DISSERTATION

CONSUMER INTENT TO DISCLOSE PERSONAL INFORMATION IN ECOMMERCE: A COMPARISON OF ESTONIA AND THE UNITED STATES

Submitted by

Stephen Cory Robinson

Department of Journalism and Technical Communication

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2014

Doctoral Committee

Advisor: Kirk Hallahan

Donna Rouner
Patrick Plaisance
Michel Walrave
Carole Makela
Karen Hyllegard

ABSTRACT

CONSUMER INTENT TO DISCLOSE PERSONAL INFORMATION IN ECOMMERCE: A COMPARISON OF ESTONIA AND THE UNITED STATES

An online survey conducted among participants in the US (n=248) and Estonia (n=225) examined willingness to disclose and perceived risks pertaining to disclosing *personally identifying information* (*PII*, also referred to as *personal data* in Europe) in ecommerce, as well as attitude toward disclosure in general, and anxiety disclosing personal data. Additionally, the study investigated how willingness to disclose and perceived risk of disclosing personal data were affected by demographic variables, trust in the Internet and trust in institutions, the Big Five personality dimensions found in the psychology literature (neuroticism, openness, agreeableness, conscientiousness, and extraversion), and four sets of perceived shopping benefits (opportunity benefits, bargain benefits, purchase benefits, and expected privacy benefits).

Despite Estonia's advanced adoption and progressive policies and practices toward the Internet, Americans were more willing to disclose, exhibited more positive attitudes, demonstrated less anxiety, and were less concerned about perceived risks. For Estonians, ecommerce experience, perceived purchase benefits, and trust in the Internet and institutions were significant predictors of willingness to disclose personal data. Americans who perceived purchase benefits were found to be the most likely to disclose PII, while Americans with lower levels of education were also more willing to disclose.

The study utilized a 17-item list of potential disclosure items (name, email address, etc.) and showed these can be categorized reliably into six sub-indices: contact information, payment information, life history information, financial/medical information, work-related information,

and online account information. Further, a reliable efficient, 20-item scale was developed that can be deployed in future studies investigating the Big Five personality traits.

Online disclosure consciousness (ODC) was introduced as a framework to conceptualize and empirically measure the gap between one's willingness to disclose and perceived risk pertaining to the overall 17-item index used in the study, the sub-indices, and particular items. Using 7-point Likert-type measures, the results showed significant gaps among participants both within and across nations.

A 5-scenario online disclosure consciousness model is presented to explain the tradeoffs involved in making a disclosure decision, with absolute willingness to disclose and absolute perceived risk on the two extremes and theoretical midpoint where the two competing motivations cancel themselves out. Changes in a person's position along the continuum are posited to be influenced by marketers' initiatives, personal experiences, and external factors.

Implications for theory, consumers, marketing practice, and public policy are discussed. The findings suggest that willingness to disclose and risk aversion can and should be analyzed empirically together. Thus, the ODC model provides an alternative conceptualization to the ideas of the privacy paradox, privacy calculus, and privacy cost-benefit ratios found in the literature. The study suggests consumers have a responsibility to educate themselves about online disclosure practices and how to protect their privacy. The findings also suggest marketers and policy makers should recognize that data disclosed online are not all equally sensitive to consumers. However, fostering trust, reducing risks, and promoting benefits are essential to the future of ecommerce.

TABLE OF CONTENTS

ABSTRACT ii
CHAPTER ONE: INTRODUCTION 1
Background: Ecommerce and online disclosure 2
Personally identifying information (PII)/Personal data 12
Estonia versus United States 15
Rationale 17
Overview 18
CHAPTER TWO: REVIEW OF LITERATURE 19
Nationality 20
Dependent Variables 27
Willingness To Disclose Specific PII Items 27
Attitude Toward Disclosing PII Online 29
Anxiety Disclosing PII Items 31
Perception Of Risk Of Disclosing Specific PII Items 33
Moderating Variables 36
Gender 36
Age 37
Education level 37
Ecommerce proficiency 38
Trust 38
Trust in the Internet 39
Trust in institutions 40
Personality 41
Perceived benefits of exchanging PII information 43
Risk taking as a personality trait 45
Hypotheses 46
CHAPTER THREE: METHODOLOGY 51
Participants 51
Sampling and Recruitment 51
Procedures 55
Survey administration, format, and translation 55
Pilot Study 56
Operationalizations 57
Independent variable 57
Dependent variables 58
Moderating variables 60
Data Analysis 64
CHAPTER FOUR: FINDINGS 66
Description of Participants 66
Gender 66
Age 68
Ecommerce experience 69
Willingness To Disclose 69

