LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Online Privacy Concerns

Introducing the effects of an individuals' perception of privacy regulation to the APCO Macro model

Master thesis 15 HEC, course INFM10 in Information Systems
Presented in June, 2018

Authors: Alexander Berntsen
Mike Dibbetz

Supervisor: Bo Andersson

Examiners: Odd Steen
Olgerta Tona

Online Privacy Concerns: introducing the effects of an individuals' perception of privacy regulation to the APCO Macro model

Authors: Alexander Berntsen and Mike Dibbetz

Publisher: Dept. of Informatics, Lund University School of Economics and Management.

Document: Master Thesis

Number of pages: 83

Keywords: GDPR, privacy concerns, trust beliefs, perceived regulatory knowledge, perceived regulatory awareness

Abstract:

With rising privacy concerns of individuals, the EU parliament actively starts protecting the privacy of its citizens with enforcement of the GDPR. This study examines if enforcement of GDPR will lead to an individuals' lower privacy concerns and higher trust beliefs with regard to E-commerce companies. The APCO framework is followed. Besides using already existing constructs within this framework, two new constructs were formed and tested. Respectively, perceived privacy regulation knowledge and perceived privacy regulation awareness. A pilot test and evaluation panel was used to increase the validity of these new constructs before using them in the final survey. This survey examined the relationship between 5 constructs and the influence of four groups based on the covariates. 217 valid responses were acquired from both an online sample (N=127) and a field sample (N=90). PLS-SEM is used to examine the outcomes. Proof is provided for the relation between how individuals perceive governmental privacy regulations and the constructs privacy concerns and trust beliefs. However, this relation does not hold for the sample as a whole, but is dependent on the groups: age, education, gender and previous privacy invasion. Furthermore, empirical justification is found confirming already established relations in the APCO framework.

Acknowledgement

We would like to express our sincerest appreciation to our supervisor Bo Andersson, for his constructive advice and supportive guidance during the writing process. Additionally, we would like to thank Miranda Kajtazi for her valuable guidance, patience and support. Furthermore, we would like to thank Olgerta Tona for the preliminary brainstorm sessions on the topic of this study. Lastly, we dedicate a special thanks to everyone who contributed in any possible way to the outcome of this thesis.

Alexander Berntsen, Mike Dibbetz

Lund, May 2018

Content

Figures

Tables

Abbreviations

TERM	DEFINITION
PPRA	Perceived privacy regulation awareness
PPRK	Perceived privacy regulation knowledge
TB	Trust beliefs
PC	Privacy concerns
WD	Willingness to disclose
GDPR	General data protection regulation
E-COMMERCE	Electronic commerce
PLS	Partial least squares
AVE	Average variance extracted
HTMT	Hetrotrait-monotrait of correlations
SEM	Structural equation model
MGA	Multi group analysis
EU	European Union
CI	Confidence Interval

1 Introduction

Nowadays, more data cross the internet every second than were stored in the entire Internet 20 years ago (McAfee, Brynjolfsson, Davenport, Patil, & Barton, 2012). Data has become so valuable that organizations are willing to pay hundreds of millions when acquiring companies that are based on customer data. For instance, Microsoft acquired online professional network LinkedIn for $26,2 billion, meaning that they were willing to pay $260 per monthly active user (Short & Todd, 2017). The value of this type of data results in organizations collecting more and more customer data.

While organizations continuously increase the collection and use of customer data, customers concern in regard to their privacy grows (Martin, Borah, & Palmatier, 2017). Furthermore, as systems and applications have developed, the individual control of both collection and usage of personal identifiable information has become limited (Terzi, Terzi, & Sagiroglu, 2015). Privacy concerns of how personal data is handled may lead to individuals removing their information, spread negative feedback, or express their concerns to third parties (Lee, Lee, Lee, & Park, 2015). Disclosure of personal information may result in benefits, for example in the form of personalized services. However, while some individuals may be willing to disclose their personal information for benefits, others may consider it to be a violation of their fundamental rights (Karwatzki, Dytynko, Trenz, & Veit, 2017). This issue has not only caught the attention of individuals sharing personal information, but also governments as to protect the data of its citizens. The most recent example of governments acting within the area of privacy regulation is the General Data Protection Regulation (GDPR). The regulation is applying to all European member states and is considered to be a landmark in the evolution of the European privacy framework (Goddard, 2017).

As the topic of privacy concerns is a hard and complex problem area for both individuals and organizations, laws and regulations can play an important role (Terzi et al., 2015). Furthermore, since customer data is perceived to become a more significant source of competitive advantage, gaining consumers' trust will be important for organizations to keep acquiring their data (Morey, Forbath, & Schoop, 2015). Perceived privacy regulations could be a way of assuring this trust according to Miltgen and Smith (2015).

To better understand the complex environment of privacy concerns, Smith, Dinev, and Xu (2011) underwent a comprehensive review of privacy-related literature. From this review, the APCO Macro model was created. This model assembled from 320 privacy articles and 128 books and book sections, creates a holistic overview of the current state of privacy research with a focus on privacy concerns. Potoglou, Palacios, and Feijóo (2015) mention that the value of this model occurs from the integration of two previous research streams within privacy research. The authors describe that he first research stream focused on privacy concerns as a dependent variable, being affected by several independent variables (antecedents). Whereas the second stream focused on privacy concerns as an independent variable, influencing behavioural

intentions. The capturing of both of these streams in one single model offers two main advantages. First, it provides an holistic overview of the constructs and established relations within privacy research (Potoglou et al., 2015; Smith et al., 2011). Second, further empirical studies could be targeted to under-researched relations and constructs, adding value to the model (Smith et al., 2011).

1.1 Problem area

Organizations today utilize personal data in order to create competitive advantage (Karwatzki et al., 2017). To be able to achieve such advantage, a vast amount of personal data is needed. Retrieving personal data, could be a concern of the customers' privacy (Awad & Krishnan, 2006). Personal data can be passed on by third parties, transferring it into other contexts that might create unwanted consequences for the individual disclosing personal data (Taddicken, 2014).

E-commerce is one context heavily depending on satisfying privacy concerns as this kind of concerns can cause sales to abate (Dinev & Hart, 2006). In 2017 global e-commerce increased to grow, reaching $2.29 trillion. However, more than two thirds of the consumers are now worried about their online privacy, threatening sales (UNCTAD, 2018). Trust has prior been proven to affect an individuals' privacy concerns within e-commerce (Belanger, Hiller, & Smith, 2002). The new regulation GDPR is enforced to increase online transparency and trust for the citizens of all EU member states (European Parliament, 2016; Goddard, 2017; Tankard, 2016). Processing, transmitting and storing personal data is imminent to complete and deliver transactions and thus vital for e-commerce (Hui, Teo, & Lee, 2007). Thereby, any e-commerce company selling to EU residents must comply with GDPR (European Parliament, 2016). Hence, it is plausible that this governmental regulation will affect an individuals' trust and privacy concerns.

The APCO Macro model includes regulations as both an antecedent and outcome of privacy concerns. However, the model does not account for the perspective on how governmental regulations may affect individuals' privacy concerns (Smith et al., 2011). Thus, this effect is only hypothetical, indicating the need for further research (as will be conducted in subsequent chapters).

1.2 Research question

As underlined in the problem area, governmental regulations regarding data privacy may be an important influencing factor for individuals' privacy concerns and trust. Hence, we aim to answer the following research question:

> *What are the associations between governmental privacy regulations, an individuals' privacy concerns and trust in disclosing personal data?*

1.3 Purpose

The purpose of this study is to contribute with new constructs to a well-known model within privacy research, the APCO Macro model (Smith et al., 2011). In accordance with the research question, the proposed factors concern governmental privacy regulations. Such privacy regulations have proved to be a timely and considerably important matter to the involved actors (Goddard, 2017; Graham-Harrison, 2018). However, research on the impact of governmental privacy regulations on privacy concerns is limited within privacy research (Miltgen & Smith, 2015). Accordingly, the results of this study can provide new insights to this important, but limited area of privacy research.

1.4 Delimitation

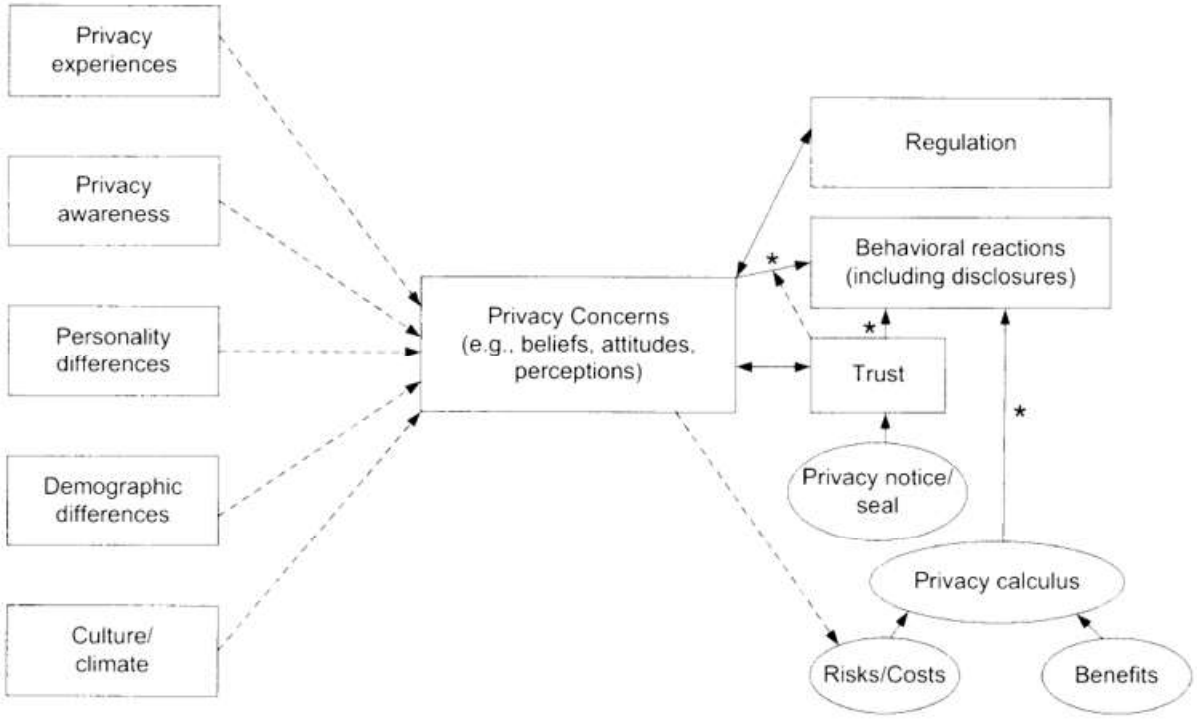
The focus of this study is online privacy, excluding the offline context of privacy. Furthermore, this study is delimited to governmental regulations rather than self-regulation. More specifically, this study looks into the General Data Protection Regulation active in all European Union (EU) member states (Goddard, 2017). As privacy concerns are reliant to the context, this study will be delimited to one (Boritz & No, 2011). E-commerce will be the context used to study the proposed hypotheses. Although GDPR is active in all EU member states, the collection of the field data delimits itself to Sweden due to resource constraints.

2 Theoretical background

2.1 APCO Macro model

Information privacy has been defined in various ways by different authors. Whilst there is no widely accepted definition of information privacy, a recurrent description includes that privacy is an individual's ability to control information that regards themselves (Bélanger & Crossler, 2011). An individuals' control of information includes but is not limited to how, when and what amount of personal data is divulged to others (Karwatzki et al., 2017). Information privacy was already in 1989 deemed as one of the most important ethical issues of the information age (Smith, Milberg, & Burke, 1996). Privacy continues to be a major concern as advancements in technology has further enabled for more extensive collection and utilization of personal information (Pavlou, 2011).

Smith et al. (2011) conducted a thorough review of existing information privacy literature in the disciplines of: IS, Marketing, and organizational behavior. The review included 320 privacy articles and 128 books and book sections that were published between the 1960's and 2010. This resulted in the APCO Macro Model, showing the relations between privacy and other constructs following the structure of: *Antecedents* → *Privacy Concerns* → *Outcomes* (Figure 2.1).



Dotted lines indicate that the relationship is tenuous (i.e., has not been confirmed through repeated studies).

Not shown: Possible two-way loop, in which some actions on the right may impact some constructs on the left.

*Results threatened by privacy paradox, since usually intentions (not behaviors) have been measured.

Figure 2.1. APCO Macro Model (Smith et al., 2011)

According to the model, privacy concerns can be seen as the central construct within privacy research (Smith et al., 2011). Most research concerning privacy constructs which has been done after the work of Smith et al. (2011) also uses privacy concerns as the main construct (Kordzadeh, Warren, & Seifi, 2016; Ozdemir, Smith, & Benamati, 2017; Zhang, Chen, & Lee, 2013). Privacy concerns can be seen as the main predictor for behavioral reactions concerning data disclosure (Smith et al., 2011). The model consists of many different constructs. To answer the research question, trust, privacy concerns, and behavioral reactions will be examined from chapter 2.3.5 and onwards. Lastly some of the paths are threatened by the privacy paradox as can be seen in figure 2.1. The privacy paradox encompasses the fact that individuals may not act in accordance with their privacy concerns (Smith et al., 2011).

2.2 Legislation

Privacy legislation is a rather complex landscape. Currently, there is a general EU directive concerning privacy. However, each member state of the EU has their own national privacy regulation (Appendix 4, I2R4). The *personuppgiftslagen* in the case of Sweden (Appendix 3, I1R2). The 25th of May the new EU data protection will become active and the Swedish national law will be repealed (Appendix 3, I1R2). With this future perspective in mind, the most important privacy regulations in Sweden concerning the E-commerce domain will be GDPR and the E-privacy regulation (Appendix 3, I1R15, Appendix 4, I2R6). However, these laws are not only applicable to Sweden but also become active within all EU member states (Goddard, 2017; Tankard, 2016).The remainder of this section will therefore focus on those regulations: GDPR and E-privacy.

2.2.1 GDPR

On the 25th of May 2018, the EU applied the general data protection regulation (GDPR) which sees to privacy as a fundamental human right. The law concerns personal data of European residents and will be enforced in all 28 member states of the European Union (Goddard, 2017). For the individual user, the GDPR will have multiple implications. Organizations seeking to gather personal data must have been granted informed and voluntary consent from individuals. The individuals have the right to access all the information that organizations possess about them (Tankard, 2016). When an individual's personal information is either disclosed by the individual themselves or by third party, they have the right to be notified. It is also possible for the correction of one's personal information (European Parliament, 2016). Individuals may object to having their data processed or restricted if there are legitimate reasoning to do so (European Parliament, 2016; Tankard, 2016). Furthermore, it is possible for individuals to ask to be forgotten. This means that organizations need to remove all data that is deemed as inadequate, irrelevant or no longer relevant (Tankard, 2016). GDPR also includes data portability which means that individuals have the right to request their personal data, that they have provided to an organization, in a structured, commonly used and machine-readable format so that it can be transmitted to another (European Parliament, 2016).

GDPR will be directly applied in the member states but does allow for some national variations under certain circumstances, such as the minimum age for consent to use an individual's personal data (Morrison et al., 2017). The law is not limited to where personal data is being stored. If organizations are storing personal data of European residents, they must comply with the

GDPR, with no exception to Cloud services (Tankard, 2016). Organizations must be able to provide proof that they are indeed complying with the GDPR if requested by any relevant supervisory authority. Failure to do so, is assumed to be a failure of compliance (Morrison et al., 2017). If organizations fail to comply with the GDPR they can either receive a fine of 2% of their global revenue or €10 million for minor breaches. More severe breaches can be fined 4% of the global revenue or €20 million. Whichever is the highest amount will be the fine, however first offences may result in a warning instead (Tankard, 2016).

2.2.2 E-privacy Regulation

To align with the new GDPR, the directive on privacy and electronic communications also needs to be revised. The E-privacy regulation will therefore repeal Directive 2002/58/EC Regulation on Privacy and Electronic Communications (EUR-Lex, 2017). The proposal for the new E-privacy regulation includes confidentiality for 'new' players providing electronic communications, such as: *WhatsApp*, *Facebook Messenger* and *Skype*. A strong aspect from this rule is that it is applicable and legally binding in the entire EU, just like the GDPR. The new regulation will in addition contain simpler rules on non-privacy intrusive cookies to improve internet experiences, such as shopping cart history and cookies that count the number of visitors. Consumers will furthermore be protected against spam. The proposal bans unsolicited electronic communication by e-mails, SMS and automated calling machines (European-Commision, 2017). The draft version of this regulation was accepted on the 10th of January 2017 and the regulation was planned to be effective on the 25th of May, just like the GDPR. However, experts think that this is unrealistic and will not be enforced in time while it is not finalized (Appendix 3, I1R11).

2.3 Research model

The remainder of this chapter will present the proposed research model and clarify the decisions made regarding the created and used constructs. Section 2.3.1 and 2.3.2 present a general overview of prior regulatory constructs and introduce the need for two new constructs in this area. Section 2.3.3 and 2.3.4 provide a thorough literature background on the newly formed constructs. Consequently section 2.3.5 and onwards offer a thorough literature background on the constructs within the research model, that are already established within the APCO Macro model, including the adapted covariates.

2.3.1 From regulation to perceived awareness and knowledge

Smith et al. (2011) present regulations as an outcome of privacy concerns in the APCO Macro Model. The authors argue that if customers do not perceive that their privacy is being protected sufficiently, the customers will distrust the organizations self-regulation. Further, this could lead to regulatory response. However, Lwin, Wirtz, and Williams (2007) mention that governmental regulations may also affect the privacy concerns that one has, not only organizations self-regulation. Likewise, the developed research model for this study (figure 2.2) aims to take a closer look at governmental regulation . Miltgen and Smith (2015) investigated how individuals' regulatory knowledge affects the perceived privacy regulatory protection, how it affects trust of organizations and governments and privacy risk concerns. The results of the study proved a significant relation between these constructs. Dommeyer and Gross (2003) on the

contrary, differentiate between knowledge and awareness in contrast to the study conducted by Miltgen and Smith (2015). The authors use the term knowledge as for example knowing how to conduct a name removal procedure from an online service, and the term awareness as being aware that such actions are possible. Furthermore, Dommeyer and Gross (2003) found in their study that knowledge of privacy practices reduces privacy concerns by establishing the perception of control.

