the data, and lastly analyse the data. All control questions could also be found in the table below.

Table 5. Demographics

Demographic Question	**Category**	**(%) Answers**
Gender	Male	14 %
	Female	82 %
	Non-binary	3 %
	Prefer not to say	1 %
Age	Younger than 15 years	2 %
	15-24 years	48 %
	25-34 years	36 %
	35-44 years	7 %
	45-54 years	4 %
	55 years or older	3 %
Occupation	Student	50 %
	Employed	40 %
	Unemployed	3 %
	Retired	4 %
	Other	3 %
Country	Sweden	95 %
	Portugal	1 %
	Hungary	1 %
	Philippines	1 %
	USA	1 %
	Japan	1 %

5.2. Descriptive statistics

Along with reviewing the demographic control questions, each independent- and dependent variable will also be examined to be able to describe the collected data. Therefore, the descriptive statistics can be displayed in *table 6* below. The table shows all independent and dependent variables through their assigned item names.

As a Likert scale was used as a tool to answer all statements, the table is categorised according to measures that will reveal the central tendencies in the data. Therefore, the table depicts the data according to the mean, median, and mode as well as the total summary.

Apart from the central tendency related measures, the descriptive statistics also depict the standard deviations of each measure. To further describe the data there are also measures showing the skewness and the kurtosis of the data and each item. Based on the suggestions from Hair et al., (2010), the skewness of the data should fall in the range of ±1, while the kurtosis measures should fall in the ranges between about -1 to about 2. Based on these suggestions, the analysed dataset showed to have a rather high kurtosis measure for the item PC1 of 2,770. This kurtosis measure shows that the distribution curve for the item is high and that it has a strong, high peak. Along with the skewness measures being close to zero for this item, one may further ensure that there is a strong peak in this distribution curve.

See table *Table 6. Descriptive statistics* below.

Measure:	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Privacy Concern 1	1	7	5,09	1,111	-,903	,241	2,770	,478
Privacy Concern 2	1	7	5,47	1,114	-,527	,241	1,433	,478
Privacy Concern 3	1	7	5,41	1,280	-,872	,241	1,095	,478
Perceived Privacy Concern 1	1	7	2,97	1,410	,980	,241	,650	,478
Perceived Privacy Concern 2	1	7	2,80	1,333	,845	,241	,918	,478
Perceived Privacy Concern 3	1	7	3,26	1,508	,590	,241	,157	,478
Perceived Privacy Risk 1	1	7	4,81	1,315	-,792	,243	1,101	,481
Perceived Privacy Risk 2	1	7	5,33	1,129	-,856	,241	3,065	,478
Perceived Privacy Risk 3	1	7	4,92	1,376	-,685	,241	,627	,478
Perceived effectiveness of privacy policy 1	1	6	3,59	1,248	,188	,241	-,549	,478
Perceived effectiveness of privacy policy 2	1	7	3,56	1,305	,534	,241	-,256	,478
Perceived effectiveness of privacy policy 3	1	6	3,31	1,447	,255	,241	-,620	,478
Perceived effectiveness of organizational self-regulation 1	1	7	3,89	1,377	,509	,241	-,003	,478
Perceived effectiveness of organizational self-regulation 2	1	7	3,59	1,747	,502	,241	-,917	,478
Trusting beliefs 1	1	6	3,12	1,266	,380	,241	,080	,478
Trusting beliefs 2	1	7	3,20	1,371	,615	,241	,222	,478
Trusting beliefs 3	1	7	3,03	1,480	,462	,241	-,047	,478
Trusting beliefs 4	1	7	3,34	1,350	,411	,241	-,056	,478
Trusting beliefs 5	1	6	3,02	1,295	,390	,241	-,057	,478
Non-self-disclosure behaviour 1	1	7	2,71	1,373	,828	,241	,910	,478
Non-self-disclosure behaviour 2	1	7	2,83	1,415	,810	,241	,685	,478
Non-self-disclosure behaviour 3	1	7	2,77	1,728	,891	,241	-,214	,478

N= 100

5.3. Quality criteria

As mentioned, questions concerning validity were considered and utilized from the beginning till the end of this research process. By conducting pre-testing before publishing the questionnaire to the targeted sample audience, as well as utilizing established research and research models as a foundation, - validity constructs were utilized. A more in-depth description of all validity constructs used can be found in the methodology chapter called *4.8 Quality Criteria*.

5.3.1 Construct Validity

To further ensure the quality of the collected data is up to standards, the correlation coefficients for the variables has been measured and put in a table. The table shows the correlations found in the data as well as the strength or significance of each variable to ensure that the results are valid.

The table shows the Pearson's correlation coefficient, which tests if there are any relationships or associations between the variables. The analysis depicted in the table below shows that there is a positive association between trusting beliefs and perceived effectiveness of organizational self-regulations and that the association between them is significant (Pearson correlation between variables: ,464***). On the other hand, the results of the correlation test also shows that there is a significant, negative association between perceived privacy risks and perceived effectiveness of privacy policy (-,226*). A more in-depth description on the correlations found in the data can be found in the discussions chapter.

Table 7. Pearson's correlation coefficient (see page below).

Pearson's Correlation Coefficient		privacy concern	perceived privacy concern	perceived privacy risk	perceived effectiveness of privacy policy	perceived effectiveness of organizational self-regulations	trusting beliefs	nonself disclosure behaviour
privacy concern	Pearson Correlation	1	-,097	,543**	-,106	,217*	-,187	,385**
	Sig. (2-tailed)		,335	<,001	,295	,030	,063	<,001
	N	100	100	100	100	100	100	100
perceived privacy concern	Pearson Correlation	-,097	1	,014	,573**	,297**	,655**	,113
	Sig. (2-tailed)	,335		,888	<,001	,003	<,001	,262
	N	100	100	100	100	100	100	100
perceived privacy risk	Pearson Correlation	,543**	,014	1	-,226*	,027	-,176	,261**
	Sig. (2-tailed)	<,001	,888		,024	,791	,080	,009
	N	100	100	100	100	100	100	100
perceived effectiveness of privacy policy	Pearson Correlation	-,106	,573**	-,226*	1	,562**	,756**	-,027
	Sig. (2-tailed)	,295	<,001	,024		<,001	<,001	,787
	N	100	100	100	100	100	100	100
perceived effectiveness of organizational self-regulations	Pearson Correlation	,217*	,297**	,027	,562**	1	,464**	,239*
	Sig. (2-tailed)	,030	,003	,791	<,001		<,001	,017
	N	100	100	100	100	100	100	100
trusting beliefs	Pearson Correlation	-,187	,655**	-,176	,756**	,464**	1	,080
	Sig. (2-tailed)	,063	<,001	,080	<,001	<,001		,429

2

	N	100	100	100	100	100	100	100
nonself disclosure behaviour	Pearson Correlation	,385**	,113	,261**	-,027	,239*	,080	1
	Sig. (2-tailed)	<,001	,262	,009	,787	,017	,429	
	N	100	100	100	100	100	100	100
**. Correlation is significant at the 0.01 level (2-tailed).								
*. Correlation is significant at the 0.05 level (2-tailed).								