Descriptive Statistics for Willingness to Disclose 69
Hypothesis 1 – Nationality Effects on Willingness to Disclose 77
Hypothesis 2 – Impact of Perceived Benefits on Willingness to Disclose 79
Hypothesis 3 – Impact of Personality on Willingness to Disclose 84
Hypothesis 4 – Impact of Trust on Willingness to Disclose 89
Summary of Hypotheses Related to Willingness to Disclose (H1-H4) 93
Attitude Toward Disclosing Information 94
Hypothesis 5 – Attitude toward disclosing information online in general 94
Anxiety About Disclosing Personally Identifying Information 97
Hypothesis 6 – Anxiety over disclosing PII 97
Hypothesis 7: Perceived Risk of Disclosing PII items 103
CHAPTER 5: DISCUSSION 108
Hypotheses Summary 108
Review of Study Variables 110
Nationality 110
Ecommerce Experience 112
Perceived Purchase Benefits 112
Personality 113
Trust – In the Internet and Institutions 114
Attitude toward disclosing 116
Anxiety toward disclosing 116
Further Examination Of Willingness To Disclose Versus Perceived Risk 117
The relationship between willingness to disclose and perceived risk 117
Conceptualizing the Willingness-Risk Gap: Online Disclosure Consciousness 124
Applying Online Disclosure Consciousness to Compare Americans and Estonians 128
Role of Risk-Taking as Personality Trait in Online Disclosure Consciousness 130
Implications 132
Developing the Online Disclosure Consciousness Continuum Model 133
Implications for Theory 137
Implications for Consumers 139
Implications for Practice 140
Implications for Public Policy 143
Limitations 145
Future Research 148
Conclusion 151
REFERENCES 152
APPENDIX A: Mturk HIT assignment directions and Informed Consent statement 183
APPENDIX B: Overview of Mturk HIT assignment details 184
APPENDIX C: English Survey Instrument 185
APPENDIX D: Estonian participant survey directions and Informed Consent statement 199
APPENDIX E: Estonian Survey Instrument 200

CHAPTER ONE:

INTRODUCTION

An important foundation of modern ecommerce involves consumer disclosure of personal information during online transactions. As a part of completing their normal daily activities, consumers may actively engage with the Internet in numerous ways: purchasing clothing from Amazon, renting movies from iTunes, booking flights on Orbitz, or searching for local restaurant discounts on Groupon. Most consumers perceive these daily online interactions aimed at obtaining basic products and information as both routine and innocuous, yet individual consumers are asked to divulge a great deal of personal information in the course of completing what have now become billions of worldwide daily Internet transactions. Individual consumers worldwide disclose all kinds of potentially sensitive personal information when completing such transactions, from the details of credit card purchases, to phone numbers, home addresses, and more.

With the ever increasing frequency of private information exchanged over the Internet, protecting personal information revealed during online transactions has become critically important. The lack of comprehensive policies in the US aimed at protecting consumer privacy and controlling access to consumer information has created a sense of urgency around issues of consumer privacy, and rightly so. Issues such as global losses of $11 billion in 2012 due to cyber fraud (Quested, 2014) underscore the need to develop better ways to protect consumers. Further, with 2013 having been declared the worst year to date for online data breaches (Acohido, 2014), consumers themselves are now placing pressure on government entities to protect their privacy and personal information.

Worldwide, entities in Europe and elsewhere are implementing privacy legislation to protect online consumers, including during ecommerce transactions. Legislation is a key step in protecting people's personal information, but policy makers also need to understand how consumers across the globe engage with ecommerce, disclosing the personal information necessary to complete various Internet transactions. In order to protect consumer information online, as well as to increase ecommerce across the globe, there is a need to understand what underlies consumers' willingness to disclose private information during online purchases. This study thus explores how, why, and under what circumstances consumers are willing to disclose personal information in ecommerce transactions.