2.3.2 Introducing two new constructs

The study conducted by Miltgen and Smith (2015) set out to measure knowledge, however only one measurement item was used which asked for the level of awareness individuals have regarding privacy regulations in the respondents country. With the separation of awareness and knowledge as mentioned by Dommeyer and Gross (2003), it appears that Miltgen and Smith (2015) were measuring awareness, not knowledge. The study of Miltgen and Smith (2015) does indicate some significant relationships between the awareness of privacy regulations, privacy risk concerns and trust. However, it was measured on a very high level of abstraction using only one item to measure the awareness of an entire regulatory framework. Due to the relevance of these relations, but missing separation between knowledge and awareness, we want to introduce a new construct. Capturing more detailed and clearly separated level of perceived privacy regulation awareness.

As previously mentioned, Dommeyer and Gross (2003) found that knowledge of privacy practices reduces privacy concerns, due to the perception of control. Furthermore, as new regulation (GDPR) aims to establish control and transparency (Goddard, 2017; Tankard, 2016), it can be argued that such regulation influence an individuals' privacy concerns and trust beliefs. Hence, we are interested in measuring the influence perceived privacy knowledge has on the constructs privacy concerns and trust beliefs. The constructs introduced above can be found in the research model, figure 2.2 alongside with already established constructs within the APCO Macro model. All constructs and covariates included in the research model will be discussed more in-depth in the upcoming sections.

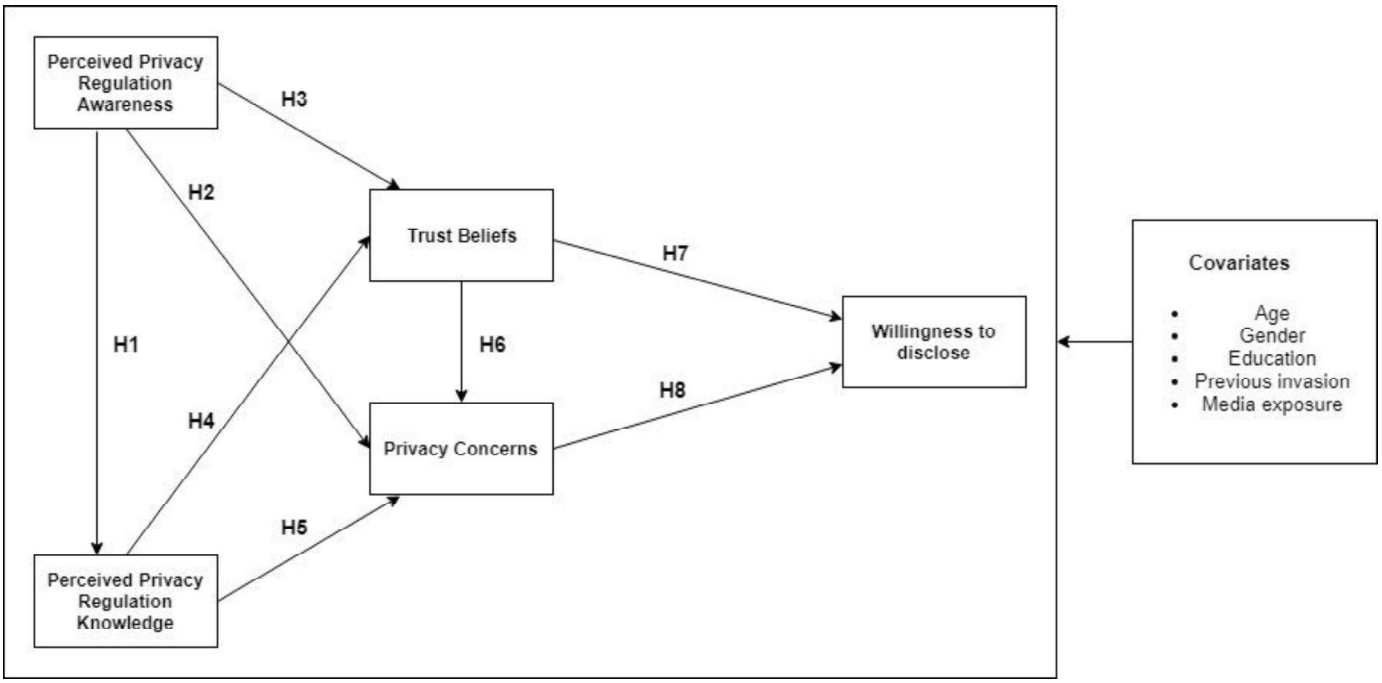


Figure 2.2 Research model

2.3.3 Perceived Privacy Regulation Awareness (PPRA)

Perceived Privacy Regulation Awareness (PPRA) is a construct which has not been recognized within the literature. Although, different studies concerning privacy and awareness can be found within the literature. Pötzsch (2008) base privacy regulation awareness on an individual's attention, perception and cognition of privacy. Malandrino et al. (2013, p. 279) on the other hand define privacy awareness as: "Encompassing the perception of: (1) Who is tracking and collecting personal information (2) When information is collected (3) What information other entities receive, store and use (4) How pieces of information are processed to potentially build detailed users' profiles."

Multiple studies have created instruments for measuring subjective awareness. Mukred et al. (2017) measured perceived awareness and its influence on behavioural intentions. However, this was within the context of IS adoption in the public healthcare sector of developing countries. The items for measuring awareness in the study of Mukred et al. (2017) were derived from Shareef, Kumar, Kumar, and Dwivedi (2011) who focused on an e-government adoption model. The authors measured the influence of perceived awareness among stakeholders on adopting an e-government. There is limited literature available within the specific context of privacy regulation awareness. The closest research we were able to find within this domain was conducted by Dommeyer & Gross (2003). The authors focus on the use of privacy protection strategies within the context of direct marketing and measure the objective awareness and knowledge of individuals involved in direct marketing. Likewise, Lwin et al. (2007) examined how privacy protection strategies are used by consumers based on their privacy concerns. One of their antecedents to privacy concerns which proven to be significant was governmental regulation.

Aforementioned, the study of Miltgen & Smith (2015) includes the measurement of the relationship between regulatory knowledge and both trust and privacy risk concerns through mediation. The study investigated both trust in regulators and companies within the same construct. Consequently, it is impossible to evaluate if the relations found leading to trust in their structural model are affecting trust in regulators, companies or both. For that reason, the relation between awareness and trust in companies or regulators separately cannot be relied on, since they are indistinguishable in their model.

As individuals who perceive to be more protected in terms of their personal data have less privacy concerns (Dommeyer & Gross, 2003; Lwin et al., 2007; Miltgen & Smith, 2015), we believe that perceived privacy regulation awareness will positively influence trust (Miltgen & Smith, 2015), as well as negatively influence privacy concerns. Furthermore, we believe that awareness will positively influence knowledge, since someone has to be aware of a regulation before they know how to deal with it. Resulting in the following hypotheses.

Hypothesis 1:
Perceived privacy regulation awareness will positively affect perceived privacy regulation knowledge.

Hypothesis 2:
Perceived privacy regulation awareness will negatively affect privacy concerns.

Hypothesis 3:
Perceived privacy regulation awareness will positively affect trust beliefs.

2.3.4 Perceived Privacy Regulation Knowledge (PPRK)

Knowledge can be separated into objective and subjective knowledge. Objective knowledge is the actual knowledge individuals possess regarding a subject. Whereas, subjective/perceived knowledge refers to the knowledge individuals perceive they possess (Zhu, Wei, & Zhao, 2016). Prior literature has examined how individuals' perception of regulatory policies are associated with their online privacy concerns. The study provided the insight that individuals' whom perceive governmental or organizational policies as weak will also have a higher level of privacy concerns. And would thereby likewise act accordingly, fabricate, protect, and/or withhold personal information (Lwin et al., 2007). Miltgen and Smith (2015) further elaborate on these findings and found that perceived regulatory protection positively effects trust in both companies and regulators enforcing the laws/policies. Moreover, the authors conclude that individuals' perceived knowledge of regulations is associated with higher levels of perceived privacy regulatory protection. Nevertheless, as mentioned in 2.3.2 it appears that Miltgen and Smith (2015) are measuring awareness rather than knowledge. However, the authors hypothetically intended to measure knowledge and stress its importance based on prior literature. Thus, it appears to be an interesting relation to examine. According to Dommeyer and Gross (2003), customers who have knowledge in regards to privacy practices and options for safeguarding their personal information can create a higher level of perceived control and therefore reduce privacy concerns.

Congruently with the literature, we suggest that individuals who perceive their knowledge on privacy regulations as high, will have a high level of trust towards organizations:

Hypothesis 4:
Perceived privacy regulation knowledge positively affects trust beliefs.

In accordance with the findings in prior literature, we also propose that perceived knowledge regarding privacy regulations may affect individuals' privacy concerns:

Hypothesis 5:
Perceived privacy regulation knowledge negatively affects privacy concerns.

2.3.5 Trust beliefs

Trust has many definitions within both online and offline contexts. However, in accordance with our delimitation this study looks to trust within E-commerce and hence an online context. McKnight and Chervany (2001, p. 46) define trusting beliefs within this context as: "Trusting beliefs means that one believes that the other party has one or more characteristics beneficial to oneself. In terms of characteristics, the consumer wants the e-vendor to be willing and able to act in the consumer's interest, honest in transactions, and both capable of, and predictable at, delivering as promised."

Trust is an often-used construct within privacy research (see table 2.1). Some studies have researched trust as a mediating variable between privacy concerns and behavioral intentions (Bansal & Gefen, 2015; Bansal & Zahedi, 2008; Metzger, 2004). Other studies looked into trust as an outcome of privacy concerns (Chellappa, 2008; Malhotra, Kim, & Agarwal, 2004). However to the best of our knowledge only one study looked into trust as an antecedent for privacy concerns (Belanger et al., 2002). More information concerning these studies can be found in table 2.1, which shows the authors, aim of the research, trust context, role of trust within the context, the dimensions of trust and the influence the factor trust has regarding its role. This table makes it clear that trust is an important factor within E-commerce, due to its high influences regardless of its role in the APCO Macro model (Antecedent, mediating variable, outcome).

Authors	Aim of Research	Trust Context	Role of Trust	Dimension of Trust	Influence of Trust
Metzger (2004)	This study proposes and tests a model of online information disclosure to commercial Websites	E-commerce websites	Mediating variable PC & Disclosure	Reliability Competent Benevolent Integrity	(β = .22, p < .01)
Bansal & Gefen (2015)	Measure the role of trust in websites based on privacy assurance mechanisms	E-commerce websites	Mediating variable PC & Disclosure	*(Items based on;)* Honesty Interest Opportunistic Service Level	(β = .50, p < .001)
Belanger, Hiller &	Measure trustworthiness in electronic commerce.	E-commerce websites	Antecedent for privacy	*(Items based on;)* Trustworthiness	(average r = .63, p< .01)

Smith (2002)				Commitment Reputation	
Chellappa (2008)	Consumers' Trust in Electronic Commerce Transactions based on privacy and security	E-commerce websites	Outcome from privacy	*(Items based on;)* Safety Reliability Problems	Not significant
Malhotra, Kim & Agarwal (2004)	Examine internet users' information privacy concerns (IUIPC) and their effects on trust beliefs (H1).	E-commerce websites	Outcome from privacy concerns	*(Items based on;)* Trustworthiness Truth Honesty Consistency	($\beta = .23$, $p < .001$)
Bansal & Zahedi (2008)	Examine the moderating role of privacy concern on how the quality of privacy policy statements and privacy assurance cues contribute to increased trust, and therefore disclosing private information online	Multiple contexts - websites	Mediating variable PC & Disclosure	*(Items based on;)* Design Professionality	Domain dependent
Dinev & Hart (2006)	Proposing and validating an extended privacy calculus model for E-commerce transactions	E-commerce websites	Antecedent for the willingness to provide personal information to transact on the internet	*(Items based on;)* Safety Reliability Competence	($r = .59$, $p<0.01$)

Table 2.1. Trust within previous research in the E-commerce domain

This study is focused on the role of trust as an antecedent to privacy concerns, similar to Belanger et al. (2002). If people have more trust in an organization, we expect that they will become less concerned regarding their privacy. We are furthermore interested in the role trust beliefs has on the willingness to disclose, since it positively influences behavioral intentions (Bansal & Gefen, 2015; Dinev & Hart, 2006). As a result, the following hypothesis are formed:

Hypothesis 6:
Trust beliefs negatively affect privacy concerns.

Hypothesis 7:
Trust beliefs positively affect willingness to disclose.

2.3.6 Privacy Concerns

Lowry, Cao, and Everard (2011) define privacy concern as the fear one may have of their privacy being compromised in an undesirable manner. Thus, concerns raised may be regarding who has access to information individuals have disclosed, and how this information is used (Lowry et al., 2011). To measure privacy concerns, several authors (see table 2.2) have used the multidimensional model created by Smith et al. (1996), called concern for information privacy (CFIP). The model consists of four dimensions, collection, error, unauthorized secondary use, and improper access. The instruments for measurement of privacy concerns were later tested and re-validated by Stewart and Segars (2002) whom verify the model with a sample size of 355 respondents. The results drafted form a confirmatory factor analysis represents consumers' attitude towards corporate use of information. The dimensions were created within an organizational context but have been applied within the area of information systems to measure information privacy concerns (Lowry et al., 2011).

Authors	Aim of the research	Dimensions of privacy concern
Angst & Agarwal (2009)	Examine if individuals can be persuaded to change attitudes towards electronic healthcare records and allow their medical information to be digitalized even when privacy concerns exist.	Collection Error Unauthorized secondary use Improper access
Dinev & Hart (2006)	Extending privacy calculus for E-commerce transactions.	(Based on:) Collection Error Unauthorized secondary use Improper access
Hann et al. (2007)	Examine individuals' information behavior and how it can be motivated.	Collection Error Unauthorized secondary use Improper access
Lowry, Cao & Everard (2011)	Investigate and validate relationship between self-disclosure technology use and culture.	Collection Error Unauthorized secondary use Improper access
Malhotra, Kim & Agarwal (2004)	Examine internet users' information privacy concerns (IUIPC). Operationalize IUIPC multidimensional notion. Propose and test IUIPC model.	Collection Error Unauthorized secondary use Improper access Control Awareness of privacy practices Global Information Privacy Concern
Son & Kim (2008)	Develop taxonomy for information privacy-protective responses (IPPR) and create nomological network for IPPR.	(Based on:) Collection Error Unauthorized secondary use Improper access

Table 2.2 Usage of CFIP for measuring privacy concerns in prior research

Dinev and Hart (2006) defined new items for measuring privacy concerns. The items were based of the CFIP created by Smith et al. (1996). The items Dinev and Hart (2006) developed were in their study used to measure privacy concerns within the E-commerce context. One of the authors, Dinev, also took part in creating the APCO Macro Model (Smith et al., 2011), thereby increasing the relevancy of their items for this study. The study found that their construct, internet privacy concerns, was affecting individuals' willingness to provide information to transact on the internet (Dinev & Hart, 2006). Likewise, prior literature has found similar results. That privacy concern affects individuals' willingness to disclose information. Individuals whom have more privacy concerns are less likely to be willing to disclose personal information (Dinev & Hart, 2006; Malhotra et al., 2004; Ozdemir et al., 2017). In accordance with this, we propose the following hypothesis:

Hypothesis 8:
Privacy concerns negatively affect the willingness to disclose.

2.3.7 Willingness to disclose

Correspondingly to the APCO Macro Model of Smith et al. (2011) behavioral reactions/intentions is often an outcome from privacy concerns (Dinev & Hart, 2006; Li, Sarathy, & Xu, 2010; Malhotra et al., 2004). An example of a behavioral reaction is willingness to disclose. The concept willingness to disclose defines the willingness people have to disclose personal information (Smith et al., 2011).

As an example, Metzger (2004) measured disclosure of personal information to an E-commerce website. The authors looked into the willingness to disclose different types of information online. Their model indicates the role of trust and past online behavior in the disclosure of personal information to a commercial website created for the study.

Dinev and Hart (2006) look to behavioral intentions as the willingness to provide personal information to transact on the internet. Their construct differentiates from what had been done within E-commerce in the past. The construct does not only look to the willingness of individuals to conduct a transaction online, but includes the perspective of the personal information needed to conduct the transaction. Consumers tend to be less willing to disclose their personal data when privacy concerns are high (Dinev & Hart, 2006; Lwin et al., 2007; Malhotra et al., 2004). We think that this study will show a similar effect.

2.3.8 Covariates

Previous research highlights several covariates influencing behavioral intentions and privacy concerns. Malhotra et al. (2004) included seven covariates to control for internet users' reaction to information privacy threats. Three of these control variables deal with demographics: sex, age and education. In addition, the authors include four variables concerning personal experiences: internet experience, how often subjects provide false information to a marketer, whether the subjects' privacy has been invaded in the past and the amount of times the subject has been exposed to media reports handling incidents of privacy invasion. The variables regarding privacy invasion where extracted from Smith et al. (1996) who differentiates previous personal experiences and media coverage influencing privacy concerns based on prior literature. Both

experience and knowledge turned out to be influencing privacy concerns significantly with beta coefficients of 0.16 and 0.22 respectively (Smith et al., 1996).

Similarly, Li et al. (2010) include five of the abovementioned control variables in their model which influence behavioral intention. The authors exclude education and how often subjects provide false information to a marketer, but further include privacy concerns as a control variable. However, none of their control variables were found to be significant. This study examines the influence of the demographical variables as mentioned by Malhotra et al. (2004) as well as the significant variables media exposure and previous privacy invasion by Smith et al. (1996) on all paths within the research model (figure 2.2).

3 Methodology

3.1 Research strategy

This thesis follows the linear process for quantitative research as proposed by Recker (2012). The process consists of five steps. First, generating models, theories and hypotheses. Second, developing instruments and methods for measurement. These instruments and measurements will mainly adhere from prior research. Third, the empirical data is collected. Fourth, data analysis including statistical modelling. And lastly, evaluation of the results.