5.3.2 Reliability constructs

To assure that the collected data was reliable, it was analysed through the Cronbach's Alpha reliability test. This tested whether the data is consistent with each item and whether each item accurately reflects each variable that is set to be measured. Therefore, the Cronbach's Alpha test was applied to all variables part of this study. The following table depicts the reliability in this study. The lowest reliability was found in the variable measuring perceived effectiveness of organizational privacy assurances with a measure of 0,566. The overall reliability results show to not be reliable according to Bryman and Bell (2015) since measures closer to 0,70 is deemed acceptable. However, as mentioned in the methodology chapter, Cronbach's alpha is considered a sensitive number. This measure has failed to measure internal consistency and reliability in the past, which is why one could measure the composite reliability. Composite reliability measures tend to be around 0,6 up to 0,7 to be acceptable and this measure is often described as a measure that takes the total variance into account. If the entire variance of each concept and each of the seven item scales are considered the presented measure is deemed acceptable (Brunner and Sub, 2005; Nully and Bernstein, 1994).

Table 8. Cronbach's Alpha across all variables

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,662	,648	7

2

5.3.3 Regressions and correlations

Once the overall statistics were described, the research model was put through data analysis, containing all variables. Each dependent- and independent variable was analysed together.

Starting off, a more general analysis with the independent variables was conducted to separate all results and analyse them separately before determining any regression results. Then, with one dependent variable at a time, a regression analysis was performed to be able to see if the hypothesis in question is rejected or not.

A visual depiction of each hypothesis and its significance measures can be found in the table below (*table 9. Hypothesis testing)*.

5.4 Hypothesis Testing

In order to generate findings, one need to analyse each hypothesis part of this study. As mentioned, a correlation or regression analysis is what is needed to produce answers to the proposed hypotheses. Each hypothesis will produce different regression results. However, it should be noted that each hypothesis is treated alone in the process to accurately analyse each concept to answer the posed research issue.

To explain this further, all regressions will be depicted in a table where all control variables are considered for each hypothesis as well as the set concepts that are connected to the hypothesis. Once all control variables and concepts are part of the regression model, one will be able to analyse the F-value or significance of each hypothesis and ultimately be able to accept or reject the hypothesis. If the regression model shows to have a level of 0,05 significance, the hypothesis will be accepted. To showcase this further, all significant and acceptable measures will be marked with the following symbol: *. In the case of having higher significance levels such as F-values as 0,01 or 0,001, it will instead be marked with ‘**’ or ‘***’, and so on, - meaning that the chance of the value being insignificant or rejected is less than a thousand.

Apart from measuring the F-values, the P-value will also be utilized to analyse each hypothesis and its level of significance. Unlike the F-value, the P-value will analyse each internal variable and its significance, which will help enforce each variables significance in the regression model.

Table 9 below depicts all regression analyses for each hypothesis with their significance values (significance and F-values), as well as measures explaining the variance of the model (R^2 and Adjusted R^2). The standard error estimates are part of the model to assess the precision of the model while the degree of freedom measure helps assesses the validity of the null hypothesis (Bryman and Bell, 2015).

Table 9. Hypothesis testing.

H1+		H2-	H3+	H4-	H5-	H6+	**H7-**	**H8-**	H9+
Significance	,009** (0,261)	,004*** (-0,176)	<,001** (0,756)	<,001*** (-0,27)	<,001***** (-0,226)	<,001** (0,464)	**<,001*** (0,297)**	**<,001*** (0,27)**	<,001** (0,543)
F – value	7,185	5,833	130,326	66,576	35,496	28,874	**16,714**	**8,370**	41,064
R^2	0,68	0,107	0,571	0,579	0,599	0,215	**0,256**	**0,261**	0,295
Adjusted R^2	0,59	0,089	0,566	0,570	0,582	0,207	**0,241**	**0,229**	0,288
Standard-Error Estimate	1,00052	,98436	,78702	,78389	,77251	1,25040	**1,22349**	**1,23273**	,87015
DF	1	2	1	2	4	1	**2**	**4**	1

N=100

The hypotheses that are in bold signify that they are rejected under the null hypothesis.

5.4.1 Accepted hypotheses and model

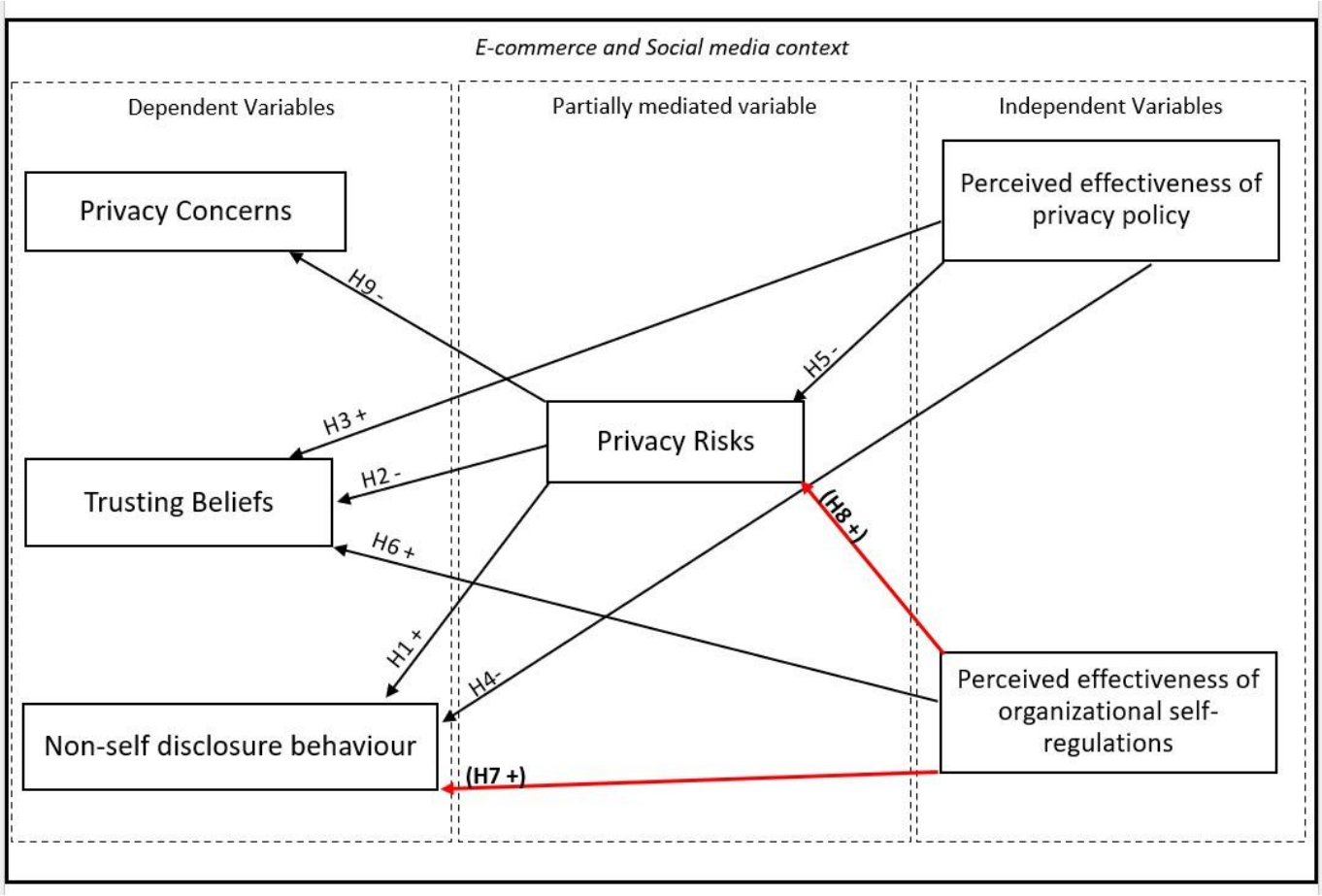
The following table depicts all accepted hypotheses and the rejected hypotheses.