Background: Ecommerce and online disclosure

The online marketplace is a complex web of merchants and consumers. Through ecommerce, the ability to purchases goods and services on the Internet has become an important part of consumers' lives, with vast economic impact. In 2013, for instance, total sales from online shopping surpassed $1 trillion globally for the first time (Leggatt, 2013, para. 1). Moreover, global sales for 2014 are predicted to surpass $1.5 trillion (Briggs, 2014, para. 1). As ecommerce becomes a global business tool, digital customers—estimated in 2013 at 1.03 billion (eMarketer, 2013)—will undoubtedly continue to expand.

Laudon and Traver (2003) define ecommerce, or the purchasing goods or services online, as "digitally enabled commercial transaction[s] between and among organizations and individuals" (p. 10). Others describe ecommerce as a "networked information system that serves as an enabling infrastructure for buyers and sellers to exchange information, transact, and perform other activities related to the transaction before, during, and after the transaction" (Varadarajan & Yadav, 2002, p. 297).

Worldwide, roughly 2.7 billion people have Internet access (International Telecommunication Union, 2013), with Internet adoption expected to increase exponentially across the globe in the coming decade. As the number of Internet users increases, so does the acceptance and usage of ecommerce. With continued Internet penetration, the expansion of ecommerce from national markets will continue to grow as a global phenomenon, crossing nearly all national boundaries.

When consumers purchase products or services online, they engage in an exchange of service for information and are required to provide information necessary to complete the transaction (such as home address, phone number, or credit card information). This process of providing general personal information is defined as *disclosure*. When such disclosure takes place on the Internet it is termed *online disclosure.*

Disclosure takes many forms. In the interpersonal communication literature, *self-disclosure* is the process of divulging personal information to another individual (Cozby, 1973; Petronio & Durham, 2008; Wheeless, 1976). Self-disclosure is an important aspect of relationships in general; it is both a relationship management strategy, and an act of closeness (Cozby, 1973; Sprecher & Hendrick, 2004). Self-disclosure is measured utilizing three parameters (1) *breadth*, the quantity of information disclosed, (2) *depth*, the intimacy of information, and (3) *duration*, the amount of time spent describing information (Cozby, 1973). The process of self-disclosure occurs throughout an individual's life, and can take place in many scenarios: when patients discuss medical history with physicians, when friends discuss secret details with other friends, and when parents share family details with their children. The common foundation of each scenario is that self-disclosure involves sharing or providing personal or potentially sensitive information to another person.

Disclosure also comes into play in online relationships (Joinson, 2001; Krasnova, Kolesnikova, & Guenther, 2009; Nguyen, Bin, & Campbell, 2012). In the case of social networking sites such as Facebook, self-disclosure is "the amount of information shared on user's profile as well as in the process of the communication with others" (Krasnova & Veltri, 2010, p. 2). Studies have identified gender differences in disclosure in online communication (Punyanunt-Carter, 2006) as well as cultural differences in patterns of self-disclosure (Chen, 1992; Durand, 2010). In online social platforms, including games, blogs, and social networks, individuals are more likely to disclose personal facts (including quite sensitive information) when friends are involved in the same platform (Taddicken, 2014). In contrast to offline interpersonal self-disclosure, online self-disclosure occurs more quickly and at a deeper level (Barak & Bloch, 2006; McCoyd & Kerson, 2006).

Building on such studies of self-disclosure, communication scholars have developed a useful framework for how people decide whether to divulge or avoid information disclosure, whether online or offline: Petronio (2002) outlines communication privacy management theory (CPM) as a potential "first step toward building a theory of online privacy management" (Metzger, 2007, p. 21). CPM has been applied to the study of interpersonal and online relationships, as well as to privacy concerns involving ecommerce. Although CPM does not provide the main theoretical framework for this study, this theory is useful in that its tenets underscore the fact that people do consciously manage what they disclose.