The main part of this thesis is based on a quantitative research method, since we are interested in the relationship between different constructs. In addition, we used unstructured interviews combined with a thorough literature review concerning the chosen laws in order to build our constructs of interest: PPRK and PPRA. The entire research strategy can be found in figure 3.3, which focusses on the research steps and the techniques applied to achieve these steps.

The research strategy in figure 3.3 is divided in three steps: stage one, stage two and stage three. The purpose of stage 1 is mainly building the unexplored constructs that we want to test and find the right items to measure them, as well as the operationalization of already established constructs. Stage 2 focuses on pilot testing the model and testing if the items are reliable in measuring the constructs. This stage is finalised by performing the final survey after the revisions based on the pilot. The last stage deals with data cleaning and assessing of the validity and reliability, the results are shown and the hypothesis are answered.

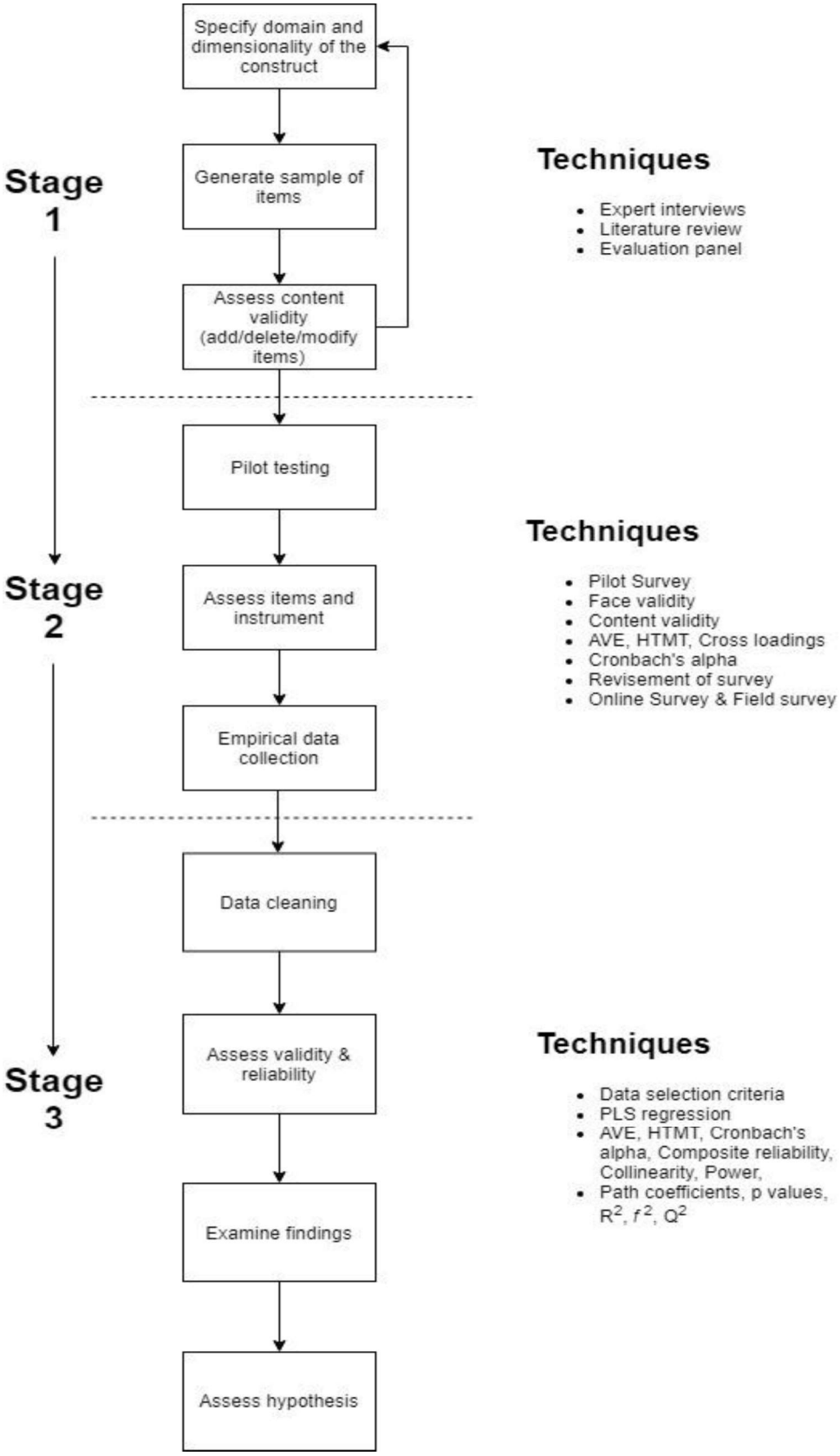


Figure 3.3. Research strategy

3.2 Data collection technique

3.2.1 Interviews

To be able to define our constructs (PPRA and PPRK) and thereby create valid items, interviews with experts were conducted. During these interviews, the goal was to identify governmental regulations that were essential to European privacy regulations. The interview focused around three main themes, active privacy laws, PPRA, and PPRK. The goal of the first theme was to extract information regarding which laws should be used to investigate our research questions and test our hypotheses. The second theme, PPRA, as well as the third theme, PPRK, strived to seek for possible new items and/or to validate our already selected items (grounded in prior literature) for the questionnaire. Additionally, for each theme we utilized questions to steer the conversation into the right direction, which can be seen in Appendix 2.

The interview was constructed in an open-ended manner, hoping for the interviewee to be able to elaborate and dwell into what they deem as important. The interviews were conducted face-to-face, at a location of the interviewees choice to make them feel more comfortable (Bhattacherjee, 2012). Moreover, inaccuracy is one of the flaws with interviews (Recker, 2012), thus the interviews were recorded and later transcribed. To further increase the information retrieved from the interviews, a literature review in regards of the active privacy regulations in the EU was carried out beforehand. This enable the possibility of follow-up questions, well aligned with the open-ended structure (Myers & Newman, 2007).

3.2.2 Questionnaire

Since the aim of the study is to determine the relations between privacy concerns, trust, PPRK, PPRA, and willingness to disclose, this study has utilized questionnaires to gather empirical data to test the extension proposed to the APCO Macro Model. By using questionnaires, the reach of the data gathering increased and we assured a high level of objectivity (Bhattacherjee, 2012).

The data collection was conducted with both self-administration where the survey was sent out via social networking sites, but also by field surveys conducted in public areas. Both techniques were used at the same time which lead to better utilization of the time available. The questionnaire used a Likert scale to capture the responses. The scale used stretches from one to seven, which is mentioned by Bhattacherjee (2012) as a viable scale. For the questionnaire, a control question was added to see how much attention the respondents were paying. This question required the respondent to select a specific question, failure to do so lead to the exclusion of their survey responses in the analysis, thereby increasing the validity of the study.

3.2.3 Sampling

For the interviews the respondents had to be selected with care to obtain rich and valid information from the interviews. A key feature that was sought after when selecting respondents was that they had extensive knowledge within EU governmental regulation regarding information privacy. It was important that the respondents had multiple years of experience of working with such regulations. In order to find such participants, universities, law firms and organizations

within compliance of information privacy laws were examined to find suitable respondents. The first respondent is a postdoctoral Lecturer at Lund's University with several publications as well as ongoing research within information privacy and information privacy law. The second respondent is another postdoctoral lecturer with a focus on EU law.

From the expert interviews it became apparent that a delimitation to EU residents rather than Sweden is more appropriate, as GDPR will enforced within all EU member states. Hence, our target population consists out of residents within EU member states. While it may be very hard to come up with a generalizable sample of this target population, a convenient sampling strategy was used to gather as many respondents as possible (Bhattacherjee, 2012). Respondents for the survey were gathered both online and in the field.

For the pilot study, data was collected at Lund University School of Economics and different public areas in Lund. For the final data collection (post-pilot), online survey responses were acquired by posting a message on the social networking websites *Facebook* and *Linked-in*. Regarding the field study responses were collected at Lund University School of Economics and in different trains within the Skåne area in Sweden.

3.3 Operationalization of Variables

To increase the construct validity, existing items and scales were used whenever possible. For the new constructs, the official directive of GDPR (chapter 3, rights of the data subject) from the EU parliament was used. The sources used in creating these items as well as the specific scale used for each construct are mentioned in table 3.3. All of the constructs within the model are of reflective nature, since the indicators are caused by the latent variables (Hair Jr, Hult, Ringle, & Sarstedt, 2016). A seven-point Likert scale is used to measure all constructs. We chose to use a 7 point Likert scale rather than a 5 point Likert scale while this is argued to increase reliability (Colman, Norris, & Preston, 1997).

*= Item is revised after pilot, **= Item is deleted after pilot, ***=Item is included after pilot			
Construct	**Items**	**Scale**	**Source**
Perceived Privacy Regulation Awareness (PPRA)	**I am aware that I, as an individual, have the right to…**	7-point Likert (1 = Not at all aware, 7 = Very aware)	Self-developed, based on: Article 3 GDPR (European Parliament, 2016)
	PRRA1: …be notified by who is collecting my personal data when my personal data is disclosed by me.		
	PRRA2: …be notified by who is collecting my personal data when the data is collected through a third party.		
	PPRA3: …request to see all the personal data that a service provider has stored regarding me as an individual.		
	PRRA4: …request for the correction of my personal data, stored by a service provider.		

	PPRA5: …request my personal data to be erased from an online service provider if certain conditions are met.		
	PPRA6: …restrict the processing of my personal data if certain conditions are met.		
	PPRA7: … request my personal data from one service provider and transfer the data to another provider. **		
	PPRA8: …protest to my personal data being processed by a service provider if certain conditions are met. **		
Perceived Privacy Regulation Knowledge (PPRK)	**When my personal data is being processed I know how…**	7-point Likert (1 = Not at all knowledgeable, 7 = Very knowledgeable)	Self-developed, based on article 3 GDPR (European Parliament, 2016)
	PPRK1: …I will be notified by who is collecting my personal data when my personal data is disclosed by me. *		
	PPRK2: …I will be notified by who is collecting my personal data when the data is collected through a third party. *		
	PPRK3: …to handle the procedure of requesting all the personal data that a service provider has stored regarding me as an individual. **		
	PPRK4: …to handle the procedure of requesting correction of my personal data, stored by a service provider. **		
	PPRK5: …to handle the procedure of requesting my personal data to be erased from an online service provider if certain conditions are met. **		
	PPRK6: …to handle the procedure of restricting the processing of my personal data if certain conditions are met. **		
	PPRK7: …to handle the procedure of requesting my personal data from one service provider and transfer the data to another provider. **		
	PPRK8: …to handle the procedure of protesting to my personal data being processed by a service provider if certain conditions are met. **		
Trust Beliefs (TB)	TB1: E-commerce websites are safe environments in which to exchange information with others.	7-point Likert (1 = Strongly disagree, 7 = Strongly agree)	(Dinev & Hart, 2006) Adapted to E-commerce context.
	TB2: E-commerce websites are reliable environments in which to conduct business transactions.		
	TB3: E-commerce websites handle personal information submitted by users in a competent fashion.		
	PC1: I am concerned that the information I submit on the Internet could be misused.	7-point Likert (1 = Strongly disagree, 7 =	(Dinev & Hart, 2006; Malhotra et

Privacy Concerns (PC)	PC2: I am concerned that a person can find private information about me on the Internet.	Strongly agree)	al., 2004; Smith et al., 1996)
	PC3: I am concerned about submitting information on the Internet, because of what others might do with it.		
	PC4: I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.		
Willingness to Disclose (WD)	**To what extent are you willing to use the Internet to do the following activities?**	7-point Likert (1 = Strongly disagree, 7 = Strongly agree)	(Dinev & Hart, 2006)
	WD1: Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information)		
	WD2: Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates)		
	WD3: Conduct sales transactions at E-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software) ***		
	WD4: Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)		
Control Variables (CV)	Demographics (Age, Gender, Education)		(Li et al., 2010; Malhotra et al., 2004)
	Privacy Invasion: How often have you personally been the victim of what you felt was an improper invasion of privacy? ***	7-point Likert (1 = Not at all 7 = Very often)	(Smith et al., 1996)
	Media Exposure: How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers? ***	7-point Likert (1 = Not at all, 7 = Very much)	(Smith et al., 1996)

Table 3.3. Operationalization of variables

3.4 Pilot study

Entering stage 2 of the research strategy (figure 3.3), we strived to ensure that the questionnaire was of good enough quality to gather data using it as an instrument, a pilot study was conducted. Respondents for this pilot study were acquired at three different public areas in Lund, Sweden. The pilot took place Friday the 20th of April 2018. Participants are not considered if they were residents outside the EU or if they did not answer the control question correctly. The control question was included at the later part of the questionnaire, which asked the participant to select the number 7. These filters resulted in removing two participants, which left us with 23 valid participants for the pilot study.

3.4.1 Descriptive statistics

The descriptive statistics of the valid responses in the pilot can be found in table 3.4. The sample represents a relatively young (Mean = 26.6) and highly educated group of respondents (Higher education = 87%). The gender distribution is more or less even, with slightly more females participants (52,2%).

Demographics	Descriptive statistics
Age	Mean = 26.6, Standard Deviation = 9, Skewness = 2.9
Gender	Male = 43.5%, Female = 52,2%, Prefer not to say = 4,3%
Completed education	High School = 13%, Higher Education = 87%

Table 3.4. Pilot descriptive statistics

3.4.2 Face validity

Face validity refers to whether an indicator seems to be a reasonable measure of its underlying construct (Bhattacherjee, 2012; Recker, 2012). To establish face validity, we asked the respondents questions to gather their subjective opinion on how they understood the questions and if they were asked in the right order. By doing so we changed the order of the questions upon request. Questions about PPRA & PPRK were asked in the end, while questions about disclosure and privacy concerns were asked in the beginning of the questionnaire, based on the respondents' feedback. In this way the respondents felt more at ease with having more general questions in the beginning rather than starting with them scaling their knowledge and awareness on regulations. Furthermore, we included a definition on the word service providers and gave an example for the questions that include if certain criteria are met, since this was not clear for some respondents. All constructs except for PPRK and PPRA were taken from literature and appeared to have established face validity. However, the items were not verified again by any experts. The new constructs, PPRA and PPRK on the other hand, were validated by experts who suggested the removal of two items within PPRK. Changes were made accordingly.

3.4.3 Content validity

To avoid measurement errors, one should make sure that the measurement items are capturing the whole of the construct they set out to measure (Bhattacherjee, 2012; Recker, 2012). Content validity was increased by using already existing constructs and their instruments wherever possible. We furthermore asked two experts within the privacy field to validate our instrument concerning the newly formed constructs, as suggested by both Recker (2012) and Bhattacherjee (2012). The feedback of these experts made us change our instrument. At first, we only wanted to measure subjective awareness and knowledge on an abstract level of GDPR and E-privacy. However, after extensive sessions with subject matter experts we decided to focus solely on GDPR and measure in-depth subjective awareness and knowledge regarding this regulation, since this was perceived to be interesting and the E-privacy regulation was not expected to be launched on time (Appendix 3, I1R29, Appendix 3, I1R11). After further revising the items for PPRA and PPRK together with a researcher of the department, it was noted that the items were quite similar which could lead to the constructs measuring the same thing. This strengthened the reasoning of creating new items, less abstract, focusing on specific articles of the GDPR within chapter 3, "Rights of the data subject".

When new items were created, these items were sent out to the subject matter experts again to validate that the items actually would measure what they are intended to. This aligns with Lawshe (1975), who mentions that content validity can be established through evaluation panels. The feedback received, consisted of some critique regarding the chosen wording. Therefore, the items were adjusted accordingly to the suggestions of the experts. These changes included the changes of PPRK1 and PPRK2 which were not clear according to the evaluation panel. Furthermore, we changed the wording in all PRRK items from 'is being disclosed' to 'is processed' which was suggested to be more accurate. However, these last changes were made after the pilot, nevertheless the changes were included in the final survey.

3.4.4 Construct validity

Construct validity considers the validity of the operationalization or measurement between constructs. This validity is assessed by looking to the convergent, and discriminant validity (Recker, 2012). Convergent validity refers to how close a measure relates to the construct which it sets out to measure (Bhattacherjee, 2012). To measure the convergent validity, the average variance extracted (AVE) was looked to. According to Joe F Hair, Ringle, and Sarstedt (2011), convergent validity is deemed as sufficient if the AVE is 0.5 or higher. As can be seen in table 5, the lowest value found was 0.635. Thus, we concluded that the convergent validity was sufficient.

Construct	AVE
PPRA	0.784
PPRK	0.635
PC	0.864
TB	0.751
WD	0.651

Table 3.5. Average variance extracted

As we created a research model, including two new constructs, it is important that we can assure that the constructs are distinct and not just duplicates of each other. This can be measured through discriminant validity (Voorhees, Brady, Calantone, & Ramirez, 2016). Discriminant validity is defined by Churchill Jr (1979, p. 70) as the following: "Discriminant validity is the extent to which the measure is indeed novel and not simply a reflection of some other variable".

When determining if discriminant validity was established or not, the hetrotrait-monotrait ratio of correlations (HTMT) was used. The HTMT is the most recent addition to discriminatory validity used within variance-based structural equation modelling (Voorhees et al., 2016). Henseler, Ringle, and Sarstedt (2015) who proposed the HTMT, argue that both the Fornell-Larcker criterion and cross-loadings are not suitable for measuring discriminant validity as they fail to detect this validity in common research situations. Thus, these methods were disregarded for determining discriminant validity. Prior literature mentions that either 0.85 or 0.90 can be used as a threshold, where a value higher than the threshold indicates that discriminant validity is not established (Henseler et al., 2015). Hence, for the evaluation of discriminant validity, we relied on a stricter threshold of 0.85. The results from the HTMT conducted on the pilot survey can be found in table 3.6. As no correlations were of value 0.85 or higher, discriminant validity was established.