Table 10. Accepted and rejected hypotheses

H1 Perceived privacy risks positively correlates with non-self-disclosure behaviour.	Accepted
H2 Privacy risks negatively affect one's trusting beliefs.	Accepted
H3 Perceived effectiveness of privacy policy increases trusting beliefs.	Accepted
H4 Perceived effectiveness of privacy policy decreases non-self-disclosure behaviour.	Accepted
H5 Perceived effectiveness of privacy policy decreases perceived privacy risks.	Accepted
H6 Perceptions of effective organizational self-regulation increase trusting beliefs.	Accepted
H9 Perceptions of privacy risks raises privacy concerns.	Accepted
H7 Perceptions of effective organizational self-regulation decreases non-self-disclosure behaviour.	Rejected
H8 Perceptions of effective organizational privacy assurance mechanisms decrease perceptions of privacy risks.	Rejected

As the results in *table 10* revealed that not all hypotheses part of the research model is supported by the null hypothesis, - the research model should be adjusted accordingly. A visual depiction of the accepted hypotheses is in *figure 2* below. This figure shows that the rejected hypotheses H7 and H8 are marked with red arrows and they have also gone from negative to positive values which have been marked with paratheses in bold.

Figure 3. The accepted hypotheses.



5.5 Statistics summary

The purpose of this thesis was to utilize a model that examined how organizational privacy self-regulations or different privacy assurance mechanisms effect users' trusting beliefs, perceptions, privacy concerns, and non-self-disclosure behaviour. As mentioned in table 5. Demographics, - a large percentage of the sample population were female students in the age groups of 20 and 30 years old. Therefore, it needs to be noted that the data may not be generalizable enough to draw a conclusion from a whole population. As a non-probability sample was applied to collect data, this skewness in the collected data was not intentional. Therefore, it is not only considered an implication but also a possibility for future researchers to measure possible

differences in results depending on the control questions concerning age, gender, and occupation (discussed at length in *chapter 8*).

The linear regression analysis also showed that the R^2 score for all hypotheses exceeded the 10 percent validation "rule". Therefore, all hypothesis measures were accepted under the basis presented in the methodology chapter by Saunders, Lewis, and Thornhill (2016), Pallant, (2010), and Falk and Miller (1992).

Apart from the mentioned limitations of the collected data to the research model, two out of nine hypotheses were rejected. The remaining accepted findings that support the model will now be discussed at length.

6. Discussion

The following chapter will discuss the presented results and provide a more in-depth explanation to the data statistics. This discussion will be based on the provided theory.

6.1. Discussion on findings

The results point to users' often being aware of the potential risks that comes with browsing social media or e-commerce sites. As different privacy assurance mechanisms pop-up on the screen, the user is instantly faced with the decision of choosing to disclose their data or not, and so privacy concerns may be raised. If the user in question happens to be risk averse, more thought might be put into the decision-making process before proceeding. In some cases, users have shown to disclose false information as a way of avoiding the potential risks (Mutimukwue, Kolowska, and Grönlund, 2020; Abri et al., 2009; Xu et al., 2011). The first hypothesis in this research analysed the probability of having a positive relationship between perceived privacy risks and non-self-disclosure behaviour. As the results suggests that this hypothesis is accepted, - the results suggest that social media and e-commerce users are aware of the potential risks of agreeing to the conditions of trading personal data, and that they may stop proceeding with this trade if they become more risk averse.

The theory also describes that those perceptions of risk are often equated together with feelings of trust. Trusting beliefs can be negatively affected in situations where perceptions of risk are heightened, which is why privacy risks showed to have a negative effect on trusting beliefs in the results (Dinev and Hart, 2004; Mutimukwue, Kolowska, and Grönlund, 2020; Dinev and Hart, 2006; Malhotra, 2004; Liu Marchewka and Lu 2005; Yu, 2005).

2

6.1.1. Discussion of organizational assurances

To answer to the research issue, one must consider the other party in the transaction, namely the social-media or e-commerce organization. More specifically, one needs to consider the different privacy assurance mechanisms they place on their sites and social media. Xu et al., (2011) and Mutimukwue, Kolowska, and Grönlund (2020) describe that organizations make efforts to bring the users different privacy self-regulation assurances to better deal with users' aforementioned perceptions of trust, risk perceptions, and non-self-disclosure behaviour. These are efforts aiming at making up for raised concerns from both users' and lawmakers, and they are working on effective ways of mitigating these privacy risks and trust concerns. The result of *this* study also points to there being positive relationships between effective organizational assurance mechanisms and users trusting beliefs and that these effective assurance mechanisms *do* increase users' self-disclosure behaviour, contrary to what was hypothesized (H7).

The analysed data and the accepted research model also show that perceptions of privacy risks may diminish when there are perceptions of organizations having effective organizational privacy assurances. This result suggests that *effective* self-regulatory activity conducted by organizations can decrease perceptions of risk.