CPM frames self-disclosure as a privacy management tool that consumers use to help decide whether to divulge or protect potentially sensitive information. The process is well worth noting here, because how, when, and whether people decide to disclose personal information in ecommerce is an important concern when considering issues of privacy, including how to update

online privacy law. Researchers such as Derlega and Chaikin (1977), for instance, have noted that "reconceptualizing self-disclosure as a form of boundary adjustment in the maintenance of privacy may provide a useful framework for integrating the self-disclosure literature" (p. 1). Because personal decision-making about self-disclosure is a factor that might easily be manipulated by savvy marketers, the psychological factors associated with self-disclosure should be strongly taken into consideration as lawmakers approach setting policies for online transactions.

Privacy and disclosure

The concept of privacy has been defined in a number of ways: Warren and Brandeis (1890) observe "the principle which protects personal writings and any other productions of the intellect of or the emotions is the right to privacy" (p. 213). Markel (2005) interpreted privacy as an "individual's right to control access to his or her personal information within defined contexts" (p. 202). Westin (1967) defined privacy as an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent that information is communicated to others" (p. 7). In further conceptualizing privacy, Mesch and Beker (2010) argue that privacy is a "general human need" (p. 570). While the United States does not have a single, comprehensive law governing privacy rights (Sessler, 1997), scholars and consumers typically cite the Fourth Amendment as the basis for the right to privacy, even though this amendment applies only to "actions of the federal, state, and local government" (Sipior, Ward, & Mendoza, 2011, p. 6). Some state constitutions in the US also explicitly grant the right of privacy to individuals (Griffin, 1991), but few legal protections exist to govern how consumers' personal information is used by the private sector (Sipior et al., 2011). Wang (2011) notes because the definition of privacy varies by individual, depending on factors such as

personality, geographical origins, and political and religious beliefs, it is extremely difficult to arrive at an all-purpose definition of the term. Further emphasizing how difficult it can be to conceptualize and define privacy, Gavison (1980) states:

> "Privacy" is a term used with many meanings. For my purposes, two types of questions about privacy are important. The first relates to the status of the term: is privacy a situation, a right, a claim, a form of control, a value? The second relates to the characteristics of privacy: is it related to information, to autonomy, to personal identity, to physical access? (p. 424)

In this view, the definition of privacy may vary according to context, suggesting a number of possible factors that enter into decision-making about self-disclosure.

Other researchers, such as Wang (2011) emphasize that privacy can further be defined as an amount that can be lost or gained (p. 7). Importantly, as this chapter argues, the categories of responsibility (voluntary or involuntary) and the parties involved (whether acting as an individual or an agent on behalf of another) are also significant for arriving at a satisfactory definition of online privacy. For example, when Individual X places photos of him- or herself on Facebook, that individual has decreased his or her own degree of personal privacy and has done so in a voluntary way. In addition, if Individual X places an unsolicited photo of a friend (individual Y) on Facebook, then individual X has decreased Individual Y's privacy, and has done so without the other person's volition. That is, Individual Y has not consented to having the photo uploaded and may indeed be unaware of its presence on the Internet. Individual Y's friend has, perhaps unknowingly, violated another's privacy and may have no idea whether Y would have wanted the photo to appear on Facebook, or whether his friend had privacy concerns that would make him reluctant to have his photos posted on a website.

As this example shows, privacy serves a number of individual, social, and cultural functions. At the individual level, privacy is critical for the development of the self (Plaisance,

2009), providing opportunities for the experimentation and self-assessment that help develop individuality (Westin, 1967). In addition to privacy's functions at the individual level, privacy serves an important social function by helping build social cohesion (Plaisance, 2009). Culturally, privacy involves four universal features: (1) individuals create social distance as an important part of social interactions, (2) individuals think they are truly never alone, (3) invading another's privacy either prevents antisocial contact or creates a perceived social benefit, (4) and the more complex a society, the greater opportunities for psychological and physical privacy (Westin, 1984). In many ways, privacy is pro-social, functioning to help build relationships by setting limits on both how much and to whom personal information is revealed.

Looking beyond privacy's role in creating social cohesion, privacy may also be viewed either as an intrinsic or an instrumental value. When individuals treat privacy as an end in itself, privacy becomes an intrinsic concern, valued for itself. Conversely, individuals, who see privacy as instrumental, value privacy primarily for what it enables them to do: develop relationships, as well as generate and initiate anonymity. The notion of privacy as an instrumental right can be derived from its cultural and social construction (Friedlander, 1982; Plaisance, 2009). The instrumental definition of privacy underscores the notion that privacy carries both rights and responsibilities, opening up the possibility for setting legal definitions for privacy.