	PPRA	PPRK	PC	TB	WD
PPRA					
PPRK	0.782				
PC	0.145	0.162			
TB	0.521	0.317	0.0515		
WD	0.467	0.236	0.465	0.637	

Table 3.6. Hetrotrait-monotrait ratio of correlations

Although the discriminant validity was sufficient, we found that both the correlation between PPRK and PPRA as well as the correlation between WD and TB are close to the threshold with respectively 0.782 and 0.637. For that reason, we took a closer look to the cross-loadings of these particular construct items, with the purpose of improving them for the final survey. Although some of the cross loadings between the items of PPRA and PPRK are close, the concepts of awareness and knowledge are somewhat related which may result in higher correlations. As previously mentioned, cross-loadings is not a suitable method for determining discriminant validity (Henseler et al., 2015). Therefore, we did not solely rely on the outcomes of the cross loadings, but rather use them to improve the HTMT values by looking at individual items. That being said, we investigated the cross loadings of items that were close to other constructs, more specific PPRA1, PPRA2, PPRK1, PPRK2, PPRK7 and PPRK8, see table 3.7.

	PPRA	PPRK	Trust belief	Willing-ness to disclose
PPRA1	**0.925**	0.769	0.447	0.289
PPRA2	**0.892**	0.775	0.353	0.249
PPRA3	**0.926**	0.668	0.64	0.397
PPRA4	**0.909**	0.67	0.5	0.363
PPRA5	**0.909**	0.67	0.4	0.435
PPRA6	**0.929**	0.598	0.379	0.417
PPRA7	**0.664**	0.373	0.063	0.264
PPRA8	**0.897**	0.661	0.451	0.429
PPRK1	0.615	**0.721**	0.126	0.022
PPRK2	0.576	**0.713**	0.102	0.032
PPRK3	0.755	**0.953**	0.317	0.22
PPRK4	0.576	**0.863**	0.315	0.239
PPRK5	0.721	**0.909**	0.35	0.188
PPRK6	0.701	**0.941**	0.319	0.127
PPRK7	0.416	**0.496**	-0.062	0.055
PPRK8	**0.663**	**0.663**	-0.032	0.274
TB1	0.483	0.386	**0.912**	0.603
TB2	0.605	0.349	**0.884**	0.429
TB3	0.222	0.185	**0.800**	0.298
WD1	0.185	0.147	0.186	**0.819**
WD2	0.369	0.25	0.44	**0.915**
WD4	0.397	0.091	0.575	**0.667**
Note: Highest value in bold				

Table 3.7. Cross-loadings of PPRA, PPRK, TB & WD

We changed the wording of the PRRK items from 'I am knowledgeable on' to 'I know' to distinguish them even more from the PPRA items. In addition, we decided to remove the items PPRK1 and PPRK2, while they were perceived to be unclear by the evaluation panel and they were hard to be distinguished from PPRA1 and PPRA2, since it is hard to measure the knowledge of being notified by something which is too closely related to awareness. Although this change negatively affected the discriminant validity (HTMT between PPRA & PPRK increased to 0.810), it positively affected the content validity.

Furthermore, the item PPRK8 loaded with the same value on both PPRK and PPRA in its cross-loadings. However, we did not want to delete this item as we consider it as essential when measuring knowledge regarding GDPR. Thus, we changed the wording of the item in order to attempt to differentiate it from PPRA. More specifically we changed the word 'object' to protest to make it clearer. Regarding PPRA7 & PPRK7, we changed the word 'transmit' to transfer, to make the question clearer. In addition, we added the item WD3, while we found it missing in the pilot.

3.4.5 Internal consistency

To assess the internal consistency and therefore the reliability of the items measuring the same construct, Cronbach's alpha is suggested (Bhattacherjee, 2012; MacKenzie, Podsakoff, & Podsakoff, 2011). Table 3.8 shows the output of Cronbach's alpha for our items. All items are above the common threshold of 0.7, indicating that all items used to form the constructs are acceptable (MacKenzie et al., 2011; Tavakol & Dennick, 2011).

Construct	Cronbach's Alpha
PPRA	0.961
PPRK	0.939
Privacy Concerns	0.948
Trust Beliefs	0.833
Willingness to disclose	0.721

Table 3.8. Cronbach's Alpha

Authors have argued that Cronbach's Alpha tends to underestimate internal consistency and is sensitive to the number of items within a construct (Hair Jr et al., 2016). The authors mention that Cronbach's Alpha can be used as a more conservative measure for internal consistency. However, they suggest that composite reliability is preferred to measure the internal consistency within PLS-SEM (Hair Jr et al., 2016). Therefore, the composite reliability was also examined to ensure that it was within acceptable thresholds. As the composite reliability of our constructs all measure above 0.7 (see table 3.9), we find that their internal consistencies are acceptable (Shook, Ketchen, Hult, & Kacmar, 2004).

Construct	Composite reliability
PPRA	0.966
PPRK	0.919
Privacy Concerns	0.962
Trust Beliefs	0.900
Willingness to disclose	0.847

Table 3.9. Composite Reliability

3.5 Generalizability and Ethics

3.5.1 Generalizability

As the population for this study includes all individuals affected by the GDPR, any resident within a European member state was a valid respondent. Nevertheless, with the selected non-probability sampling strategy (convenience sampling), generalizability becomes lacking. The questionnaires were sent out on specific social media platforms and handed out in specific areas, indicating that groups of individuals have been left out. This further limits the generalizability of the study (Bhattacherjee, 2012).

Additionally, the possible impact of a non-response is hard to measure. This may be harmful for the generalizability (Bhattacherjee, 2012). For the field surveys, the response rate is estimated to roughly 70-80%. However, for the survey distributed online, it was impossible to

measure how many individuals had actually seen the survey. Nevertheless, it is expected that the response rate was much lower than the field survey, while the online survey had a possibility to reach out to more respondents than the amount of answers received. Consequently, it is plausible that non-response bias is further affecting the generalizability.

3.5.2 Ethics

For contacting possible respondents for the pre-study, emails were utilized. The emails contained a short description of who we are, what the aim of the study was, and why we would like to interview them. Aligned with the ethical principles of research mentioned by Bhattacherjee (2012), the possible participants were free to decline the offer without any negative impact. The participants who agreed on an interview were later engaged in a verbal agreement that the interview would be recorded, transcribed, and later included in the final report. The respondents were also enlightened that their identity would be anonymized in the final report, which also is mentioned by Bhattacherjee (2012) as an important factor of ethical principles to assure the respondents future well-being.

Furthermore in line with Bhattacherjee (2012) we understood our ethical obligation in providing all results and findings, without letting out information that did not suit our research. Therefore, we provided the entire transcripts of the interviews in the appendix (appendix 3 and 4).

The data provided by the respondents of the questionnaire survey was kept completely anonymous. This means that the answers of a respondent cannot be traced back to the respondent (Bhattacherjee, 2012). Confidentiality is furthermore guaranteed to respondents, we will not publish results that could be traced back to the individual answering the survey. When inviting respondents to answer the survey, we included a description of the purpose for the study. This further enabled the respondents to make an active decision whether they wanted to participate or not. To strengthen this aspect, we included a text on top of the survey indicating the purpose of this research and the way their data is being handled. This research is furthermore in line with the AIS code of conduct stating an ethical way of doing research within the IS field (Bhattacherjee, 2012).

3.6 Analytical tools

3.6.1 Structural Equation Modeling (SEM)

This study used SEM to validate the proposed model. SEM can be seen as a collection of statistical techniques allowing the examination of a set of independent variables and one or more dependent variables (Ullman & Bentler, 2003). Within SEM two main branches exist, covariance based SEM (CB-SEM) and partial least squares SEM (PLS-SEM). As this study is predictive in its nature, since its aim is to examine newly formed constructs, PLS-SEM is preferred (Joe F Hair et al., 2011). PLS-SEM enables the estimation of latent variables from observed variables (Ullman & Bentler, 2003). In order to conduct a PLS-SEM analysis, the analytical software SmartPLS was used. Furthermore, SPSS was utilized to calculate and visualize the descriptive statistics of the different data samples.

4 Data analysis

Collection of the online survey data took place from Tuesday the 24th of April 2018 at 17:20 until Friday the 27th of April 2018 at 12:00, within this timeframe we received 143 responses. The field data was collected on Wednesday the 25th of April 2018 this resulted in an additional 100 responses. Leading to a total of 243 participants.

4.1 Data cleaning

The data was cleaned before any statistical tests were performed, advancing to stage 3 of our research strategy (figure 3.3). This preliminary data cleaning expands the validity and quality of our results. When selecting valid data, we handled 4 criteria:

1. The participant needs to be a resident in an EU member state
2. The control question must be answered correctly
3. There should be no missing data
4. There should be at least some deviation in the respondents' answers (std > 0)

These requirements resulted in the exclusion of 26 responses, we therefore acquired 217 valid responses. The percentage of deleted answers according to the requirements per sample can be found in table 3.10. No data was removed regarding criteria 4, since the lowest standard deviation for a respondent was 0.751 which we deem as acceptable.

Sample	Responses	Deleted after criteria 1	Deleted after criteria 2	Deleted after criteria 3	Deleted after criteria 4	Valid responses
Online	N=143	8 (5.6%)	8 (5.6%)	0 (0%)	0 (0%)	127 (88.8%)
LUSEM	N=28	0	1 (3.6%)	0 (0%)	0 (0%)	27 (96.4%)
Train	N=72	0 (0%)	1 (1.4%)	8 (11.1%)	0 (0%)	63 (87.5%)
Total	N= 243	8 (3.3%)	10 (4.1%)	8 (3.3%)	0 (0%)	217 (89.3%)

Table 3.10. Overview data cleaning per sample

4.2 Descriptive statistics

Table 4.11 shows an even distribution according to the gender of the respondents. Out of the 217 valid participants 108 are female (49.8%), 107 are male (49,3%) and 2 respondents preferred not to mention their gender (0.9%). The table shows the differences in gender for the different samples. The sample in LUSEM had almost 3 times more female than male participants, respectively 19 and 7. Females were also the majority in the train sample (38) over 25 male participants. However, the online sample consisted out of more male participants (75) versus 51 female participants. Resulting in a nearly even gender distribution for the combined samples.

			Gender			Total
			Prefer not to say	Female	Male	
Location	LUSEM	Count (N)	1	19	7	27
		% of Total	0.5%	8.8%	3.2%	1 %
	Train	Count (N)	0	38	25	63
		% of Total	0.0%	17.5%	11.5%	29.0%
	Online	Count (N)	1	51	75	127
		% of Total	0.5%	23.5%	34.6%	58.5%
Total		Count (N)	2	108	107	217
		% of Total	0.9%	49.8%	49.3%	100.0%

Table 4.11. Location * Gender Crosstabulation

The majority of the participants had completed a higher education (71%), the other 29% of the participants completed at least their high school, no participants had not completed high school, see table 4.12. Some differences regarding education can be found for the different samples. Both the online and the train sample consisted out of the majority of the participant having a completed higher education, while the majority in the LUSEM sample only completed high school. A possible explanation for this can be that participants in this sample were attending higher education at the moment.

			Education		Total
			High school	Higher education	
Location	LUSEM	Count (N)	17	10	27
		% of Total	7.8%	4.6%	12.4%
	Train	Count (N)	13	50	63
		% of Total	6.0%	23.0%	29.0%
	Online	Count (N)	33	94	127
		% of Total	15.2%	43.3%	58.5%
Total		Count (N)	63	154	217
		% of Total	29.0%	71.0%	100.0%

Table 4.12. Location * Education Crosstabulation

Table 4.13 shows the mean age of the participants. The mean age of the total sample was 28.35 with a standard deviation of 10.27. The mean age for the online and the LUSEM sample were quite close with 26.26 and 24.07 respectively, nevertheless the standard deviation for the online sample was twice as high compared to the LUSEM sample. The mean age of the total sample therefore increased by the higher mean for the train sample (34.40). However, this sample also had the highest standard deviation (12.97).

Location	Mean	N	Std. Deviation
LUSEM	24.07	27	4.10
Train	34.40	63	12.97
Online	26.26	127	8.24
Total	28.35	217	10.27

Table 4.13. Age of participants

4.3 Validity

During the pilot study, face validity and content validity were established. Since new data had been collected, the construct validity needed to be revised once more. To assess the convergent validity, the average variance extracted was used (Joe F Hair et al., 2011). In table 4.14 the results can be seen. It is acknowledged that the AVE for PPRA is much lower than in the pilot study (AVE = 0.784) and both PPRA and WD are close to the threshold of 0.5. However, the constructs do uphold the suggested threshold proving that convergent validity is sufficient (Joe F Hair et al., 2011).

Construct	AVE
PPRA	0.555
PPRK	0.769
PC	0.733
TB	0.728
WD	0.538

Table 4.14. Average variance extracted

To determine if discriminant validity between constructs was established, HTMT was looked to. As can be seen in table 4.15, the highest correlation is between trust beliefs and willingness to disclose which has a value of 0.695. This led to the conclusion that a satisfactory level of discriminatory validity was established, with a threshold of 0.85 as recommended by Henseler et al. (2015).

	PC	PPRA	PPRK	TB	WD
PC					
PPRA	0.090				
PPRK	0.076	0.582			
TB	0.401	0.072	0.059		
WD	0.381	0.103	0.079	0.695	

Table 4.15. HTMT ratio of correlations

4.4 Reliability

To examine the internal consistency reliability of the measurements used, Cronbach's Alpha and composite reliability were looked to. All constructs pass a threshold on Cronbach's Alpha of 0.7 (see table 4.16), which indicates that a consistency among the measures exist (MacKenzie et al., 2011; Tavakol & Dennick, 2011). It is noted that willingness to disclose is barely passing

the threshold (0.704) of the Cronbach's Alpha. However, as mentioned in the pilot study (chapter 3.4) it can be argued that Cronbach's Alpha tends to underestimate internal consistency (Hair Jr et al., 2016). Looking to composite reliability, which according to Hair Jr et al. (2016) is suggested for PLS-SEM, the lowest value found is on willingness to disclose at the value of 0.820. Thereby, the construct passes the threshold of 0.7 with much more margin compared to its Cronbach's Alpha value. As the constructs pass both thresholds, we conclude that internal consistency is present.

Construct	Cronbach's Alpha	Composite reliability
PC	0.878	0.916
PPRA	0.920	0.905
PPRK	0.946	0.952
TB	0.814	0.889
WD	0.704	0.820

Table 4.16. Cronbach's Alpha and Composite reliability

4.5 Collinearity and Common method bias

To assure that collinearity between constructs in not too high, which would mean that the constructs are measuring the same thing, the inner variance inflation factor (VIF) was examined (Hair Jr et al., 2016). The yielded results can be seen in table 4.17, where the highest value is 1.454. To ensure that no constructs need to be eliminated or merged, as the highest tolerated VIF value is 5.00 (Joe F Hair et al., 2011; Hair Jr et al., 2016). Therefore, no action needed to be taken.

	PC	PPRA	PPRK	TB	WD
PC					1.130
PPRA	1.454		1.000	1.453	
PPRK	1.453			1.453	
TB	1.002				1.130
WD					

Table 4.17. Collinearity (VIF)

The VIF can also be used when determining if any common method bias (CMB) is affecting the results from the PLS-SEM analysis. In the context of PLS-SEM, CMB sees to if the results are caused by the measurement method rather than the causes and effects (Kock, 2015). To assess the CMB, a new column of random data (integer ranging from 1-7) was added to the empirical data. This data was used to create a dummy latent variable in SmartPLS, to which all latent variables were set to point. This method suggested by Kock and Lynn (2012), also referred to as a full collinearity test, enables the assessment of CMB through these VIF values. The results can be seen in table 4.18, where "DUMMY" refers to the new dummy latent variable. With the highest VIF value being much lower than the suggested threshold of 3.3 (Kock, 2015; Kock & Lynn, 2012), we concluded that common method bias was not present.

	DUMMY
DUMMY	
PC	1.039
PPRA	1.023
PPRK	1.024
TB	1.032
WD	1.062

Table 4.18. Full collinearity test

4.6 Model fit

SmartPLS provides different measurements to examine model fit (SRMR, d_ULS, d_G1, d_G2, Chi-Square and NFI). However, caution needs to be taken when interpreting these results, since further research is needed when it comes to examining model fit using PLS-SEM (Hair Jr, Sarstedt, Ringle, & Gudergan, 2017). We therefore do not fully rely on these results when it comes to the model fit. We focus on the SRMR and the NFI values, since the Chi-Square value in itself is not sufficient to determine model fit and the exact tests (d_ULS, d_G1 and d_G2) are argued to offer little value (Joseph F Hair, Hult, Ringle, Sarstedt, & Thiele, 2017).

The SRMR value is described by Henseler, Hubona & Ray (2016) as the square root of the sum of the squared differences between the model implied and the correlation matrix. The SRMR for the estimated model is 0,063, see table 4.19. This value is below the recommended threshold of 0,08, indicating appropriate model fit (Hu & Bentler, 1999). The NFI measurement on the other hand indicates the normed fit index. Bentler & Bonett (1980) define NFI as 1 – the Chi-Square value of the proposed model divided by the Chi-square values of the null model, resulting in a value between 0 and 1. The closer to 1 the better the fit (Bentler & Bonett, 1980). A rule of thumb for the NFI threshold regarding acceptable fit is set to ≥ 0.9 (Hulland, Chow, & Lam, 1996). Indicating that our model does not show an acceptable fit (0.8), see table 4.19. However, we are not too worried, since the NFI value has been widely criticized within literature for not penalizing for model complexity (Bentler, 1990; Henseler et al., 2016; Hsu, Chen, & Hsieh, 2006). More parameters would therefore result in a better NFI, making it a non-reliable measurement for PLS-SEM at the moment. A non-normed fit index (NNFI) partially solves the disadvantages of NFI, making it a more suitable measurement (Bentler, 1990). Nevertheless, such a measurement is not available within SmartPLS at the moment.