The results also point towards respondents having a fine line between what they perceive as effective self-regulatory activity and non-effective self-regulatory activity, and that it may vary depending on *how* the organization chooses to assure their users of their commitments to privacy. Past literature suggests that organizations can actively affect these behaviours and thoughts amongst their users' by making the assurance mechanisms more effective in assuring their users of their trustworthiness by showing what information they 'take' and what they do with it. However, the presented results suggest that it may vary from the users' perspective and that it is not always straight forward with what users may consider risky (Xu et al., 2011; Mutimukwue, Kolowska, and Grönlund, 2020; Culnan and Bies, 2003; Culnan and Armstrong, 1999; Graham, 1994).

In the context of privacy policies which aim at being informative of how the organization plans to handle the collected data, - past literature have showed that users' trust, risk perceptions, non-self-disclosure behaviour are concepts that play a part in users' accepting the stated policies. In the case of privacy policy, past literature has also stated that there may be high perceptions of risk at play as the users' have the option to read through the designed safe-guards and make decisions to alter their data sharing settings. This could cause organizations to lose accurate information on their users, which is also why these policies or safeguards are designed to appear as accurate and reliable to their users (Chang et al., 2018; Shim, Johnson, and Jiang, 2006; Mutimukwue, Kolowska, and Grönlund, 2020; Culnan and Armstrong, 1999; Culnan and Bies, 2003; Xu et al., 2011; Hui et al., 2007; Clarke et al., 2000). The results of this thesis also comply with these findings. Privacy policy statements that are considered reliable and accurate in the context of social media and e-commerce sites increases the probability of coming of as trustworthy to users. Effective privacy policies also point towards decreasing the probabilities of having users choosing to not disclose their information, and that they perceive these policies to as less risky.

7. Contributions and conclusions to the thesis

The following chapter will discuss the theoretical and practical contributions to the literature topic as well as the conclusions with the key findings of this thesis.

7.1. Theoretical contributions

The research model aimed at researching the similar concepts as Mutimukwue, Kolowska, and Grönlund (2020), but in the context of social media and e-commerce sites, instead of separately examining the model in the contexts of e-commerce sites, e-government sites, and social networking. As this thesis have attempted to extend on the literature findings from Mutimukwue, Kolowska, and Grönlund (2020), this thesis has also extended on the gap in literature that links concerns, behaviour, and perceptions to organizations' different privacy assurances, in one comprehensive model. As other previous literature has only picked certain fragments of the model and used it in other contexts, this research model suggests that not only users' concerns, behaviour, and perceptions are equated in relation to organizations privacy assurances, - but that users also equate their *own* different privacy protection mechanisms as a response and compares it to their own needs and wants. This also illustrates the importance of being context specific in regard to the research model, - constructs may vary depending on the context, and users' sensitivity to these concepts may vary depending on the context.

This thesis has also provided results that expands on a limitation of Mutimukwue, Kolowska, and Grönlund's (2020) research. They found that effective organizational assurances reduce risk perceptions for all contexts, except the e-government context. The authors argued that this finding implies that effective self-regulation mechanisms are mostly only suited for non-governmental organizations. Although, it should be noted again that Mutimukwue, Kolowska, and Grönlund (2020) only conducted their study in Rwanda and therefore only Rwandan e-governmental sites. This thesis would however also have to be conducted in Rwanda in order to make a fair comparison, - which is why this matter will be discussed in the limitations and implications chapter.

However, Mutimukwue, Kolowska, and Grönlund (2020) did not conclude that lowered risk perceptions correlate with effective organizational assurances for all contexts, - which is confirmed under the null hypothesis in *this* thesis. The provided results in this thesis suggest that organizations self-regulating assurance mechanisms do in fact correlate with users' risk perceptions in contexts concerning e-services that are not governmentally owned.

7.2. Practical Contributions

As mentioned, the accepted research model may also provide practical contributions to how organizations can design their different privacy assurance mechanisms in an effective way according to their users. The findings may come in use when formulating these types of assurances in efforts of aligning them with what potential users may react positively- or negatively to. It may also assist social media and e-commerce providers in adjusting established assurances in a way that is more aligned with users' perceptions, trusting beliefs, and behaviours if they have recorded cases of non-self-disclosure behaviour, low perceptions of risk and/or trust.

As it has been explained that organizations privacy assurance mechanisms and policies *do* relate to users and their perceptions of risk, trusting beliefs, and non-self-disclosure behaviour. The findings suggest that these factors have significant effects on how the organizations' privacy assurance mechanisms and privacy policies are perceived, which is why the contribution to organizations is to make use of the findings when implementing information privacy policies and self-regulatory mechanisms concerning user privacy.

7.3. Conclusions to the thesis

The findings serve to develop a practical- and theoretical understanding of organizational privacy assurances and users' privacy concerns, trusting beliefs and self-disclosure behaviour. In conclusion, social media and e-commerce sites users' have been studied through quantitative analysis in the form of a survey that received

100 valid responses. The key findings of this thesis answer the posed research problem of wanting to explain the relationship between organizational privacy assurances and policies, - and users' perceived concerns, risks perceptions, trusting beliefs, and information-disclosure behaviour.

It should also be mentioned that most of the measures had strong and significant correlations. To illustrate this, one may analyse the significance of each measure to see what constructs had the largest effect on each other in *table 9*. Hypothesis three had the strongest value of 0,756 and it measured perceived effective privacy policies and how it affects trusting beliefs. This measure implies that roughly 75 % of the variable concerning organizations privacy policies can be explained by how much trust a user holds.

The findings suggest that risk perceptions, trusting beliefs, and non-self-disclosure behaviour are equated amongst users as a response to questions and/or conditions regarding users' private information trade. If perceptions of risk are heightened, trusting beliefs will be negatively affected and the probability of non-self-disclosure behaviour heightens. This implies that organizations can work to better generate positive perceptions through developing privacy policies and self-regulations in a way that assures users of their devotement to user privacy and their high commitments to users' safety management of personal data.

Furthermore, the results also suggest that users show non-disclosure behaviour in case the perceptions of risks are higher and trusting beliefs are low. The findings also suggest that effective organizational self-regulations affect non-self-disclosure behaviour *positively*, - contrary to what was hypothesized. Effective organizational privacy policies and mechanisms do in fact positively relate to users' willingness to disclose information, as well as to users' perceptions of low levels of risk, - which increases trusting beliefs.

8. Limitations, implications, and recommendations

The following chapter explains the found limitations of this thesis as well as the implications found. The thesis will then be concluded by recommending future researchers to build upon this thesis.

8.1. Limitations

Time and resource constraints were perhaps the biggest limitations on this research. It is perhaps what hindered this research from producing more responses, more results, and more generalizable results.