Lastly, it is important to note that individuals may either desire or evade privacy (Bryce & Klang, 2009). While one person might appreciate the freedom to control how their information is used, others may be apathetic to the entire concept of privacy and information protection. This difference shows how self-disclosure can actually be seen a privacy protection mechanism. Further, the relationship between privacy and self-disclosure is not always clear. As Joinson and Paine (2007) posit:

> Privacy is particularly important for understanding self-disclosure, since the relationship between privacy and self-disclosure is somewhat paradoxical. Privacy is a prerequisite for disclosure, and yet, the process of disclosure serves to reduce privacy (p. 245)

Self-disclosure and privacy clearly go hand in hand, since privacy concerns are a significant aspect of decision-making around all types of self-disclosure (Mesch & Beker, 2010). Disclosure in ecommerce signifies that the consumer has accepted the website's privacy assurances and trusts the site (Bargh, McKenna, & Fitzsimons, 2002; Joinson & Paine, 2007). Yet privacy issues are much more complex in online self-disclosure than in other types of interpersonal communication, since online communication involves a variety of actors, some of whom may be unknown to the person revealing his or her information in an online format.

The issue of privacy has gained more and more attention as consumers have become progressively more aware of the complex array of privacy concerns in online environments (Krasnova et al., 2009). In response, scholars have begun to delve more deeply into issues of privacy online and to question the effect that privacy needs and potential privacy violations have in online self-disclosure (Krasnova et al., 2009). According to Petronio and Durham (2008), CPM's broader view of self-disclosure makes an important contribution to the debate by showing how privacy and self-disclosure are not merely related concepts, but rather combine to create private disclosures. Additionally, Petronio asserts “CPM makes private information, as the content of what is disclosed, a primary focal point” (Petronio, 2002, p. 3). Joinson, Reips, Buchanan, and Schofield (2010) concluded that an individual’s privacy concerns directly influences an individual’s willingness to disclose information online. Further, Krasnova et al. (2009) identified privacy concerns as significant hurdles to self-disclosure online. Social network users, for example, are constantly engaged in balancing their private information, while still engaging in and receiving pleasure from online social network activities. Even though a user of

an online social network third-party application is often warned in advance of the potential for his or her information to be collected and used, the individual may decide to actively engage in the application.

Krasnova et al. (2009) argue that a user's decision to bypass *privacy warnings* (disclosures by organizations about their practices to the use of information provided online) and freely utilize an application can be attributed to a consumer's attraction to instant gratification and enjoyment, which often override vague and less immediate concerns about privacy risks. Moreover, the privacy risks inherent in online communication will continue to exist as long as consumers are willing to reveal personal information in the process of "looking for fun" (Krasnova et al., 2009).

At first glance, the decision-making process involved in whether or not to disclose seems hard to explain. CPM theory states, for instance, that individuals are constantly maximizing rewards and minimizing the costs associated with self-disclosure, revealing information by using criteria such as risk-benefit analysis (Petronio, 2002). Petronio (2002) finds that it is "necessary to control our privacy boundaries…because we need to balance the risks and gains of revealing private information" (p. 65). Yet in deciding how much to reveal online, people may underestimate the risks of self-disclosure, revealing more than is safe in an online venue because it appears either neutral or accepting. Whether or not people are able to protect their boundaries around private information online depends to a great degree on that individual's understanding of the potential consequences of sharing such information, as well as on their comprehension of how and by whom that information may be used or shared.

Privacy is affected by self-disclosure, and influenced by *trust* as well as *anonymity.* Trust, "the willingness of a party to be vulnerable to the actions of another party based on the

expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer, Davis, & Schoorman, 1995, p. 712) is another important aspect of deciding whether or not to self-disclose. The perceived trustworthiness of a conversant or organization will affect a person's willingness to disclose information to that entity, so trust is as important in online communication as in interpersonal communication.