	Saturated Model	Estimated Model
SRMR	0.062	0.063
d_ULS	1.259	1.272
d_G1	0.844	0.844
d_G2	0.638	0.638
Chi-Square	783.198	783.745
NFI	0.8	0.8

Table 4.19. Model fit measurements

4.7 Power Analysis

A power analysis was conducted to verify if the model was strong enough to detect significant effects. Outcome of the Cohen D Post-hoc statistical power analysis showed that the observed statistical power was 0.999 (N=217, $\alpha = 0.05$, effect size = 0.15), which is higher than the threshold of 0.8 (Cohen, 1988). Indicating high statistical power, if there are at least medium significant effects they will be detected. However, in order to detect smaller effect sizes, more statistical power is needed.

5 Results

This chapter will investigate the results of the structural model. It will take into account the path coefficients, p values, R^2, f^2 and the Q^2 values to determine the influence of the paths. The formed hypothesis in chapter 2 will be accepted or rejected based on these values. The full structural model can be found in figure 5.4. Furthermore, multiple MGA's were performed to test the model according to different context based on the covariates.

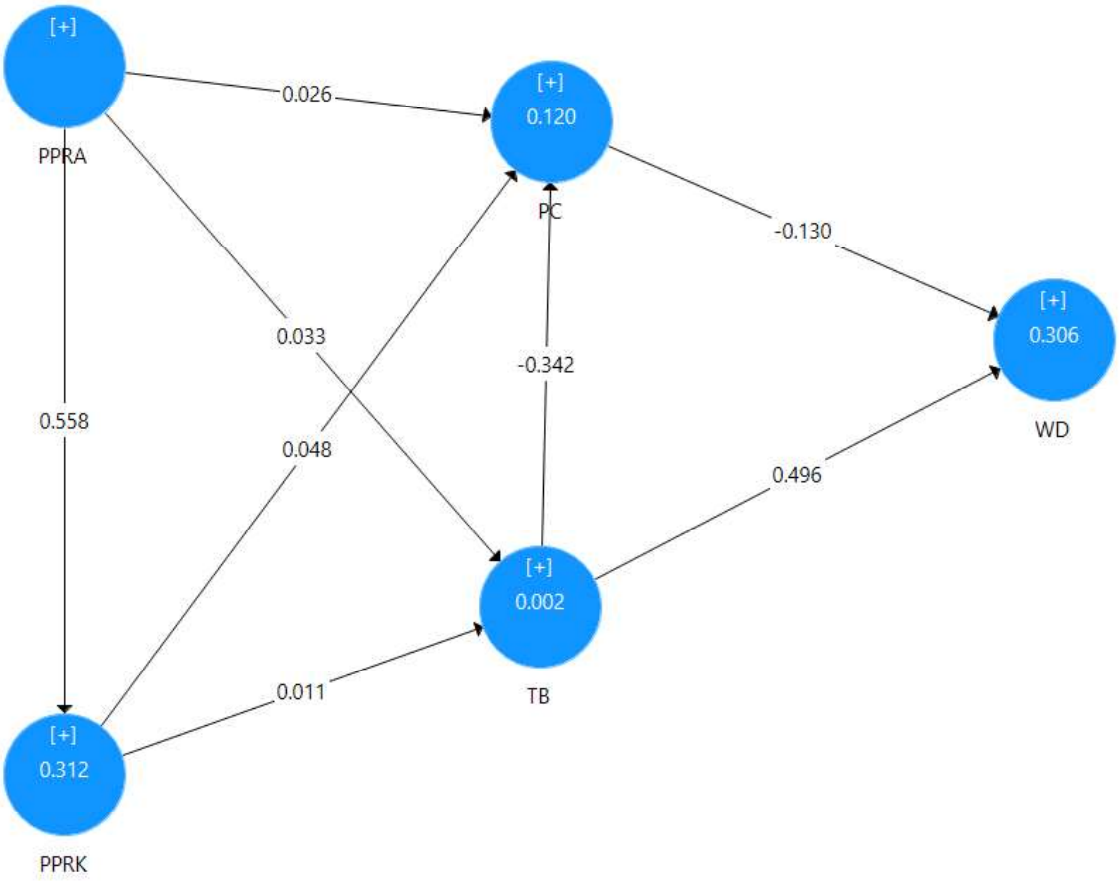


Figure 5.4. Structural model

5.1 Path coefficients (β)

In order to look to the path coefficients of the structural model, the bootstrapping technique within SmartPLS was utilized. This resampling technique draws subsamples from the original data and estimates models for every subsample (Joe F Hair et al., 2011; Hair Jr et al., 2016). The bootstrapping was ran with 5000 samples as suggested by Hair Jr et al. (2016). The results of the path coefficients along with the p values and significance can be seen in table 5.20. The results indicate that four out of the eight paths are significant.

Path	β	p Values	Significance
PC -> WD	-0.130	0.028	**
PPRA -> PC	0.026	0.735	NS
PPRA -> PPRK	0.558	0.000	***
PPRA -> TB	0.033	0.774	NS
PPRK -> PC	0.048	0.534	NS
PPRK -> TB	0.011	0.913	NS
TB -> PC	-0.342	0.000	***
TB -> WD	0.496	0.000	***
Note: NS = Not significant *p < .10. **p < .05. ***p < .01.			

Table 5.20. Significance Testing Results of the Structural Model Path Coefficients

5.2 Mediating effects

Mediation occurs when a construct is affected not only by a direct effect (x→z) but also indirectly through a so called mediating construct (x→y→z, y = mediator). When mediation exists, a total effect can be calculated which is calculated as the indirect effect (x→y * y→z) plus the direct effect (x→z) (Hair Jr et al., 2016). We found that PC significantly mediates the effect between TB and WD (t = 9.198 > 1.96, CI = 95%). Looking further into this mediation, we find that the indirect effect is significant (t = 2.009) as well as the direct effect (TB --> WD, t = 7.806) indicating that the mediation is a partial mediation (Hair Jr et al., 2016). The structural model furthermore does not include any other significant mediators at the 95% CI level (t > 1.96), see table 5.21.

	Mediating effect 1	Mediating effect 2	Mediating effect 3	Mediating effect 4	Mediating effect 5	Mediating effect 6
Mediator tested	PPRK	TB	PC	TB	PC	PC
Dependent Variable	PC	PC	WD	PC	WD	WD
Path (a)	PPRA --> PPRK	PPRA --> TB	PPRA --> PC	PPRK --> TB	PPRK --> PC	TB --> PC
Path (b)	PPRK --> PC	TB --> PC	PC --> WD	TB --> PC	PC --> WD	PC --> WD
β (a)	0.559	0.020	0.120	0.031	0.101	-0.340
β (b)	0.060	-0.344	-0.296	-0.345	-0.298	0.496
Direct effect (c)	0.053	0.102	-0.055	0.088	-0.050	-0.130
Indirect effect (a*b)	0.034	-0.007	-0.036	-0.011	-0.030	0.044
Total effect (a*b+c)	0.087	0.095	-0.09	0.077	-0.080	0.540
t-value	0.692	0.698	0.637	0.709	0.618	9.198

Table 5.21. Mediating effects

5.3 Coefficient of Determination (R^2)

The R^2 value is an often used measure to evaluate the structural model, indicating the predictive accuracy (Hair Jr et al., 2016). It furthermore represents the amount of variance in the endogenous construct explained by all connected exogenous constructs (Hair Jr et al., 2016). Table 5.22 shows the R^2 values of the endogenous constructs.

Construct	R^2
PC	0.120
PPRK	0.312
TB	0.002
WD	0.306

Table 5.22. R-Square of secondary constructs

- **PC:** 12% of the variation in Privacy Concerns can be explained by the constructs: Trust beliefs (TB), Perceived Privacy Regulation Awareness (PPRA) and Perceived Privacy Regulation Knowledge (PPRK).
- **PPRK:** 31% of the variation in Perceived Privacy Regulation Knowledge can be explained by the construct Perceived Privacy Regulation Awareness (PPRA).
- **TB:** 0.2% of the variation in Trust beliefs can be explained by the constructs: Perceived Privacy Regulation Awareness (PPRA) and Perceived Privacy Regulation Knowledge (PPRK).
- **WD:** 30.6% of the variation in Willingness to Disclose can be explained by the constructs: Trust beliefs (TB) and Privacy Concerns (PC).

5.4 Effect size (f^2)

To examine the impact that individual exogenous constructs have on a endogenous construct, their effect size (f^2) was examined (Hair Jr et al., 2016). Three different thresholds are suggested for the examination, 0.02, 0.15, 0.35, which represent small, medium, and large effects respectively (Hair Jr et al., 2016; Selya, Rose, Dierker, Hedeker, & Mermelstein, 2012). The effect sizes of this study for each path can be found in table 5.23.

Path	f^2
PC -> WD	0.022
PPRA -> PC	0.001
PPRA -> PPRK	0.453
PPRA -> TB	0.001
PPRK -> PC	0.002
PPRK -> TB	0.000
TB -> PC	0.133
TB -> WD	0.313

Table 5.23. Effect size

5.5 Predictive relevance (Q^2)

In addition to the R^2 values we examined the Stone-Geisser's Q^2 value (Geisser, 1974; Stone, 1974). This test examines if the model succeeds in predicting each endogenous latent construct's indicators (Joe F Hair et al., 2011). In order to get these values from smartPLS we used the blindfolding procedure, the values can be found in table 5.24. Any value above 0 indicates that the model has predictive relevance regarding a particular endogenous construct. Table 5.24 shows that all endogenous constructs except for TB have predictive relevance.

Construct	Q^2
PC	0.078
PPRA	
PPRK	0.231
TB	-0.006
WD	0.154

Table 5.24. Predictive relevance

5.6 Assessing the hypotheses

After the examination of the path coefficients, coefficient of determination, effect size, and predictive relevance, we were able to assess the hypotheses formulated from the research question, see table 5.25. The hypothesis H1 is supported ($\beta = 0.558$, $p = 0.000$, $f^2 = 0.435$), perceived privacy regulation awareness is displaying to have a large effect on perceived privacy regulation awareness. H2 was in our study rejected ($\beta = 0.026$, $p = 0.735$, $f^2 = 0.001$), not providing a significant relation between perceived privacy regulation awareness and privacy concerns. H3 was rejected ($\beta = 0.033$, $p = 0.774$, $f^2 = 0.001$) on the same grounds as H2, proving that perceived privacy regulation awareness in our study does not significantly affect trust beliefs. Hypothesis H4 was also rejected ($\beta = 0.011$, $p = 0.913$, $f^2 = 0.002$), indicating that perceived privacy knowledge does not have a significant effect on trust beliefs. H5 was rejected ($\beta = 0.048$, $p = 0.534$, $f^2 = 0.002$) providing the insight that perceived privacy regulation knowledge does in our study not necessarily influence privacy concerns. H6 has been supported ($\beta = -0.342$, $p = 0.000$, $f^2 = 0.113$) as our results display a significant relationship with a small effect that trust beliefs negatively affect privacy concerns. H7 is supported ($\beta = 0.496$, $p = 0.000$, $f^2 = 0.313$), trust beliefs positively affect willingness to disclose. H8 is accepted ($\beta = -0.130$, $p = 0.028$, $f^2 = 0.022$) indicating that privacy concerns significantly influence willingness to disclose.

Hypothesis		Supported/ Rejected	β	p Value	Significance	f^2
H1	Perceived privacy regulation awareness will positively affect perceived privacy regulation knowledge.	Supported	0.558	0.000	p < 0.01	0.435
H2	Perceived privacy regulation awareness will negatively affect privacy concerns.	Rejected	0.026	0.735	NS	0.001
H3	Perceived privacy regulation awareness will positively affect trust beliefs.	Rejected	0.033	0.774	NS	0.001
H4	Perceived privacy regulation knowledge positively affects trust beliefs.	Rejected	0.011	0.913	NS	0.001
H5	Perceived privacy regulation knowledge negatively affects privacy concerns.	Rejected	0.048	0.534	NS	0.002
H6	Trust beliefs negatively affect privacy concerns.	Supported	-0.342	0.000	p < 0.01	0.113
H7	Trust beliefs positively affect willingness to disclose.	Supported	0.496	0.000	p < 0.01	0.313
H8	Privacy concerns negatively affect the willingness to disclose.	Supported	-0.130	0.028	P < 0.05	0.022
Note: Hypothesis are rejected based on p value and f^2 value						

Table 5.25. Hypothesis assessment

5.7 MGA based on covariates

To get a deeper insight of the proposed model, the results of different groups are analyzed. This is according to Hair Jr et al. (2016) an important step to avoid biased path coefficients, as neglecting such analysis could lead to not detecting the heterogeneity between groups. Two MGA's were executed to see the differences based on the demographical variables (Gender, Age, Education) and the other covariates (Privacy invasion and Media exposure). Using demographics as a source of heterogenicity is especially mentioned by Hair Jr et al. (2016) as a viable observable characteristics. Furthermore, the author mentions that other observable characteristics can be used as well.

The influence of the different groups within the demographical covariates can be found in table 5.26. The results were created by forming different groups within SmartPLS. Gender is divided by female (N=108) / male (N=107), disregarding the answers prefer not to say, since the group was too small (N=2). Age is divided by the median (24). Every age of 24 or under is therefore categorized as low age (N=122), whereas everything above 24 is categorized as high age (N=95). Education is categorized in high education including all education above high school (N=145) and low education including high school and all lower education (N=63). The results which can be seen in table 5.26, indicate that for all paths, except PPRA → PC, there is at least one group for which the path coefficient is significant (p < 0.1).

	β						p Value					
	Age		Education		Gender		Age		Education		Gender	
	High	Low	High	Low	Female	Male	High	Low	High	Low	Female	Male
PC -> WD	-0.134	-0.135	-0.076	-0.325	-0.100	-0.171	**0.092**	0.147	0.306	**0.008**	0.245	**0.046**
PPRA -> PC	-0.154	0.133	-0.051	0.202	0.105	-0.079	0.229	0.214	0.599	0.199	0.388	0.478
PPRA -> PPRK	0.567	0.552	0.579	0.484	0.467	0.631	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
PPRA -> TB	0.304	-0.209	0.215	-0.356	-0.112	0.218	**0.034**	0.162	**0.071**	**0.072**	0.461	0.160
PPRK -> PC	0.191	-0.039	0.070	-0.021	-0.101	0.206	0.114	0.724	0.458	0.899	0.362	**0.058**
PPRK -> TB	-0.197	0.207	-0.182	0.387	0.089	-0.120	0.158	0.123	**0.084**	**0.017**	0.495	0.392
TB -> PC	-0.307	-0.331	-0.335	-0.350	-0.290	-0.369	**0.005**	**0.000**	**0.000**	**0.005**	**0.000**	**0.000**
TB -> WD	0.533	0.450	0.491	0.450	0.537	0.461	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
Note: All significant values are in bold												

Table 5.26. MGA based on demographics

Media exposure is not included in the MGA, while the group of low media exposure was too small (N=15). Privacy invasion is categorized in low and high. Low privacy invasion includes all results <4 (N=122), high privacy invasion therefore includes all results from 4 and higher (N=95). The results from the MGA based on these groups can be found in table 5.27. Similar to the results of the demographics (table 5.26), all paths but one (PPRK --> PC) indicate a significant path coefficient for at least one of the groups.

	β		p Value	
	Privacy Invasion			
	High	Low	High	Low
PC -> WD	-0.087	-0.154	0.380	**0.035**
PPRA -> PC	0.316	-0.234	**0.005**	**0.032**
PPRA -> PPRK	0.593	0.547	**0.000**	**0.000**
PPRA -> TB	-0.219	0.286	0.208	**0.016**
PPRK -> PC	-0.067	0.164	0.613	0.110
PPRK -> TB	0.273	-0.232	**0.070**	**0.048**
TB -> PC	-0.282	-0.282	**0.003**	**0.003**
TB -> WD	0.534	0.494	**0.000**	**0.000**
Note: All significant values are in bold				

Table 5.27. MGA based on privacy invasion

5.8 Construct Means

Table 5.28 shows the average means and standard deviations for the constructs based on the participants responses. In general people seem to be concerned about their privacy (Mean = 5, scale = 1-7, where 7 is strongly agree). Although participants have been often exposed to the potential use and misuse of computerized information about consumers in the media (Mean = 5,61, scale = 1-7, where 7 is very often). Participants furthermore do not seem to be very knowledgeable or aware concerning regulations regarding their online privacy, (Mean = 4.08 and Mean = 2.84 respectively).

Construct	Mean	Std. Deviation
WD	4.92	1.66
TB	4.15	1.28
PC	5	1.56
PPRA	4.08	1.91
PPRK	2.84	1.69
CV: Privacy invasion	3.24	1.48
CV: Media Exposure	5.61	1.35

Table 5.28. Construct means

6 Discussion

This study provides two main contributions to the privacy literature. First, two new constructs were formed based on the awareness and knowledge of privacy regulations, more specifically GDPR. Although previous literature looked into the effect of regulations on privacy concerns and trust beliefs (Lwin et al., 2007; Miltgen & Smith, 2015), there is a sharp distinction between those studies and this study, which takes into account a detailed measurement of the future privacy regulation framework in place for all EU member states. A clear distinction is furthermore made between awareness and knowledge in a similar fashion as Dommeyer & Gross (2003). Second, the influence of these new constructs is tested on prior constructs from the APCO Macro model and empirical justification is found for relationships that have been previously confirmed within this model.

6.1 PPRK & PPRA

As hypothesized in H1, one must be aware of privacy regulations in order to have knowledge regarding it, the results indicated the correctness of the statement (table 5.25). Unsurprisingly this path has a large effect size and path coefficient. Between the different groups based on the covariates, the path coefficient does not differentiate much (lowest 0.467, highest 0.631) indicating that perceived privacy regulation awareness affects perceived privacy regulation knowledge in all groups examined in the MGA.

Looking to the means (table 5.28), we find that PPRA has a value of 4.08 (scale 1-7) indicating that the respondents, in average, perceived to be slightly aware of GDPR. For PPRK, the mean value was 2.84 providing the insight that the respondents have tendencies towards not having much knowledge regarding GDPR. It should be noted that both PPRA and PPRK are measuring subjective knowledge and thus could be over- or underestimated by the respondent. We believe it to be plausible to argue that the level of both perceived awareness and knowledge regarding GDPR may increase over time. This due to the fact that the regulation was not enforced at the time of the data collection (European Parliament, 2016).