8.1.1. Implications

Since there were time and resource constraints, it was argued in the methodology that a convenience sample would be used, and that the questionnaire would be distributed via my own Facebook feed. This choice of method was perhaps the reason to why many of the respondents were Swedish females who are students in the ages of 20 and 30. This implication may imply that the results are not generalizable or representative enough for a whole population. Even though a non-probability sampling method was chosen, it appears as if the targeted population could have been young, Swedish female, - and students which is *not* the sample this research set out to address as a non-probability sampling method was used. However, it is considered an implication that the statistics ended up being skewed towards Swedish female students in the ages of 20 and 30, and that the results of this thesis may be limited to a sub-category of the sample population. The findings may for example have been different if there were more male participants as females may be more risk averse (Hibbert, Lawrence and Prakash, 2008). Similarly, the findings may have been different if people in their 60s as opposed to people in their 20s were participating in this study, as a study conducted by Albert and Duffy (2012) concluded that older adults have shown to be more risk averse than younger people since they calculate the consequences of potential losses more. This is also addressed as a future recommendation for other researchers to investigate, which is mentioned in the *8.3 recommendations* sub-chapter.

One should also consider the total amount of collected responses for this research. In an ideal situation where there were fewer limitations, - one would have been able to collect a lot more responses like Mutimukwue, Kolowska, and Grönlund (2020), which had around 500 responses. As this was not the case for this thesis, it should be considered as an implication to the total study.

8.1.2 Recommendations

The recommendation for future researchers is to allocate more time towards this research model. With more time and resources, this research model could be applied in multiple other contexts and reach a substantial number of responses in other countries than Sweden to see if there are any possible cultural differences. As the collected data showed to be skewed towards Swedish female students in the ages of 20 and 30, it is also recommended that future researchers collect data from other sample populations. It would for example be interesting to research the possible differences in opinions and attitudes amongst 20-year-olds versus 60-year-olds, across different occupations and gender identifications- as mentioned.

Future studies should also explore possibilities of expanding the model to research other privacy assurance mechanisms than those who are created for social media and e-commerce sites. It would also be interesting to tie the research model to possible social constructs part of using social media or e-commerce sites as some respondents put in their own answers in the last question of the questionnaire, saying: *I refuse to provide personal information to social media and e-commerce sites*. Respondents answered that they in some cases would like to stop using social media or e-commerce sites because of perceptions of privacy risks but that they feel they would lose their built-up networks and suffer consequences socially. A study considering social constructs in the research model could perhaps contribute to organizations even more than what has been presented yet.

9. Bibliography

Aaker, D., Kumar, V., Day, G. and Leone, R. (2011). Marketing research. 10th ed. Hoboken (N.J.): Wiley.

Abri, D. A., McGill, T., & Dixon, M. (2009). Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: an oman perspective. *Journal of Information Privacy and Security*, *5*(2), 3-26.

Albert, S. M., & Duffy, J. (2012). Differences in risk aversion between young and older adults. *Neuroscience and neuroeconomics*, *2012*(1).

Bansal, G., & Zahedi, F. (2008). Efficacy of privacy assurance mechanisms in the context of disclosing health information online. *AMCIS 2008 proceedings*, 178.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*(6), 624-644.

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

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends® in Marketing*, *11*(1), 1-71.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems*, *11*(3-4), 245-270.

Bethlehem, Jelke. (1999). Cross-sectional research. In Adèr, Herman J., and Mellenbergh, Gideon J. Research methodology in the social, behavioural and life sciences (pp. 110-142). London: Sage Publications.

Brunner, M., & Süß, H.-M. (2005). Analyzing the Reliability of Multidimensional Measures: An Example from Intelligence Research. *Educational and Psychological Measurement, 65*(2), 227–240.

Bryman, Alan and Bell, Emma. (2015). Business Research Methods. 4. ed., Oxford: Oxford university press.

C. Graham Self-regulation. G. Richardson, H. Genn (Eds.), Administrative law and government action, the courts and alternate mechanisms of review, Clarendon Press, Oxford, England (1994).

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445-459.

CIGI-ipsos 2018 global survey on internet security and trust Bricker, D. A. R. R. E. L. L., FELLOW, C. S., HAMPSON, F. O., & FELLOW, C. D. (2018). Internet Security and Trust.

Clarke, R. (2000). Beyond the OECD guidelines: privacy protection for the 21st century. *Canberra, Australia: Xamax Consultancy Pty Ltd. Retrieved August*, *5*, 2009.

Cohen, Jacob. (1988). Statistical power analysis for the behavioral sciences. 2. ed., New York: Lawrence Erlbaum associates.

Cook, R. Dennis and Weisberg, Sanford. (1982). Residuals and Influence in Regression. New York: Chapman and Hall.

Creswell, John W., and Creswell, J. David. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 5. ed., California: Sage Publications.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, *59*(2), 323-342.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure*. Sage Publications, Inc.

Dillman, D. A. (1983). Mail and other self-administered questionnaires. *Handbook for survey research*, 359-377.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422.

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

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human–Computer Interaction*, *36*(19), 1834-1848.

Easterby-Smith, M., Thorpe, R., Jackson, P. and Jaspersen, L. (2018). Management & Business Research. 6th ed. Thousand Oaks: SAGE.

Ebert, N., Ackermann, K. A., & Heinrich, P. (2020, April). Does context in privacy communication really matter?—A survey on consumer concerns and preferences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-11).

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. University of Akron Press.

Farooq, M., & Qureshi, Q. A. (2020). Privacy of internet users in the era of transformative marketing. *Journal of Management Practices, Humanities and Social Sciences*, *4*(2), 25-28.

Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, *100*, 102082.

Fidell, S., Silvati, L., Howe, R., Pearsons, K. S., Tabachnick, B., Knopf, R. C., ... & Buchanan, T. (1996). Effects of aircraft overflights on wilderness recreationists. *The Journal of the Acoustical Society of America*, *100*(5), 2909-2918.

George, Darren and Mallery, Paul. (2003). SPSS for Windows step by step: A simple guide and reference. 4. ed., Boston: Allyn and Bacon.
Ghauri and Gronhaug, 2005.

Ghauri, P. and Grønhaug, K. (2010). Research methods in business studies. 4th ed. Harlow: Pearson Education.

Gómez-Barroso, J.L. (2021). Public Economics: A Concise Introduction (1st ed.).

Google n.d : Google (n.d.). Google Forms: Free Online Surveys for Personal Use. [online] Google.se. Available at: https://www.google.se/intl/en/forms/about/

[Accessed April 10th 2019].