Krasnova, Spiekermann, Koroleva, and Hildebrand (2010) note to encourage trust in their users, online social networks need to implement fair privacy policies, as well as to clearly define the consequences of privacy abuses. For Krasnova et al. (2010) social networks must "behave in a consistent and fair manner" with network users (p. 122). At the same time, Joinson et al. (2010) have noted how anonymity (a form of privacy) can increase self-disclosure, since trust issues may become irrelevant to a person who feels anonymous. These research findings underscore the argument that Internet users are not equally skilled at evaluating whether or not to trust. Many users do not understand that their self-disclosures could later be used against them, while the belief that they are anonymous may lead some users to share personal information more recklessly than they might do in other, more familiar settings.

According to Suler (2002) individuals involved in online interactions are more likely to loosen up, may be less guarded in expressing their ideas, and may feel generally less inhibited. Anonymity, which means a person assumes his or her real identity is neither sought nor known, comes into play in the decision-making process in part because many people assume they are anonymous in the online environment. Many people have the tendency to say or do things they might not say or do in a face-to-face environment (Suler, 2004). While anonymity is important in online free speech, it is not as relevant in ecommerce, because consumers must identity

themselves to receive the desired product or service. Here, anonymity may not be of value to either a company or a consumer.

Anonymity can be expressed either in the visual or the discursive online fields (Scott, 2004). Visual anonymity refers to the situation “when one cannot sense the physical presence of a message source” (p. 129), whereas discursive anonymity is related to verbal communication, when “specific comments cannot be attributed to a specific individual source” (Scott, 2004, p. 129). Many of us have experienced the feeling that "no one will know" when we write or post something out of character. The feeling the online environment is anonymous may spark a sense of bravado; however, online anonymity is virtually an oxymoron, since we also know online activity is traced and catalogued and is quite difficult to keep private in any sense of the word. Online activity is more or less "public," and anonymity is only anonymous until someone tries to "find out" who we are.

Computer mediated communication (CMC), in the context of chats or bulletin boards, encourages people to accept the concept of anonymity at face value. Indeed, anonymity seems plausible since we see that commentators do indeed leave online comments with no visual identification. This aspect of online communication makes people feel "no one is watching," giving users a sense that others are somehow "not really there" and fostering the appearance that all users belong to the same social group (Walther, 2011). Additionally, Tidwell and Walther (2002) compared face-to-face and CMC in order to understand how relationships are formed in each situation, and found due to their sense of anonymity, individuals in the CMC group were more likely to elicit and disclose personal information than were members of the face-to-face group. Because individuals in the CMC group used emails setup solely for the study, the CMC group was able to maintain anonymity while the face-to-face group was not. Further, Walther,

Pingree, Hawkins, and Buller (2005) noted how email and Internet-based chat systems allow for hiding the sender's identity separately from the content of the message sent. The feeling of being anonymous thus becomes problematic in online communication when we feel we cannot be identified and so believe divulging personal information is safe while at the same time online communication may be shared in ways the naïve user may never expect.

Personally identifying information (PII)/Personal data

Much of the self-disclosure literature deals with feelings, anxieties, passions, desires, and intentions – not personal facts or data. This distinction is important in the case of ecommerce, where consumers disclose more sensitive, unique personal information. Through the act of online disclosure, individuals reveal private and/or sensitive facts about themselves that may or may not be readily available through other public channels. Every individual is, of course, a unique entity, in possession of characteristics and traits (such as fingerprints, date of birth, or DNA) that can be utilized for identification for various purposes. Personal data are one way of identifying a person, and personal data are pieces of "information relating to an identified or identifiable natural person," with an identifiable person defined as someone who can be identified, directly or indirectly, by "one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (IAPP, 2014, para. 1). Sometimes used interchangeably with "personal data," the term "personal information" refers in the US to *personally identifiable information* or *PII* (IAPP, 2014; United States Government Accountability Office, 2008).

Personally identifying information, or PII, is a subset of general personal information. PII is defined by the United States Government Accountability Office (2008) as:

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an

> individual, such as medical, educational, financial, and employment information (p. 1).