Wirtz et al. (2007) found that perceived regulations negatively affects privacy concerns. However, we did not find a significant relation between PPRA and PC, resulting in the rejection of H2. Possible explanations for the different results in this study can be found in the way Wirtz et al. (2007) formed their construct. Although the authors argued to measure perceived regulatory protection of the legal and regulatory framework in place, they did so at a very low level of granularity including items where they used the wording ‘existing laws in the country’. Contradictory this study includes a much higher level of granularity focusing on detailed items capturing the future regulatory framework in place for all EU member states (GDPR). This brings us to another possible explanation for the non-significant results of this relationship, since we measured the perceived awareness and knowledge of a regulation that was not in place during the data collection in contrast to Wirtz et al. (2007).

Nevertheless, we did find a significant effect when dividing the sample into two groups based on their privacy invasion (low vs high). This separation resulted in contradictory results. For people with a low level of privacy invasion, PPRA negatively affected PC ($\beta = -0.234$). For this

group, more awareness of privacy regulation resulted in less privacy concerns. While for individuals with a high level of privacy invasion, PPRA positively affected PC (β = 0.316). However, one could argue that people whose privacy has previously been invaded have higher concerns regarding their privacy. This finding is in line with Smith et al. (1996), who found a significant positive effect between the level of previous privacy invasion and privacy concerns (β = 0.16), although measured on the construct instead of the path in our case.

Unexpectedly, perceived privacy regulation awareness did not significantly affect the trust beliefs which was stated in hypothesis 3 to be a positive correlation. With our delimitation, this means that awareness of GDPR does not significantly influence the amount of trust individuals have towards E-commerce websites. It was argued that trust would increase when awareness was high as it had been found in a previous study (Miltgen & Smith, 2015), where the awareness was focusing on governmental protection of personal data from a holistic perspective.

However, examining the multi group analysis provides interesting insights that the level of education an individual has significantly affects the relationship between perceived privacy regulation awareness and trust beliefs. Individuals who have completed high school as their highest completed education were affected by their perceived privacy regulation awareness in a way that increased their trust beliefs in E-commerce organizations. On the contrary, individuals whom had completed higher education were affected oppositely. For these individuals, perceived privacy regulation awareness created less trust towards E-commerce organizations. Looking to the sample used in the conducted study of Miltgen and Smith (2015) the education is spread between secondary school or less and several higher educations. As the authors do not conduct a multi group analysis, we cannot assess if our findings within the groups are similar to theirs. However, education has in the study of Malhotra et al. (2004) proven to be an significant factor affecting trust beliefs in online companies. The study indicated that higher levels of education lead to a decrease of trust in online companies. These results are closely related to ours, however our results are measured on the path between perceived privacy regulation awareness and trust beliefs rather than the construct of trust.

Nevertheless, it is important to note that Miltgen and Smith (2015) do not focus on any specific laws when looking to the perceived regulatory protection but seeks the respondents subjective opinion regarding UK specifically and public authorities. As this study on the other hand looks to GDPR regulations, this may be one explanation as to why the results differ.

The relationship between PPRK and PC was not significant, rejecting H5. This result is in contrast with Dommeyer & Gross (2003) stating that knowledge in regard to privacy practices can create higher levels of perceived control and therefore reducing privacy concerns. GDPR is introduced by the EU parliament to increase the privacy levels of its citizens (Goddard, 2017; Tankard, 2016). We are therefore surprised that H5 does not hold, since greater knowledge of these regulations should increase the perceived level of privacy protection, lowering their concerns (Miltgen & Smith, 2015). We foresee two possible explanations: the first one could be that GDPR only captures the legal framework of protection, disregarding individuals/collectives not complying to the law (e.g. identity theft or phishing). A second possible explanation could be that people do not trust the government in pursuing the regulation, creating distrust.

Although the relationship between PPRK and PC did not hold for the entire sample, A significant path was found in the MGA based on gender. This path indicates a significant relationship between PPRK and PC for male participants (β = 0.206). In other words, if males have more

knowledge on privacy regulations, they are more concerned. This result is although only focused on males, in contrast with the findings of Miltgen & Smith (2015). Prior literature looked into gender as a control variable to privacy control without finding any significant effects (Malhotra et al., 2004).

Another unexpected finding, was that H4 was rejected. As with H3, the possible correlation was drawn from prior literature written by Miltgen and Smith (2015). This study was unable to provide significant evidence that PPRK significantly effects trust beliefs. Besides similar effects as earlier mentioned for not rejecting H3, we believe to another explanation to be plausible, the possible influence of perceived quality (Lwin et al., 2007). Since this study does not take into consideration the perceived quality of the regulation, which could influence an individuals' trust beliefs.

The MGA revealed multiple interesting significant paths for different groups regarding the relation between PPRK and TB. Both groups in previous privacy invasion (low/high) and education (low/high) showed significant relations for the path PPRK to TB. When we split the groups based on education two contradicting significant relations arise. First regarding people who completed higher education, having more knowledge on GDPR tends to lower their trust beliefs (β = -0.182). While on the other hand people without a post-high school education tend to have higher trust beliefs when their knowledge on GDPR increases (β = 0.387). Malhotra (2004) found that a higher level of education negatively influences trust beliefs. Nonetheless, we cannot claim to have found the same result, since we measure on the path rather than the construct itself.

Furthermore, we found a difference in a separation of groups based on previous privacy invasion. Individuals with a high level of previous privacy invasion, who have high knowledge on GDPR, have higher trust beliefs (β = 0.273). A low level of privacy invasion, but a high level of GDPR results in lower trust beliefs (β – 0.232). Previous literature found that previous privacy invasion increases privacy concerns and hence lowers trust beliefs (Bansal, Zahedi, & Gefen, 2016). In accordance with our results, we found that a high level of knowledge on GDPR changed this relation and that knowledge on GDPR increases trust for people whose privacy has previously been invaded.

6.2 Trust beliefs

The hypothesis H6, that trust beliefs negatively affect privacy concerns, was supported. This finding was in line with prior literature (Belanger et al., 2002; Smith et al., 2011). For the results of the multi group analysis, all groups were found to have a significant path coefficient. The findings proved that a similar relation for all groups existed, trust beliefs negatively affect privacy concerns. These results are alike what can be found in the article of Miltgen and Smith (2015). Howbeit, the path coefficient in their study is lower than the ones found in our study. In our structural model, the path coefficient is -0.342 whereas Miltgen and Smith (2015) discover a path coefficient of -0.10. The stronger relationship in our study can be explained by the fact that their study looks into trust into governmental authorities and companies (online personal data context), contra our study solely looks to E-commerce websites. It could thus be argued that trust is more important in the context of privacy concerns within E-commerce compared to the internet in general. Albeit, such argument should treated cautiously as there is an apparent difference in the sample in this study versus the sample in the study of Miltgen and

Smith (2015). Furthermore, the multi group analysis shows that trust beliefs negatively affect privacy concerns regardless of the individuals past perception of privacy invasion. Indicating that all groups show a similar effect regarding the relation between trust beliefs and privacy concerns.

In addition previous literature found a positive relation between trust beliefs and willingness to disclose information online (Bansal & Gefen, 2015; Dinev & Hart, 2006). Our findings support this relationship, accepting H7. The effect size ($f^2 = 0.313$) of this relationship was considered medium (Hair Jr et al., 2016). Trust is therefore an important factor within E-commerce to encourage transactions by diminishing privacy concerns.

From the multi group analysis it becomes apparent that trust beliefs are important for individuals' willingness to disclose regardless of age, education, gender, and past privacy invasion. Our results align well with past literature (Malhotra et al., 2004), especially with Dinev and Hart (2006) who in their study also discover that trust is a highly important construct for individuals willingness to disclose personal information to conduct transactions online.

6.3 Privacy Concerns

The final hypothesis H8, which states that privacy concerns negatively affect the willingness to disclose, is accepted. This finding aligns with prior research (Dinev & Hart, 2006; Ozdemir et al., 2017). The effect size of this relation ($f^2 = 0.022$) is close to the lowest threshold of 0.02 indicating a low effect size according to Selya et al. (2012). Hence, caution needs to be taken with the acceptance of this hypothesis since our sample has problems with the detection of small effect sizes ($f^2 = 0.02$) due to its sample size (N=217) and corresponding power (Power = 0.38), increasing the possibilities of a type two error (Cohen, 1988).

Smith et al. (2011) mentions in the APCO Macro model that this relation may be affected by the privacy paradox, pointing out that an individual may not act according to their concerns. We therefore contemplate that this relation may not hold up during an actual E-commerce purchase. Within the different groups of demographics and privacy invasion, all paths are negative however not all are significant. Thus, the groups cannot be fully interpreted but there is a seemingly correlation that privacy concerns negatively affect the willingness to disclose as can also be seen in the structural model.

6.4 Implications

6.4.1 Theoretical implications

Prior literature has to our knowledge not taken awareness and knowledge of governmental privacy regulations into account when looking to trust beliefs or privacy concerns. The focus has in the past been on perceived privacy regulatory protection, organizations self-regulation/policies, and how they affect privacy concerns (Miltgen & Smith, 2015; Smith et al., 2011). However, as the general data protection regulation is becoming enforced, governmental privacy regulations are now efficiently affecting all organizations and residents within the European union.

Organizational self-regulation/policies will plausibly not become obsolete in the context of privacy concerns or trust. However, governmental regulations will lay a baseline of protection of the data subjects (European Parliament, 2016), forcing organizations to comply with this new regulation. As previously confirmed by Miltgen and Smith (2015), perceived privacy regulatory protection does have an significant effect on both trust and privacy concerns. However, the study does not consider both the perceived awareness and knowledge of such regulations. Therefore, we proposed and tested two new constructs (perceived privacy regulation awareness and perceived privacy regulation knowledge) as an extension to the APCO Macro model. The results implied that such a relation was persistent within groups of the sample, strengthening a relatively un-explored domain for future research. Consequently, perceived privacy regulation awareness and knowledge should be acknowledged and re-validated in further research. Finally, already existing relations from prior literature focusing on the APCO Macro model were confirmed.

6.4.2 Practical implications

The conducted study provided insight into how individuals perceived awareness and knowledge regarding the general data protection regulation currently effects their privacy concerns. As both trust and privacy concerns affect individuals' willingness to disclose personal information to conduct transactions online, it is of high interest of E-commerce organizations to uphold high levels of trust and low levels of privacy concern. The findings of this study indicate that, if such organizations know their customer base well enough, they could use this to motivate disclosure of personal data to transact. In example, if a customer base is of high education it is preferred to spread awareness of the fact that the E-commerce organization follows the general data protection regulation which according to our findings would increase their trust beliefs. However, the organization should refrain from providing actual knowledge regarding the general data protection regulation as this may decrease trust beliefs. Although the results seem interesting, caution should be taken due to the constructs still being in a development stage and further validation is needed.

6.5 Limitations

Although this study managed to gather both a large field sample as well as an online sample, caution regarding generalization needs to be taken. Four areas of the study are hence considered as limitations.

First, the age of the sample is relatively young (median = 24) and skewed to the right (skewness = 2.068). One should in addition note that 71% of the respondents completed higher education, indicating a non-representative sample of all EU citizens. The data is furthermore mostly collected in Sweden, except for the online data collection where people from all over the EU could be reached due to the use of social media websites. However, no exceptions were made in the sample regarding the origins of the respondents, besides the requirement that they should be an EU citizen. Hence, we cannot exclude the possible influence of cultural differences.

Second, the constructs PPRK and PPRA are developed for this study, due to the absence in prior literature. Consequently, we were had to develop the items for these constructs ourselves. The items are created with care and by using the official GDPR regulation as provided by the

EU parliament. Furthermore, we used evaluation panels and a pilot test to increase the validity of these items. Nevertheless, we recommend using the constructed items as a starting set for validation, indicating the need for further research upon them.

Third, the power of the study is insufficient in detecting small effect sizes (Cohen, 1988). A larger sample increases the detection of smaller effect sizes and would therefore be preferred in future research. In that way the possibility of a type two error could be reduced to a minimum.

Last, the empirical data is collected before the GDPR was enforced (25th of May). We therefore foresee the possibility that people will obtain more awareness and knowledge regarding this regulation, when time passes. This could change the relations between the different constructs.

7 Conclusion

With organizations continuously increasing the collection and use of customer data, customers concern in regard to their privacy grows. Hence, governments have become more active in protecting the online privacy of its citizens. A recent example is the enforcement of GDPR at the macro level, affecting all EU member states. In this study we propose and tested a model that incorporates an individuals' awareness and knowledge regarding privacy regulation (of GDPR) and its effects on trust beliefs and privacy concerns, resulting in the willingness to disclose. This study therefore follows the APCO macro structure, *Antecedents → Privacy Concerns → Outcomes.* This research should be seen as a first step towards exploring the effects of regulatory knowledge and awareness towards already established constructs within the APCO macro model. To address the above, this study sought to answer the following research question:

> *What are the associations between governmental privacy regulations, an individuals' privacy concerns and trust in disclosing personal data?*

From the results of the study, the research question could be answered. Governmental privacy regulations are partially associated with individuals' privacy concerns and trust regarding the disclosure of data. From the structural equation modelling it was found that, for the sample as a whole, governmental regulations do not have a significant effect on privacy concerns nor trust. However, from the multi group analysis it became evident that several significant associations exist. The associations were apparent when grouping the sample in; age, education, gender and previous privacy invasion. The results further implicated that depending on the individual demographical background as well as past privacy invasion, differences can be found in how perceived privacy regulation awareness and knowledge affect privacy concerns and trust beliefs (table 5.25 & 5.26). The perceived privacy regulation awareness and knowledge are both having the effect of lowering privacy concerns and/or strengthening trust beliefs within particular groups (e.g. high education, high age, and high privacy invasion), but also increasing privacy concerns and/or lowering trust within other groups (e.g. low education, male, and low privacy invasion). Furthermore, empirical justification is found for the already established relations: trust beliefs → privacy concerns, trust beliefs → willingness to disclose and privacy concerns → willingness to disclose. Lastly, we confirm the role of privacy concerns as a mediator between trust beliefs and willingness to disclose.

7.1 Future research

Some limitations of this study can be seen as an opportunity for future research. This section presents these opportunities and further extends them with ancillary research opportunities. An obvious extension to increase the generalizability of this study would be to secure a cross-border sample of multiple EU member states. In this way one could control for possible cultural differences in the understanding and relations between the measured constructs.

Second, an interesting addition to the proposed research model would be to introduce perceived privacy regulatory protection as a mediator between PPRK, PPRA and PC, as well as trust.

A similar mediating role regarding perceived privacy regulatory protection has been confirmed in prior literature, without considering the separation between awareness and knowledge.

Third, the limitation section acknowledged that the perceived awareness and knowledge of the GDPR could change after enforcement. Hence, it would be interesting and useful to perform a post-study whereby the same model is tested after the enforcement of the GDPR. Enforcement likewise reveals further research opportunities for directives that can play an important role when they are established by the EU parliament, to extend the regulatory framework with specific directives (e.g. E-privacy).

Fourth, this study delimits itself to subjective knowledge and awareness. Nevertheless, it would be interesting to further examine the objective awareness and knowledge of individuals and their influence on trust beliefs and privacy concerns. Finally, it would be interesting to see if differences can be found in the level of subjective awareness and knowledge versus objective awareness and knowledge.

Appendix 1 – Online Questionnaire

Online Privacy Survey

Welcome to this online privacy survey, this survey is made with the intention to collect empirical data for our Master thesis on privacy at Lund University. First of all thank you to take part in this important survey measuring willingness to disclose data in an e-commerce context. This survey should only take around 5 minutes to complete. Be assured that all answers you provide will be kept in the strictest confidentiality.

* Required

1. **Gender** *
   Mark only one oval.
   - ◯ Male
   - ◯ Female
   - ◯ Prefer not to say

2. **Age** *
   _____

3. **Education (completed)** *
   Mark only one oval.
   - ◯ Elementary school (grundskola)
   - ◯ High school (gymnasium)
   - ◯ Higher education (eftergymnasial)

4. **Residency** *
   Mark only one oval.
   - ◯ Within an EU member state (including temporary residency)
   - ◯ Other

5. **How often have you personally been the victim of what you felt was an improper invasion of privacy?** *
   Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very often

6. **How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers?** *
   Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very much

To what extent are you willing to use the Internet to do the following activities?

7. **Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information)** *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very much

8. **Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)** *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very much

9. **Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates)** *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very much

10. **Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)** *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all	◯	◯	◯	◯	◯	◯	◯	Very much

Trust

11. **E-commerce websites are safe environments in which to exchange information with others,** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

12. **E-commerce websites are reliable environments in which to conduct business transactions.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

13. **E-commerce websites handle personal information submitted by users in a competent fashion.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Indicate the extent to which you are concerned about the following:

14. **I am concerned that the information I submit on the Internet could be misused.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

15. **I am concerned that a person can find private information about me on the Internet.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

16. **I am concerned about submitting information on the Internet, because of what others might do with it,** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

17. **I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

I am aware that I, as an individual, have the right to…

In the upcoming section the term service provider is mentioned. Service provider is an organization or person that delivers services on the internet (e.g. Zalando).
The questions will also include the statement "if certain conditions are met", these are conditions such as: when the service provider no longer needs the personal data for the purposes of the processing.

18. **… be notified by who is collecting my personal data when my personal data is disclosed by me.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

19. **... be notified by who is collecting my personal data when the data is collected through a third party,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

20. **... request to see all the personal data that a service provider has stored regarding me as an individual.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

21. **... request for the correction of my personal data, stored by a service provider.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

22. **... request my personal data to be erased from an online service provider if certain conditions are met,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

23. **... restrict the processing of my personal data if certain conditions are met,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

24. **...request my personal data from one service provider and transfer the data to another provider,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

25. **... protest against my personal data being processed by a service provider if certain conditions are met,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all aware	◯	◯	◯	◯	◯	◯	◯	Very aware

When my personal data is being processed I know how…

26. … to handle the procedure of requesting all the personal data that a service provider has stored regarding me as an individual. *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

27. … This is a control question, Select number 7, *
Mark only one oval.