Hair, Joseph F., Black, William C., Babin, Barry J., and Anderson, Rolph E. (2013). Multivariate Data Analysis. 7. ed., Harlow: Pearson Education

Harring, N. (2018). Trust and state intervention: Results from a Swedish survey on environmental policy support. *Environmental Science & Policy*, *82*, 1-8.

Hoffman, D. L.; Novak, T. P.; and Peralta, M., "Building Con Trust Online," Communications of the ACM, Volume 42, Number 4, 1999.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Mis Quarterly*, 275-298.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Mis Quarterly*, 19-33.

Iacobucci, D. and Churchill, G. (2015). Marketing research. 11th ed. Nashville: Earlie Lite Books, Inc.

Jacobsen, Dag I. (2002). Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund: Studentlitteratur.

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?. *Government Information Quarterly*, *32*(4), 363-368.

Johnson, R. E., & Ranganathan, S. (2002). Exact algorithm for dynamics of charged particles in a magnetic field. *Physics and Chemistry of Liquids*, *40*(5), 527-538.

Kantarcioglu, M., & Ferrari, E. (2019). Research challenges at the intersection of big data, security and privacy. *Frontiers in big Data*, 1.

Kanwal, T., Anjum, A., & Khan, A. (2021). Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing*, *24*(1), 293-317.

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, *126*, 221-238.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., Ha, Y. W., & Park, M. C. (2016). Understanding antecedents to perceived information risks: An empirical study of the Korean telecommunications market. *Information Development*, *32*(1), 91-106.

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

Malhotra, N. (2010). Marketing research: An applied orientation. 6th ed. Upple Saddle River, New Jersey: Pearson.

Malhotra, Naresh K., Kim, Sung S., and Agarwal, James. (2004). Internet Users Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, Information Systems Research, vol. 15(4), pp. 336-355

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5-21.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of consumer research*, *26*(4), 323-339.

Mousavizadeh, M., & Kim, D. (2015). A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory.

Mousavizadeh, M., Kim, D. J., & Chen, R. (2016). Effects of assurance mechanisms and consumer concerns on online purchase decisions: An empirical study. *Decision Support Systems*, *92*, 79-90.

Murray, K. B., & Häubl, G. (2009). Personalization without interrogation: Towards more effective interactions between consumers and feature-based recommendation agents. *Journal of Interactive Marketing*, *23*(2), 138-146.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Nam, C., Song, C., Lee, E., & Park, C. (2006). Consumers‟ Privacy Concerns and Willingness to Provide

Nielsen, J. and Lindvall, J., 2021. Trust in government in Sweden and Denmark during the COVID-19 epidemic. *West European Politics*, 44(5-6).

Nunnally JC, B IR. Psychometric Theory. 3rd ed. New York: McGraw-Hill (1994).

Pallant, Julie. (2010). SPSS survival manual: a step by step guide to data analysis using SPSS. 4. ed., Maidenhead: McGraw Hill.

Patel, Runa and Davidson, Bo. (2003). Forskningsmetodikens grunder. Att planera, genomföra och rapportera en undersökning. Lund: Studentlitteratur

Pedhazur, E.J. (1997) Multiple Regression in Behavioral Research: An Explanation and Prediction. Holt, Rinehart & Winston, New York.

Rains, S. A., Brunner, S. R., & Oman, K. (2016). Self-disclosure and new communication technologies: The implications of receiving superficial self-disclosures from friends. *Journal of Social and Personal Relationships*, *33*(1), 42-61.

Saunders, M., Lewis, P. and Thornhill, A. (2009). Research methods for business students. 5th ed. Harlow: Pearson Education Limited.

Saunders, M., Lewis, P. and Thornhill, A. (2016). Research methods for business students. 7th ed. Harlow: Pearson.

Sharma, S., Singh, G., & Pratt, S. (2022). Modeling the multi-dimensional facets of perceived risk in purchasing travel online: a generational analysis. *Journal of Quality Assurance in Hospitality & Tourism*, *23*(2), 539-567.

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

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. l. Rev.*, *154*, 477.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, *68*(3), 459.

Süb, H. M., & Beauducel, A. (2005). Faceted models of intelligence. *Understanding and measuring intelligence*, 313-322.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in human behavior*, *29*(3), 821-826.

Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets*, *17*(1), 68-81.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 16.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research*, *122*, 915-925.

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. *Government Information Quarterly*, *31*(1), 150-159.

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

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information systems*

research, *23*(4), 1342-1363.

Yu, J. W. K. (2005). Electronic government and its implication for data privacy in Hong Kong: Can Personal Data (Privacy) Ordinance protect the privacy of personal information in cyberspace?. *International Review of Law, Computers & Technology*, *19*(2), 143-163.

10. Appendices

10.1Appendix A – Operationalization table

Table 4. Operationalization

Concept	Dimensions	Authors	Items	Measurement
Privacy concerns	Concerns	*Malhotra et al., 2004.* *Dinev and Hart, 2004. Dinev and Hart, 2006. Hong and Thong, 2013.* *Xu et al., 2011.* *Derlega et al., 1993.* *Rains, Brunner, and Oman, 2016.* *Mutimukwe, Kolowska, and Grönlunda, 2020.*	**PC1**	I am concerned about giving up private information about myself to social media and e-commerce sites
	Control		**PC2**	I am concerned about giving up private information about myself to social media and e-commerce sites because my private information might be used in ways I did not foresee
	Perceived risks		**PC3**	I am concerned about giving up private information about myself to social media and e-commerce sites because of what others may do with it.
Perceived privacy risks	Perceived risks	*Xu et al., 2011* *Abri et al., 2009*	**PPR1**	I feel that it is risky to provide personal information to social media and e-commerce sites.

	Trust	*Mutimukwue, Kolowska, and Grönlund, 2020* *Dinev and Hart 2004, 2006*	**PPR2** **PPR3**	I believe personal information could be inappropriately used by social media and e-commerce sites. I believe that providing personal information to social media and e-commerce sites may lead to unexpected problems
Perceived effectiveness of privacy policy	Accuracy	*Xu et al., 2011* *Chang et al., 2018* *Shim, Johnson, and Jiang, 2006* *Mutimukwue, Kolowska, and Grönlund, 2020* *Culnan and Armstrong, 1999* *Culnan and Bies, 2003* *Hui et al., 2007*	**PEPP1**	I believe that the majority of privacy statements made by social media and e-commerce sites are representing how they protect my personal information.
	Reliability		**PEPP2** **PEPP3**	I believe that the majority of privacy statements made by social media and e-commerce sites reflect that they will keep my private information confidential. I believe that privacy assurance statements made on social media and e-commerce sites is an effective system of ensuring my privacy