The term PII originated in US policy and information technology security. It was originally described by the Federal Trade Commission (FTC) in a report to the U.S. Congress regarding online profiling of consumers (Federal Trade Commission, 2000a). Subsequently, the term was further developed and investigated in multiple government reports, including an Executive memorandum (Johnson, 2007), the United States Government Accountability Office (2008), US Department of Commerce (Neal, 2009), the US National Institute of Standards and Technology (McCallister, Grance, & Scarfone, 2010), and most recently, a privacy-awareness training program by the United States Department of Health and Human Services (2014).

Contradictions exist among various departments in the US government of what constitutes PII. The 2012 US Department of Homeland Security report cites name, email, home address and phone number as examples of PII (Callahan, 2012), while United States Department of Health and Human Services states that name, social security number (SSN), date of birth (DOB), mother's maiden name, financial records, email address, driver's license number, passport number, and health information are types of PII (United States Department of Health and Human Services, 2014). Interestingly, several of these items identified by the US-HHS are included as "sensitive PII" by US Homeland Security, specifically SSNs, DOBs, financial records (such as "financial account numbers"), driver's license numbers, and passport numbers.

Building further on the federal government's definition, US Department of Homeland Security defined PII as "information that permits the identity of an individual to be directly or indirectly inferred," and includes any information that is "linked or linkable to that individual, regardless of whether the individual is a US citizen, legal permanent resident, [or] visitor to the U.S" (Callahan, 2012, p. 4). The Department of Homeland Security further refines PII by

identifying what is considered *sensitive PII* (see Table 1.1) as PII "which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual" (Callahan, 2012, p. 4). A recent study sought to redefine PII in terms of, "general or group identifying information, information that can be used to identify uniquely, to contact, or to locate a single person or group of persons" (Poritz, 2007, p. 385). Importantly, any information not deemed "PII" is defined by federal government agencies as "non-PII" (Baker & Matyjaszewski, 2010). Notably, non-PII may become PII whenever supplemental information is publicly available that can be used to identify the individual when combined with other available data (United States General Services Administration, 2013).

The US General Services Administration states that PII is not defined by any single category of information or technology; rather, identifying data should be approached case-by-case based on the odds of identifying the individual. In contrast to the GSA's assertion that PII is not defined by a specific category of information, other US government departments define specific examples of PII.

Table 1.1
Department of Homeland Security's Classification of Types of Sensitive PII

If information stands alone:	**If paired with another identifier:**
Social Security number	Citizenship or immigration status
Driver's license or state ID #	Medical information
Passport number	Ethnic or religious affiliation
Alien registration number	Sexual orientation
Financial account number	Account passwords
Biometric identifiers	Last 4 digits of Social Security number
	Date of birth
	Criminal history
	Mother's maiden name

In Europe, legislation protecting an individual's personal information does not refer to PII, as in the United States, but rather to *personal data* (Mcafee, 2014). European law defines *personal data* as "information relating to an identified or identifiable person" (European Union, 1995, p. 38), with an identifiable person being considered an individual whose identity is clear or can be established by providing additional information (European Commission, 2014). In contrast to PII, which can be defined by multiple forms of information, personal data can be any kind of information related to a person, including information pertaining to an individual's private or public life (European Commission, 2014).

American industry has largely adopted the definition for PII as provided in the original FTC report. Indeed, marketers rely on PII to provide services as well as to complete transactions. Marketers insist, without having access to personal data, they would be unable to reach customers with relevant offers "at the right time," adding that they also need personal information to understand consumer's product preferences (DMAaction.org, 2011).

Clearly, the boundary between PII and non-PII information is blurring (Brill, 2010). For this study, PII and personal data will be used interchangeably and will be defined as necessary information for completing online purchases. Building upon Treiblmaier and Chong (2011), examples of PII/personal data include name, email address, home address, telephone number, and credit card number as information vital to completing ecommerce transactions. In addition, PII will include date of birth, annual income, credit history, medical history, age, marital status, Twitter handle, Skype username, PayPal account, and Facebook profile.