1	2	3	4	5	6	7
◯	◯	◯	◯	◯	◯	◯

28. … to handle the procedure of requesting correction of my personal data, stored by a service provider. *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

29. … to handle the procedure of requesting my personal data to be erased from an online service provider if certain conditions are met. *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

30. … to handle the procedure of restricting the processing of my personal data if certain conditions are met. *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

31. … to handle the procedure of requesting my personal data from one service provider and transfer the data to another provider. *
Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

32. **... to handle the procedure of protesting to my personal data being processed by a service provider if certain conditions are met,** *

Mark only one oval.

	1	2	3	4	5	6	7	
Not at all knowledgeable	◯	◯	◯	◯	◯	◯	◯	Very knowledgeable

Appendix 2 – Interview script

Topic 1: Active Privacy Laws

Q1: What are the most important information privacy laws active in Sweden?
Q2: What are the most important characteristics of these laws?

Topic 2: Perceived Privacy Regulation Awareness (PPRA)

To measure the perceived awareness regarding privacy regulations, we are considering using items from prior literature for measuring subjective awareness, such as:

- I am aware of *Privacy Regulation X*
- I am aware of the benefits that *Privacy Regulation X can provide to me*
- I have come across *Privacy Regulation X* in a media channel

Topic 3: Perceived Privacy Regulation Knowledge (PPRK)

To measure the perceived knowledge regarding privacy regulations, we are considering using items from prior literature for measuring subjective knowledge, such as:

- I know pretty much about *Privacy Regulation X*
- I do not feel very knowledgeable about *Privacy Regulation X.*
- Among my circle of friends, I'm one of the "experts" on *Privacy Regulation X*
- Compared to most other people, I know less about *Privacy Regulation X*
- When it comes to *Privacy Regulation X*, I really don't know a lot.

Q3: Do you see any flaws when using the items for constructing PPRA & PPRK?
Q4: Do you feel like anything is missing when measuring the perceived knowledge and awareness of particular laws?

Appendix 3 – Interview 1

Time and date – 10:00, 4th of April 2018
Location – Lund, Sweden
Duration – 35 minutes
Interview format – Face to face
Interviewee – Privacy expert
Transcription date – 8th of April 2018

I = interviewer, R = respondent

Row (R)	Speaker	Text
1	I	The first question that we have is about the active privacy laws in Sweden, but not only laws which are active now but also which are becoming active as this is our timeframe for the thesis. So, our first question is, what are the most important information privacy laws active in Sweden?
2	R	Well currently it is the personal data act, "personuppgiftslagen" in Swedish, and that is an implementation of the data protection directive from 1995 which is a EU directive. But of course, that has been repealed, and on the 25th of May the GDPR will become applicable. It is already in force, but it becomes applicable in the member states on the 25th of May. And, the current Swedish legislation will be repealed on the same day, it has not happened yet, but it will be by the parliament. So the main difference, I don't know how much EU law you know…
3	I	Not so much…
4	R	Not so much, ok. We'll start with some of the basics. Currently the Eu regulation is a directive. And a directive needs to be implemented into national law. So that is why we have "personuppgiftslagen" and other civil laws in other member states. However, the new regulation the GDPR, general data protection regulation, doesn't need to be implemented. So, it is directly applicable in all member states immediately. However, there is some special things about the GDPR, because it requires sort of supplementary national legislation and also, member states can make exceptions, national exceptions. They cannot make any exceptions they want, but they can make some kinds of exceptions. So, for example you have some sort of room to decide the age when a child can consent to processing of personal data for instance, and then you can also make other kinds of exceptions. And you also need to fill in the details on the national level. Especially for the public-sector bodies, because that is just very sketchily regulated

		in the GDPR, and the GDPR sort of assumes that you will have complementary or supplementary legislation. So, on the 25th of May, hopefully, we will get a new data protection act in Sweden. And that is not going to be a complete legislation, it's just going to be supplementary legislation. So, the GDPR becomes applicable and then we have some national provisions that are specific for Sweden. So, what you want to look at is of course the GDPR and you will also want to look at the new complementary Swedish legislation, if you are looking at only Sweden if you are looking at other member states you need to look at their national complementary or supplementary legislation as well. But that's the most important and most general rules. But then of course, if we talk privacy and not just data protection, because there is a slight difference between privacy and the right of privacy and the right to data protection, so... Data protection is only about personal data, nothing else. Whereas privacy is a broader concept so it covers other things as well, so that is your right to privacy, it covers some other things than, in addition to personal data. So, the right to privacy is also a fundamental right, so you have human rights and fundamental rights. Both in the Swedish constitution for instance. There is right to privacy, and you have that also in the EU primary legislation, so there are those kinds of rules to look into as well. So, it depends on how broadly you define privacy.
4	**I**	Yea, we are looking into privacy in the online context. So, I think we're mostly bound to personal data I would say.
5	**R**	Yea, I think that would be the most relevant rule. So, the GDPR and the new Swedish supplementary legislation .
6	**I**	But the supplementary legislation is part of the GDPR?
7	**R**	No, it is completely national. So, you have the GDPR, and you can find that on the EURLex. And the Swedish supplementary legislation is not in force. It has not been adopted even by the parliament. But there are some preparatory works. I mean there are, so we know fairly well what it would look like. And I can give you the, some kind of reference to that if you want to read it. And unfortunately it is in Swedish, but if you can somehow manage that so. But there are some important complementary provisions in that. But that's basically what you want to measure. Then of course there are also a lot of special regulations. That's when it becomes a bit complex because there are specific regulations for scientific research for instance. And since everything is in movement not in this area, we have old legislation about that and we will have new legislation. So there will be a "forskningsdatalag" for instance. A special act on research data. And there will be one for hospitals and almost every other area. So there are basically hundreds of special data protection acts and those are mostly national laws supplementing, in the future they will, or rather on the 25th they will supplement GDPR but are currently supplementing "personuppgiftslagen". So that's basically how it works, it is

		a rather complex are depending on, there are a lot of sectors specific rules. However, EU level, there are also some special legislation and the most important if you are looking at the digital context is called the e-privacy directive. And that is also going to be replaced of course. So we will have new e-privacy regulation. And that has not been adopted yet by the EU legislator. But you have some old legislation and you also have preparatory works, proposals for the new law and, well it is a little bit of a mess right now actually. So I guess people are a little bit excused if they feel like they do not have a grip on this now. Because it is basically on flux right now. So, it is rather hard to pin down what… So I would focus on the GDPR and perhaps the national… General legislation and I would skip the special legislation, unless you want to look specifically at some specific sector.
8	**I**	Yea, we're interested at looking into e-commerce, because most privacy literature is focusing on e-commerce.
9	**R**	There is of course an e-commerce directory also on the EU level. Which is relevant for this because the rules about sort of… If you have some internet service provider for instance, the liability for internet service providers when it comes to data protection, not their own processing but for instance ISP could of course just transport bits of data of course in, and their liability for that kind of action is actually in the e-commerce directory. It is a little bit complex but there is a reference of course from the GDPR to the e-commerce directive saying that GDPR will not affect those rules.
10	**I**	Oh okay, so the e-commerce directive is not part of GDPR?
11	**R**	No, so it is a little bit of a complex landscape basically. So, as I said, you will have to excuse people for not having a grip on all of it. I think most people know about "personuppgiftslagen" of course. But I think a lot of people are not aware of the regulation on the EU level. Because previously it has been in the form of directives and directives are implemented into national law, so you know about national law but not necessarily that they are implementations of EU directives. And now EU is moving a little bit away from directives and are instead doing these kinds of regulations that are directly applicable. And of course, it has to do with the fact that there are so many member states today, so 28. And of course, one of them are going to leave soon, or someday at least. But again, it is becoming a little bit too complex to monitor all of this compliance with the EU legislation so that is why they are moving away from directives and saying "No we don't need any national legislation, we go directly for these kinds of EU regulations that are directly applicable. So, both the GDPR and the new e-privacy regulation will be directly applicable". And the plan is actually that the new e-privacy regulation should also enter into force in May this year. It doesn't look like it at the moment but that is the plan. I don't know, are you looking specifically at privacy

		or are you also looking at like information security or network security issues?
12	**I**	I think we're mostly focused on information privacy in online context with a focus on e-commerce. So, I don't really think we're on the security level I would say.
13	**R**	Ok, so you might want to be aware of that there is also another directive called the NIS directive, which is about network information security. So, I mean it has to do with privacy but it is more information security and network security, and of course that is related to privacy. You can't have good privacy without good security. But, they are not really the same thing, but there are some overlap between them. You might want to know about that it is… I think it is fairly unknown actually, that people are aware of the GDPR but not aware that in May a lot of new, other kinds of new regulations affecting this area is entering into force, becoming applicable. So, but GDPR is rather well known, of course.
14	**I**	So, I think the second question might be a bit too specific then, but what I maybe can ask instead is. If you know the context of which we are looking into, what kind of laws do you think we should focus on? Is that GDPR and e-privacy law?
15	**R**	Yea, I think you should focus on those two. Because I mean they are soon becoming applicable, and they are going to be the most important. I mean, you have to know at least that. Depending on what sector you are in, I mean if you are working at a hospital for instance you clearly have to know the sector specific privacy regulation for, about the health industry as well. Because of course that kind of personal data they are processing is of course extra sensitive. So, there are even stricter rules for that.
16	**I**	Are there also specific rules for e-commerce or is it only directives?
17	**R**	No, I would say that there are no specific rules specifically for e-commerce, so it is basically the GDPR there are no sector specific. But, it is good to know that the intention of the legislator is to have not only law but also some amount of self-regulation, and actually that is what is missing at the moment. So, they want approved codes of conduct, that are approved by the supervisory authority. So they are not law but they are not completely self-regulation either, they are somewhere in between, because they have been approved by the supervisory authority. So, by this approval they sort of do not immunize you from liability but it is the burden of proof becomes much easier if you follow a code of conduct that has been approved, and also they want certification mechanisms. So, this kind of self-regulation with codes of conduct and certification and privacy seals and things like that. They are talking about European wide privacy seal

		for instance, or data protection seal. But that is not in place at the moment so that is one of the biggest problems because the GDPR is very abstract actually. So, it is really hard to implement in reality, to understand "So, ok I understand the text, but what am I supposed to do? How is this dialog box, supposed to look like? What kind of information do I need to ask about and how to". That is supposed to go into the codes of conduct and specifies the rules in a sector. So, of course there will be a code of conduct and a specific certification for e-commerce. But, not at the moment. So, that is one of the biggest problems with implementing GDPR really. I mean the rules are not… We should finish the work on the 25th which is really soon and the problem is that the rules are not yet there. So it is going to leave basically no time at all to implement it.
18	**I**	So the rules need to be a bit more sector specific? They are too broad now?
19	**R**	Yea. There are going to be a lot more sector specific rules and especially a lot of them are going to be in the form of self-regulation, like codes of conduct but the approved versions of it. There are currently some codes of conduct and self-regulations within this area but they are not formally approved so they are just, well, recommendations, more guidelines. But the approved codes and certifications are going to be more than just recommendations or guidelines, they are going to have some kind of legal value. Especially in the form of easing the burden of proof. It is good to know that the biggest difference between the current regulation and the new regulation is a shift in the burden of proof. Basically, old regulation says that the supervisory authority needs to prove that you are processing data indirectly, that you are not complying with the current regulations. New regulation is completely different, it has shifted the burden of proof to the organization that are processing the data so it is basically saying that if you cannot prove that you are complying, you are in breach, and then you are fined. So, you need to document a lot more basically. And that is where codes of conduct and certifications come in. Cause, if you follow an approved code of conduct, if you have an approved certification, well that can be used not as a complete evidence of compliance but it can be used as a really good sort of proof for compliance. It is much harder for the supervisory authority to say that you are not in compliance with a code that we have approved, or if you have passed a certification with an accredited certification sort of a supervisory body, if you have passed all of that already it is much harder for the supervisory authority to say that you are in breach. So that, that's how that mechanism works. So basically the new privacy regulations in the EU will work pretty much as how information security works. Because that of course is using standards and certification and codes of conduct and things like that. So it is going to be more self-regulation. But that's actually lots of misconceptions now

		of the GDPR, a lot of people are completely unaware of the fact that it is going to be a law of self-regulation.
20	**I**	Okay, and then we have some questions about how we are going to measure our constructs. Because we want to look into the awareness and knowledge of those regulation, so first we have some questions about the awareness. To measure the perceived awareness regarding privacy regulations we are considering using items from prior literature, to improve construct validity and for measuring subjective awareness and we have some items in place and we are wondering what you think of those items in measuring perceived regulation awareness, so the first one is: Are you aware of privacy regulation X.
21	**R**	Well I guess that's going to be an item measuring for example GDPR?
22	**I**	Yes correct, those are going to be the specific laws. The second one I am aware of the benefits that privacy regulation X can provide to me. And the third one I have come across privacy regulation X in a media channel.
23	**R**	Well so, empirical studies are not my expertise. I know the basics but that's not my area of expertise. I usually cooperate with other researchers who have that expertise. Just so you are aware of that. But I think those seem to be sound, I guess that would be a good way to measure basic awareness. It is definitely going to be one of those questions that the supervisory authority asks, I mean if the personnel don't even know about the regulation I mean that is pretty shocking for GDPR of course. So I usually say that I mean everyone always handles processing data and that is basically everybody in an organization, very view are not processing any personal data at all. I mean there is a minimum I think will need like some kind of minimum training about this. Like a 20 minute video or something, just may be creating awareness. So that's the first step is of course to be able to name the regulation at least to say that oh yes I have heard about that. So if they say I have no clue what that is, of course that is a breach.
24	**I**	And we are also interested in the last question in a media channel. But maybe we want to divide that because we are also interested in maybe people saw it for example on a governmental advertisement or a commercial or something or maybe a commercial company. So maybe we can divide that?
25	**R**	Yes perhaps, I haven't seen any official information at all. I think that is one of the problems. A lot of small and medium size especially the small companies they are completely unaware of this and of course this applies as much to them. I mean there are some exceptions for small and medium size companies but very few actually. So

		they are going to be hit quite hard by this. But I haven't seen any actually. Not at all.
26	**I**	No me neither.
27	**R**	I mean they are on the authority supervisory webpage but there is some information but I haven't seen any more active information about this for official channels. It has been actually just the traditional media. Of course there have been a lot of them. Especially in the IT press of course. There is a new article every day it feels like, unfortunately they are very incorrect. That's one of the biggest problems. There is so much misconceptions or incorrect information. Even in media. But I think that is a good question.
28	**I**	Okay and then we also want to measure the perceived regulation knowledge. To measure the perceived knowledge regarding privacy regulations we are considering using items from prior literature for measuring subjective knowledge such as: I know pretty much about privacy regulation X. I know how to judge the quality of privacy regulation X. I think I know enough about privacy regulation X to feel pretty confident when I share my personal information. I do not feel very knowledgeable about privacy regulation X. Among my circle of friends I am one of the experts on privacy regulation X. Compared to most other people I know less about privacy regulation X. I have heard of most of the new privacy regulations that are around. When it comes to privacy regulation X I don't know a lot.
29	**R**	So as you said these are subjective. So ehm and you are not going to measure knowledge in a more objective way? Like asking questions about the subject matter of the law or anything like that?
30	**I**	Well we have been thinking about that, first we wanted to put in some parts of the law and then basically ask them true or false questions. But what we want to do now is measure those on a Likert scale because that will be easier to verify the model. So that's why want to measure subjective knowledge, because it is harder to measure objective knowledge in such a way.
31	**R**	So okay the only thing that I was thinking about was that it might be possible to sort of control whether there perceived knowledge is accurate, but on the other hand it might have to be a lot of questions than. To make that and you might have to ask at least 20 questions or something like that about GDPR.

32	**I**	Yes but what we hope to see is that there is a difference in how aware people are and their knowledge. So maybe for example we figure that people are very aware of certain regulations, but they don't know so much about it so that could be interesting.
33	**R**	Yes I mean this is really in the beginning and there is a lot of change going on so I guess it is interesting just to measure awareness actually. I mean even that question is interesting at the moment. Because we actually don't know for sure how much or little awareness there is. Of course the large organizations, they know about this but I also know about several large organizations that didn't know about this or fairly large organizations. Like public sector bodies that were more or less unaware of this only a year ago. So I think every I haven't met any large organization that are currently unaware of this and that are not working of it of course. Everyone is working on this so every other one special in IT said no we have dropped everything, we are just working on GDPR compliance. So especially in the media industry of course.
34	**I**	But also we are more interested in the individual rather than the organizational level. So we basically want to ask everyone, like end-users.
35	**R**	Yes I also got the impression from the questions that was my next question if you were focusing on end-users like people using e-commerce shops etc.
36	**I**	Yes
37	**R**	Well rather than as employees perhaps. Although it is good to know that employees as in your role as employee you are also protected of course for your employer in using your personal data. So it perhaps not necessary to answer that but we are not only protected in our private lives but also in our work life. So that is probably something if you ask about that you will probably see that people think that they are not protected in their work life. So okay as a professional am I really protected? Yes, it is not just employees I mean if you are self-employed you are still protected. So it is all physical and its regardless of the context. So its only the organization as such that is not protected.
38	**I**	I think we already discussed this question about the items and if they are suitable. But do you see any flaws in using these items?
39	**R**	(Looks at paper with items) Not for the purpose that you want to use them for. As I said before I mean it could be interesting to also measure objective knowledge and not their perceived knowledge. But that is probably outside your scope and I mean to do that accurately I guess you need to have a 20 to 50 multiple choice questions and it seems really out of scope. But otherwise I think that it seems to be

		sound and focus on some of the more general legislations I mean that is realistic to ask about. If you are not making a sector specific study you shouldn't ask sector specific questions, because nobody is going to know about them of course. Unless you are a researcher or employed by an university I mean you are not going to know about sector specific regulation for scientific research.
40	**I**	Yes we are interested in the e-commerce sector but as you said before I don't think that there are sector specific regulations within that sector at the moment.
41	**R**	At the moment there are no sector specific regulations in that sector but as I said before there will be sector specific codes of conduct and sector specific certification mechanisms. And there are already certifications like that but for information security. So there is an organization called svensk handel that has certification that is used by the larger Swedish e-commerce sites they have a seal so that you can feel saver. But I think its I can't remember but I think its trygg ehandel or something like that to feel safe or e-commerce. But it is rather popular but also rather expensive so that is why the smaller e-commerce sites, they don't have it. Or perhaps they don't have the security. But I also know that it is because it costs a little bit. But there is going to be a similar mechanism so that is going to be for e-commerce. So when you have this e-commerce site you will have this sign that they have good information security to build confidence with the consumer, but there is also going to be some other kind of seal saying that this e-commerce site processes your personal data in compliance with GDPR. But that is for the future and unfortunately there is nothing like that at the moment. And also you can apply for such an approval for the 25th of may. So there are obvious reasons why there are no approved codes of conduct, but hopefully we will get some of those during this year. I know that some organizations; trade organizations are prepared and on the 25th they will send them in and apply for approval and then that is of course going to take a few months. I haven't heard anything about e-commerce but I'm sure that svensk handel is working on something like that.
42	**I**	That will be a code of conduct then?
43	**R**	That will probably be a code of conduct and perhaps a certification mechanism. So and I'm in a research program called Fair data it's a nova project and we working on codes of conduct and also certification mechanisms and at the moment we are mostly focused on doing the background research with a lot of partners. So trade organizations for digital media and marketing research companies and things like that in Sweden. And eventually I think we are going to use that so actually make a sort of certification mechanism, probably for digital

		media and ecosystem around digital media like marketing research and so on. So that's my sort of current research project. But again: we are not going to produce any certification mechanism or anything before the 25th of may. And to be honest it is going to take a little bit longer. Because there is a lot of issues to iron out and of course it needs to be realistic and good for business and privacy of course. So we have to do a lot of balancing there and of course a code of conduct that isn't going to be both good for privacy and businesses will never be used by anyone. But it is interesting. When you are finished with this I would be interested in of course looking at your results when you have published it. And when you have any other questions you can just e-mail me. But I think this looks sound.
44	**I**	Thank you very much for this interview.