Perceived effectiveness of organizations self-regulations	Relevance Trust	*Xu et al., 2011* *Mutimukwue, Kolowska, and Grönlund, 2020* *Culnan and Bies, 2003* *Culnan and Armstrong, 1999* *Graham, 1994*	**PEOS1** **PEOS2**	I believe that privacy regulations will impose sanctions on social media and e-commerce sites who do not comply with privacy policies. I believe that privacy regulations will help me in case my personal information is misused on social media and e-commerce sites.
Trusting beliefs	Risk Control Dependability	*Sharma, Singh & Pratt, 2021* *Mutimukwe, Kolowska & Grönlunda, 2020* *Libaque-Saenz et al., 2016* *Abri, Mcgill, & dixon, 2009* *Libaque-Saenz, Chang, Kim, Park, & Rho, 2018* *Malhotra, Kim & Agarwal, 2004* *Chang et al., 2018*	**TB1** **TB2** **TB3** **TB4** **TB5**	I believe that social media and e-commerce sites are trustworthy in handling private information I trust that social media and e-commerce sites fulfill their promises in handling my personal information with care I trust that social media and e-commerce sites have my best interest in mind when handling my personal information. I trust that social media and e-commerce sites are predictable and consistent in their ways of handling personal information.

				I believe that social media and e-commerce sites are honest and trustworthy in how they handle personal information.
Non-self-disclosure behaviour	Control	*Xu et al., 2011, 2012* *Abri et al., 2009* *Mutimukwue, Kolowska, and Grönlund, 2020* *Chang et al., 2018* *Liu et al, 2005* *Taddei and Contena, 2013* *Culnan and Armstrong, 1999* *Clarke, 2000*	**NSDB1**	I chose to not use social media and e-commerce sites because I do not want to provide them with my personal information.
	Perceived risk		**NSDB2**	I chose to not use social media and e-commerce sites because I disagree with their ways of handling personal information
			NSDB3	I refuse to provide personal information to social media and e-commerce sites

10.2. Appendix B – Questionnaire

Information Privacy

Hello, my name is Miranda. I am a master's student at the knowledge-based entrepreneurship program at the School of Business, Law and Economics in Gothenburg. I am in the process of conducting a master thesis on information privacy on social media and e-commerce sites, and I want to know your opinions and attitudes on this topic! All of your answers will be anonymous and only used in the context of this master thesis. It should only take about 5 minutes of your time, and it would be much appreciated if you choose to participate!

Here is a short background to the topic. The increasing internet and social media use has lead to an increase of users' privacy concerns, as technology continually offers ample opportunities for organizations to store, process, and exploit personal data. This may reduce individuals' perceived ability to control their personal information and increase their perceived privacy risks. This study seeks to examine different privacy assurances made by organizations and how users react and act in response to them. Throughout this survey you will go through questions relating to your own privacy concerns, privacy control, risk perceptions, non-self-disclosure behavior and trusting beliefs.

Note! The survey is divided into different sections where you are asked to answer to statements through a scale of 1-7, where (1) represents 'strongly disagree' and (7) represents 'strongly agree'. Try to not to fill in too many neutral answers (4) if possible!

Feel free to send me an email if you have any questions at: gusokemi@student.gu.se

milstenmiranda@gmail.com (Delas inte) Byt konto

*Obligatorisk

What gender do you identify with? *

- Female
- Male
- Non-binary
- Prefer not to say

What is your age? *

- Younger than 15
- 15-24
- 25-34
- 35-44
- 45-54
- 55 or older

What is your occupation? *

- Student
- Employed
- Unemployed
- Retired
- Other

Country of residence *

Ditt svar

Nästa

Rensa formuläret

privacy concerns

I am concerned about giving up private information about myself to social media and e-commerce sites *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I am concerned about giving up private information about myself to social media and e-commerce sites because my private information might be used in ways I did not foresee

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I am concerned about giving up private information about myself to social media and e-commerce sites because of what others may do with it.

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Bakåt Nästa Rensa formuläret

I feel that it is risky to provide personal information to social media and e-commerce sites

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe personal information could be inappropriately used by social media and e-commerce sites

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe that providing personal information to social media and e-commerce sites may lead to unexpected problems

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

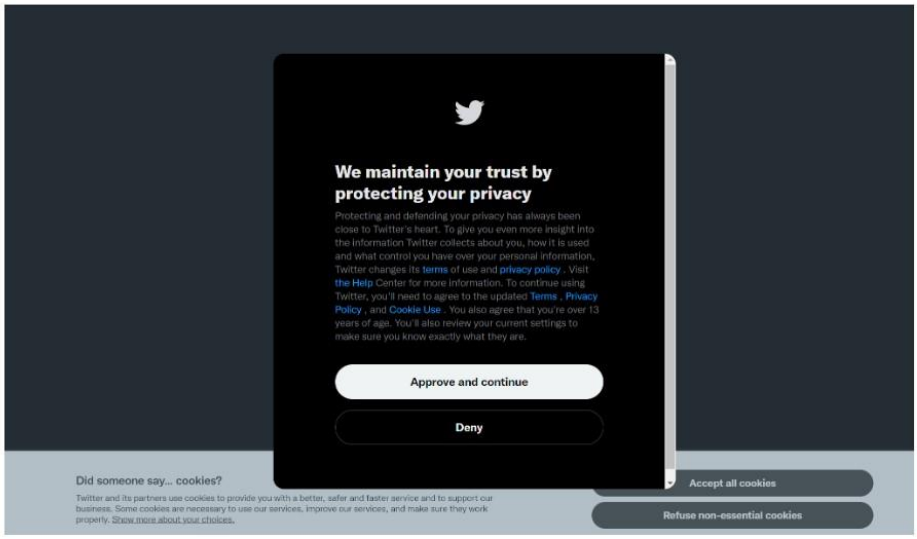
Want to add something?