Appendix 4 – Interview 2

Time and date – 10:15, 10th of April 2018
Location – Lund, Sweden
Duration – 24 minutes
Interview format – Face to face
Interviewee – Privacy expert
Transcription date – 10th of April 2018

I = interviewer, R = respondent

Row (R)	Speaker	Text
1	I	So our first question is regarding the active privacy laws. So we were wondering what are the most important information privacy laws active in Sweden? And we are also thinking of the laws that are becoming active within the next 6 months.
2	R	Well I think my suggestion now is just to focus on the new regulation because we had the privacy law in Sweden which is the PUL, but I don't know if you know how the European framework law works?
3	I	Yes a little bit
4	R	Well there are basically two kinds of European law. One is the directive and one is the regulation. The difference is that the directive set a target and then say okay, every member state must obtain these targets objective. But then each member state is free to decide in which way they arrive to the point. So it means that Italy, Sweden, Portugal, Spain every state is going to make a national law saying okay we want to achieve this topic with this. So you have the EU directive on top and then in each country you have a national law, could be a law or something else but let's call it a law telling in which way you get there. So there can be a difference of course. We are 28 member states, there will be 28 national different laws. Not totally different because the aim is one, but they are different. In the previous framework, the privacy was regulated in this way. We had an EU directive and so we had in each country, national law telling how the directive should have been enforced and in Sweden this law was called PUL. Now it is from May on the old EU directive is going to be repealed. And the main EU law will be the new regulation the GDPR regulation. The regulation is different because the directive set just to aim and then each state must make an internal law to decide how to perform this. The regulation instead tells everything. So tell the aim and tell how to get there. So when you have a regulation you do not need any internal law. You just apply the regulation. This is going to change a lot, because nowadays there will not be these need of internal national law about privacy like before. Of course this

		doesn't mean that everything will be a bullshit, just that on certain matter for example about national law, the regulation is going to recall national agreements and so on. So what we will still have, something regulated by the EU regulation and something by national law. But of course the balance has shifted, we have a much more uniform norm now, which is basically the regulation. So if you are looking for the legal provision I would focus mainly on this regulation and of course on how these regulation is applied. Because privacy is not just a law or regulation, it is an entire system. In general we have a law and then we have the court applying the law. With privacy of course we have this, but we also have the authority, the privacy authority. So each member state has a privacy authority and then we have a EU privacy authority which are should control how the privacy regulation is applied. And this is important, because of course the directive/ the law can't tell everything and privacy is very broad. So if I want to I have a truck and I want to put an alarm, which is connected with GPS and of course I need it because otherwise someone will steal the truck. But at the same time I could see where the truck is and so I could tell if my employee is driving the truck or if the truck is out close to the café. Okay so there are very big privacy problems. And of course all of this stuff can't be written in the regulation, that is impossible and so are the national and EU data protection authority which are dealing with these rules. So I would focus mostly on these regulation and on all the guidelines and decision from the data authority. I think that these is the most important. And you can easily find everything online. There is the so called group of article 29, which I don't know if you have or already seen something. Well it is basically a group composed by representatives of data protection authority of every member state. And so at central level and decide how to apply the data protection, how to cope the data protection regulation with the single matters. So they can really give you precise insides on what is going on. Of course even if we have a new regulation something is going to change, but a lot of stuff will basically remain the same. So this mean that all the previous guidelines will be still valid. So you can also go on the website of the Swedish authority which is data exceptional. Sorry for my Swedish. (7.28) And there you can find a lot of decisions guidelines and other stuff. I think that this is mostly, yes I would focus mostly on this.
5	**I**	In our previous interview someone mentioned besides GDPR you also have the E-privacy regulation still in place.
6	**R**	Yes this was most focusing on the employment which is more general. You also have e-privacy and you also have a directive concerning privacy linked to criminal proceedings. Which is another thing. So more sectoral, so there is also a directive concerning how police could manage personal data when it comes to crime. Of course the topic is very broad, so I think you should also decide if you want to

		address all the topic of privacy or if you maybe want to focus on the private sector.
7	**I**	Yes we focus on the online context of privacy and we focus on e-commerce in particular.
8	**R**	Okay, I'm not really about this because there is also a big part about business law I'm more liberate lawyer, so my focus could be a little bit different. Of course now with all the stuff with Facebook going on and Cambridge Analytics that is really on the rise.
9	**I**	I think we should go on to one of our construct which we are making, which is both the perceived privacy regulation awareness and perceived privacy regulation knowledge. So we want to make these two constructs, since they have not been used within the literature before. So to do this we are for the perceived awareness concerning privacy regulations, we are considering to use items from prior literature for measuring subjective awareness. Such as I'm aware of privacy regulation X, I'm aware of the benefits of privacy regulation X can provide to me and I have come across privacy regulation X in a media channel. Just to see how aware are they of the laws eh regulations. So we kind of want to measure it at a subjective level. And we are curious as if you see any flaws just viewing them spontaneously? If you feel anything is missing just to measure the perceived awareness
10	**R**	(takes a look at the items) I think that about this topic from may on there will be a very big change. Because there are a couple of things that will be modified, very important. One is the principal of accountability I don't know if you already know something about this?
11	**I**	With the burden of proof?
12	**R**	Yes! Basically. So now until may the data protection authority, sorry. For the privacy law there are something that you can do and something that you can't do. If you do something wrong, there are sanctions, fines. At the moment the data protection authority must demonstrate that you have done something wrong, some infringement. From may on this is going to change, so will be the single person that has the duty to demonstrate that he is complying with the privacy law. So the data protection authority can only ask okay, show me that everything is okay with the data law. And even if you are complying but you are not able to demonstrate it, you will get the fine. And also the amount of sanctions is going to increase, because before we had fines that were not so big. Now we have a fine up to 20 million euro, or 5 percent of you know a fee. So you know, there is much more attention on this, for this moment I think that you can't see out in the society, because the new law is still not applicable. But from may on of course all of this will become you know applied also to the public.

		Know it is just business to business and a lot of things going on, consultants and this kind of stuff. The most simple thing for example, how many times you have put a signature, for a contract or something and they say yes this is for privacy. And you sign. That signature is to give the permission to use your personal data, but also nowadays the law says that it is not sufficient to give the permission only. The consult should be after you give a full information concerning how and in which way you use personal data. Actually this information could also not be written and in a lot of case for example maybe for a telephone company you just sign and maybe there is written I have received full information on how my data will be used and they give the consent and you sign. From may on this will not be sufficient any more because it will be the perceiver that will then demonstrate that it gave full information. And so if it is just a signature but not able to prove what was the information content, of course it will be a big mess. So I think you are leaving a little bit this changing moment. So I think that those instrument will be still very good, but of course the social appreciation/awareness of this will change.
13	**I**	Yes I think we are measuring basic awareness now so for example we want to measure; Im aware of privacy regulation – GDPR for example, so it is very broad.
14	**R**	Yes it is very broad, but of course I think that most of the people don't know what is going on. So maybe they don't know that there will be this big change, but once the change will be active they will see okay that is something different. For example Lund university is changing some policy, in order to get ready for privacy regulation. For example the applicants put a picture on their CV. They use it to ask okay when you use your CV to apply for a position put a picture. But why should you put a picture on a CV? Is how I look like important to state if I am good to teach or not? And so now they put okay picture is not compulsory. Something is changing.
15	**I**	Okay I think that we can move on to the next construct, is perceived regulation knowledge. And to measure this we have some new items that we consider to use, you can find them on the paper (points at items)
16	**R**	(Looks at items) Well I think of course yeah this are items for quantitative research. And I think that the change will not be really concerning the quantitative point of view. Because we are more in a certain information which we have. Privacy regulation is very important, and we are moving to a situation where we still have privacy regulation. So it is not about how much privacy regulation in our life, we already have a lot. I think it is just the quality of the regulation. That is going to change. So I think that probably you can, you will have almost the same answer, before and after the new regulation coming to force. Because today yes if I want, I don't know I was now replying

		for a membership reward program and I will say I will give the concern to give my telephone number to have messages about new offers and so on. And like this for everything. The point is that the quality of the information that we will have the control that I could have on my data and so on is going to change. So, I think that these are pretty good items, but I would also focus on this, if you have time. And if you already have some data about the current situation. And I know this is about privacy and I know that its changing can I appreciate that something new, do I feel more safe now or not? And also to which is the public you are going to pose this question to? Is it everybody or someone working with something.
17	**I**	Well it is basically everyone who bought something on a e-commerce website.
18	**R**	So basically a common citizen.
19	**I**	Yes
20	**R**	Not someone with some special skill
21	**I**	Could be
22	**R**	Yes, could be if a privacy expert is going to buy something, but it is not a requirement. And I think that it is fine, but I would also try to focus on the qualitative stuff. For example, in the new regulation concerning internet and this kind of stuff. It will be also possible to instead of course in addition to long written part to all the stuff. Also, some laws some picture colors to have more impact. Because of course especially online, you scrolled down and say yes. Because otherwise you can't go on and you don't read. But this was Expert X telling us sometimes ago. Especially when it comes to privacy consent of underage people and this kind of stuff. They say go okay, we should understand that a service is addressed to this target; lower age are not so aware about privacy and that kind of stuff. It is better to use also this color picture this kind of stuff. And this is something that is going to change.
23	**I**	Okay, so do you suggest maybe only focusing for example on the new situation?
24	**R**	Well if you already have some data about the current situation.
25	**I**	Yes, but we don't have empirical data about the current situation, only from literature.
26	**R**	Okay, so you want to collect empirical data for your research?

27	**I**	Yes we want to collect empirical data from a survey which we will compose from the items that we are handling at the moment.
28	**R**	So I think this I don't know the deadline for your research?
29	**I**	We have a hand-in the 25th of may.
30	**R**	Okay so it is not possible, but of course you can still measure if people are aware of the new law.
31	**I**	I think that is the interesting part, if you think you are protected and you think you know a lot are you more concerned about sharing your data.
32	**R**	Maybe you could add something like do you know that this would be something changing. Do you think that you need more protection and this kind of stuff? Because of course you can't collect data for the new law. But you can measure maybe, if people are aware now and if people think that there are some kind of problems. And of course, this is also maybe if you would have acquired data about the current situation two months ago, maybe you would have some answer but maybe now with all this big Facebook stuff going on, maybe the same person, because of the newspaper will have a different answer. And of course, this is a little bit the problem when you do this kind of enquiry about the common people with this very big topic. Everyone focusing on that but if you read the Facebook guidelines it was already knew that Facebook was using your personal data, because Facebook is free and there are a lot of people working for it, so yes. Some money, sure. So, I think, maybe you can switch on this, asking if people think that something is needed, if they know that something is going to change and if they will have a better situation. This is unlucky, you have a deadline and the law is changing.
33	**I**	But I don't think it is a big deal, we can still ask them for example like about GDPR or E-privacy, because we are measuring basic awareness and knowledge. It is not very in-depth and also not objective but rather subjective, so I think it would still be very interesting.
34	**R**	Definitely yes. Also, because I told you it is not really changing the level of protection, it is more or less the same. It is just giving more effectiveness.
35	**I**	That was the last question, thank you for your cooperation!
36	**R**	You are welcome.

References

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly, 33*(2), 339-370.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Bansal, G., & 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.

Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*, 7.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.

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.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological bulletin, 107*(2), 238.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological bulletin, 88*(3), 588.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices.

Boritz, J. E., & No, W. G. (2011). E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems, 25*(2), 11-45.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. *under submission, 13*.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of marketing research*, 64-73.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences 2nd edn: Erlbaum Associates, Hillsdale.

Colman, A. M., Norris, C. E., & Preston, C. C. (1997). Comparing rating scales of different lengths: Equivalence of scores from 5-point and 7-point scales. *Psychological Reports, 80*(2), 355-362.

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

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34-51.

EUR-Lex. (2017). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

European-Commision. (2017). Proposal for an ePrivacy Regulation. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika, 61*(1), 101-107.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703-705.

Graham-Harrison, C. (2018, 17-03-2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, Newsarticle. *The Guardian*.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science, 45*(5), 616-632.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*: SAGE Publications.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of management information systems, 24*(2), 13-42.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial management & data systems, 116*(1), 2-20.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135.

Hsu, S.-H., Chen, W.-H., & Hsieh, M.-J. (2006). Robustness testing of PLS, LISREL, EQS and ANN-based SEM for measuring customer satisfaction. *Total Quality Management & Business Excellence, 17*(3), 355-372.

Hu, L. t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal, 6*(1), 1-55.

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

Hulland, J., Chow, Y. H., & Lam, S. (1996). Use of causal models in marketing research: A review. *International journal of research in marketing, 13*(2), 181-197.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems, 34*(2), 369-400.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (IJeC), 11*(4), 1-10.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations.

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management, 36*(5), 724-734.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology, 28*(4), 563-575.

Lee, S., Lee, Y., Lee, J.-I., & Park, J. (2015). Personalized e-services: Consumer privacy concern and information sharing. *Social Behavior and Personality: an international journal, 43*(5), 729-740.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-71.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of management information systems, 27*(4), 163-200.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572-585.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS quarterly, 35*(2), 293-334.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013). *Privacy awareness about information leakage: Who knows what about me?* Paper presented at the Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society.

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

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

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D., & Barton, D. (2012). Big data: the management revolution. *Harvard business review, 90*(10), 60-68.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International journal of electronic commerce, 6*(2), 35-59.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4), JCMC942.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741-759.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard business review, 93*(5), 96-105.

Morrison, M., Bell, J., George, C., Harmon, S., Munsie, M., & Kaye, J. (2017). The European General Data Protection Regulation: challenges and considerations for iPSC researchers and biobanks. *Regenerative medicine, 12*(6), 693-703.

Mukred, A., Singh, D., & Safie, N. (2017). Investigating the impact of information culture on the adoption of information system in public health sector of developing countries. *International Journal of Business Information Systems, 24*(3), 261-284.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization, 17*(1), 2-26.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642-660.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS quarterly*, 977-988.

Potoglou, D., Palacios, J.-F., & Feijóo, C. (2015). An integrated latent variable and choice model to explore the role of privacy concern on stated behavioural intentions in e-commerce. *Journal of choice modelling, 17*, 10-27.

Pötzsch, S. (2008). *Privacy awareness: A means to solve the privacy paradox?* Paper presented at the IFIP Summer School on the Future of Identity in the Information Society.

Recker, J. (2012). *Scientific research in information systems: a beginner's guide*: Springer Science & Business Media.

Selya, A. S., Rose, J. S., Dierker, L. C., Hedeker, D., & Mermelstein, R. J. (2012). A practical guide to calculating Cohen's f2, a measure of local effect size, from PROC MIXED. *Frontiers in psychology, 3*, 111.

Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). e-Government Adoption Model (GAM): Differing service maturity levels. *Government information quarterly, 28*(1), 17-35.

Shook, C. L., Ketchen, D. J., Hult, G. T. M., & Kacmar, K. M. (2004). An assessment of the use of structural equation modeling in strategic management research. *Strategic management journal, 25*(4), 397-404.

Short, J., & Todd, S. (2017). What's Your Data Worth? *MIT Sloan Management Review, 58*(3), 17.

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

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

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS quarterly*, 503-529.

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

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the royal statistical society. Series B (Methodological)*, 111-147.

Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016*(6), 5-8.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53.

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2015). *A survey on security and privacy issues in big data.* Paper presented at the Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for.

Ullman, J. B., & Bentler, P. M. (2003). *Structural equation modeling*: Wiley Online Library.

UNCTAD. (2018). *Global Survey on Internet Security and Trust*. unctad.org Retrieved from http://unctad.org/meetings/en/Presentation/dtl_eWeek2018p01_EricJardine_en.pdf.

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science, 44*(1), 119-134.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348.

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems, 53*(4), 31-38.

Zhu, W., Wei, J., & Zhao, D. (2016). Anti-nuclear behavioral intentions: the role of perceived knowledge, information processing, and risk perception. *Energy Policy, 88*, 168-177.