Ditt svar

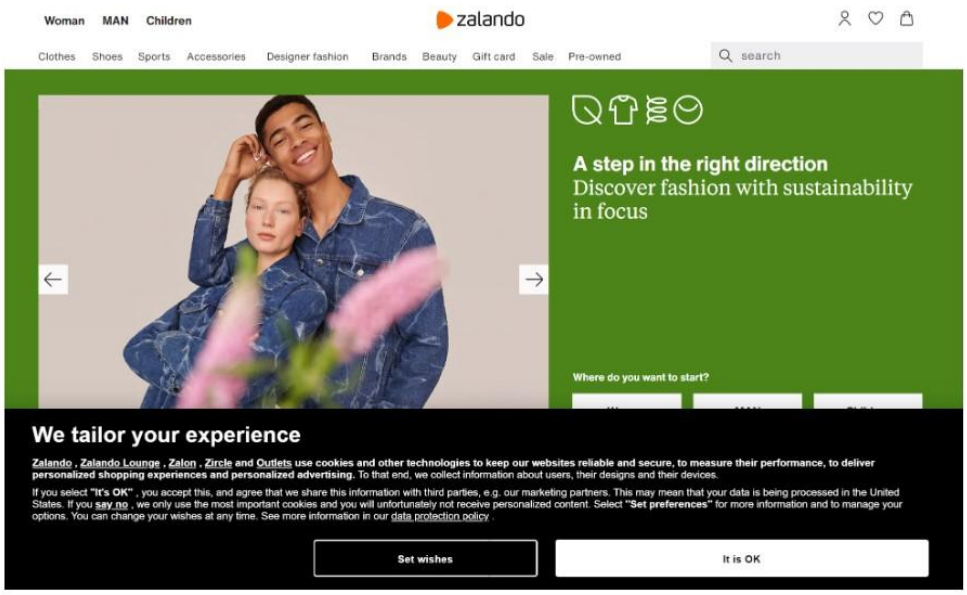
Bakåt Nästa Rensa formuläret

Take a look at the following pictures of privacy statements made by social media and e-commerce sites

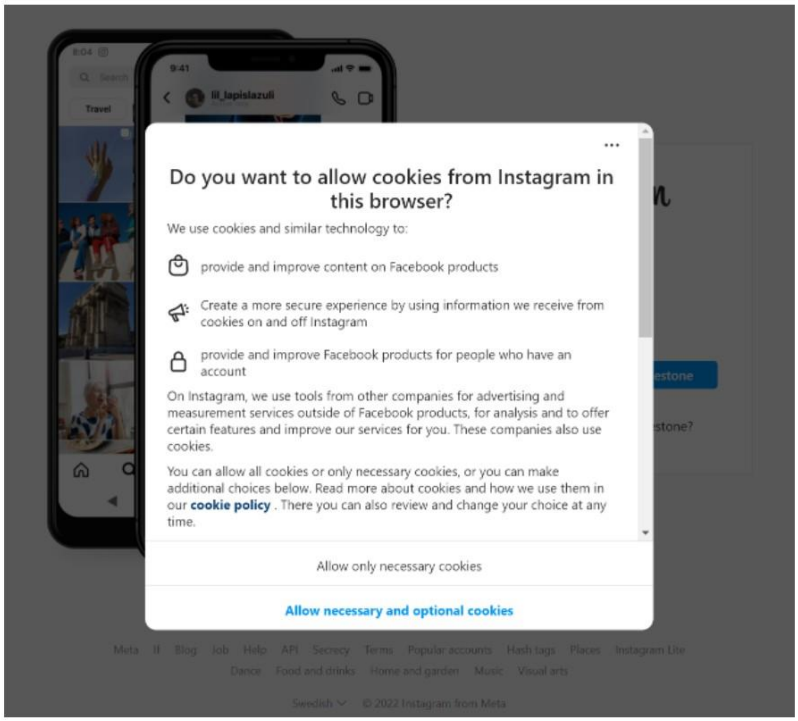
Twitter



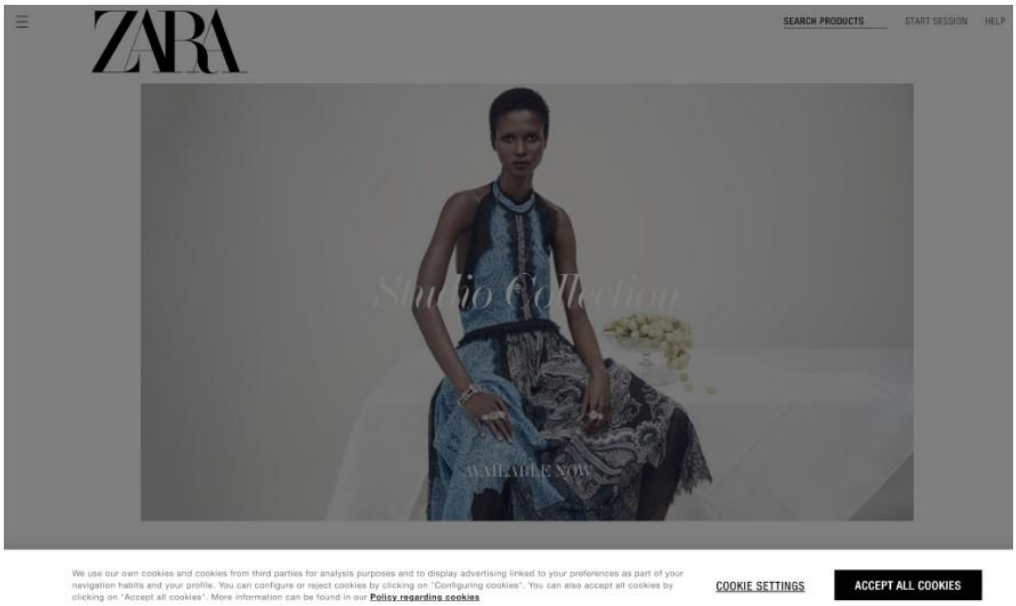
Zalando



Instagram



Zara



Bakåt Nästa Rensa formuläret

Privacy Policy

I believe that the majority of privacy statements made by social media and e-commerce sites are representing how they protect my personal information. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe that the majority of privacy statements made by social media and e-commerce sites reflect that they will keep my private information confidential. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe that privacy assurance statements made on social media and e-commerce sites is an effective system of ensuring my privacy *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Want to add something?

Ditt svar

Privacy Regulations/Laws

I believe that privacy regulations will impose sanctions on social media and e-commerce sites who do not comply with privacy policies. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe that privacy regulations will help me in case my personal information is misused on social media and e-commerce sites. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Want to add something?

Ditt svar

Bakåt Nästa Rensa formuläret

Trust

I believe that social media and e-commerce sites are trustworthy in handling private information *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I trust that social media and e-commerce sites fulfill their promises in handling my personal information with care *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I trust that social media and e-commerce sites have my best interest in mind when handling my personal information. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I trust that social media and e-commerce sites are predictable and consistent in their ways of handling personal information. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I believe that social media and e-commerce sites are honest and trustworthy in how they handle personal information. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Want to add something?

Ditt svar

Bakåt Nästa Rensa formuläret

Non-self disclosure

I chose to not use social media and e-commerce sites because I do not want to provide them with my personal information. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I chose to not use social media and e-commerce sites because I disagree with their ways of handling personal information *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

I refuse to provide personal information to social media and e-commerce sites *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Want to add something?

Ditt svar

Ditt svar

Thank you for your participation

Bakåt Skicka Rensa formuläret