Estonia versus United States

As the number of consumers engaging in ecommerce increases, investigating ecommerce's effect on disclosure is important for understanding how consumers divulge and

protect personal information. More importantly, as the digitally connected society continues to expand and develop, it will be important to understand how consumer disclosure practices evolve and to pinpoint factors that might influence them. Importantly, the United States is not necessarily the only model. Valuable insights can be gained from studying disclosure patterns in other countries that already function at the forefront of technology, such as Estonia, because these patterns can help provide a model for how different societies have and will adopt and embrace technology in the future. Although this study compares ecommerce, privacy, and policy, in the US and Estonia, the US is used as a starting point for comparison. Thus, while this study's primary concern is to examine how privacy issues comparatively impact Estonian and US citizens, it also aims to influence and possibly improve US policy regarding the protection of personal information online. As the basis of comparison, the countries of Estonia and the United States provide strong contrasts.

Estonia, a former Soviet nation with independence since 1991, is a member of the European Union and NATO. Estonia, perhaps more than other former Soviet Republics, has made an extraordinary commitment to adopting the Internet and using it in a number of important social settings. Davis (2007) argues that Estonia "is like a window into the future" (para. 9) that provides a glimpse into how many societies will adopt and use technology, creating digital citizens. Estonia serves as a precursor of the constantly connected society and digitally connected citizen. Because Estonia is a pioneer in e-government, ranked first in the world for Internet freedom (Keefer, 2012), and is one of the most wired and technologically advanced societies in the world (Freedom House, 2014), its experience can provide helpful lessons for others seeking to implement similar systems.

As will be detailed in Chapter 2, Estonia possesses five main attributes that make it particularly valuable to the current study: advanced standing of technological systems, advanced legislation and regulations intended to foster the use of communication technology, a culture that is collectivist and long-term oriented, a high level of citizen proficiency with the Internet, and a unique aversion to risk due to a historic cyber-attack.

RATIONALE

This study represents a potentially important contribution to the understanding of online consumer behavior and could potentially benefit both businesses seeking to maximize their effectiveness in conducting ecommerce and governments concerned with consumer attitudes and practices related to online disclosure. Across the globe, businesses are striving to promote the adoption of ecommerce—a process influenced by marketing practices, culture, the political environment, technology, and consumer behavior and confidence, including concerns regarding online privacy. This study offers insights into how consumers self-disclose via ecommerce platforms, exploring and informing consumers' privacy concerns, and to do so proposes a conceptual model. Seminerio (1998) observed, “Ensuring the validity of online transactions, along with assuaging consumers' privacy fears, is key to the growth of ecommerce.” (para. 7). Finding ways to alleviate consumer fears about risks to their online privacy and protection of their personal data has the potential to exponentially increase the adoption of ecommerce, particularly in business-to-consumer (B2C) marketing.

Discovering regional or national differences in consumers' willingness to disclose personal information can also benefit both businesses and governments. Despite arguments about media technology homogenizing world culture, marketing practices are not universal, but must be adapted to local circumstances. Effective organizations might think globally, but they must

act locally in order to prosper (Endline, 2013). By exploring possible differences in online disclosure, businesses can better understand the nuances of conducting ecommerce in different nations and might be able to adapt their strategies. Understanding national perspectives in online disclosure can benefit government policy, as governments around the world seek to establish comprehensive privacy policies.

Understanding the details of how privacy concerns in the digital age affect different people, governments, and businesses will become increasingly important as more and more countries become fully digitally connected. For instance, this study, and others like it, could help provide national governments seeking to adopt more secure e-government systems (such as online voting, digital health records, or online tax processing), with insights into how privacy concerns affect people's willingness to self-disclose during digital transactions.

OVERVIEW

The remaining sections of this dissertation are organized into four main parts. Chapter 2 contains the literature review, conceptualization of variables, and outline of the hypotheses that are the basis for the study. Chapter 3 details the methodology for the two parallel online surveys conducted as the basis of comparison between the US and Estonia, including a description of procedures for the recruitment and instrumentation of the surveys in both countries. Chapter 4 contains the results of the study, while Chapter 5 discusses its implications.

CHAPTER TWO:

REVIEW OF LITERATURE

CONCEPTUAL FRAMEWORK

This study will test an exploratory model to examine the effect of nationality on the disclosure of personally identifying information during online ecommerce transactions. As outlined in Figure 2.1, several variables moderating the effect of nationality, the study's independent variable (IV), have been identified to test in this model. The disclosure of information online during ecommerce transactions will be analyzed using four dependent variables (DV) intended to provide alternative ways to assess outcomes.

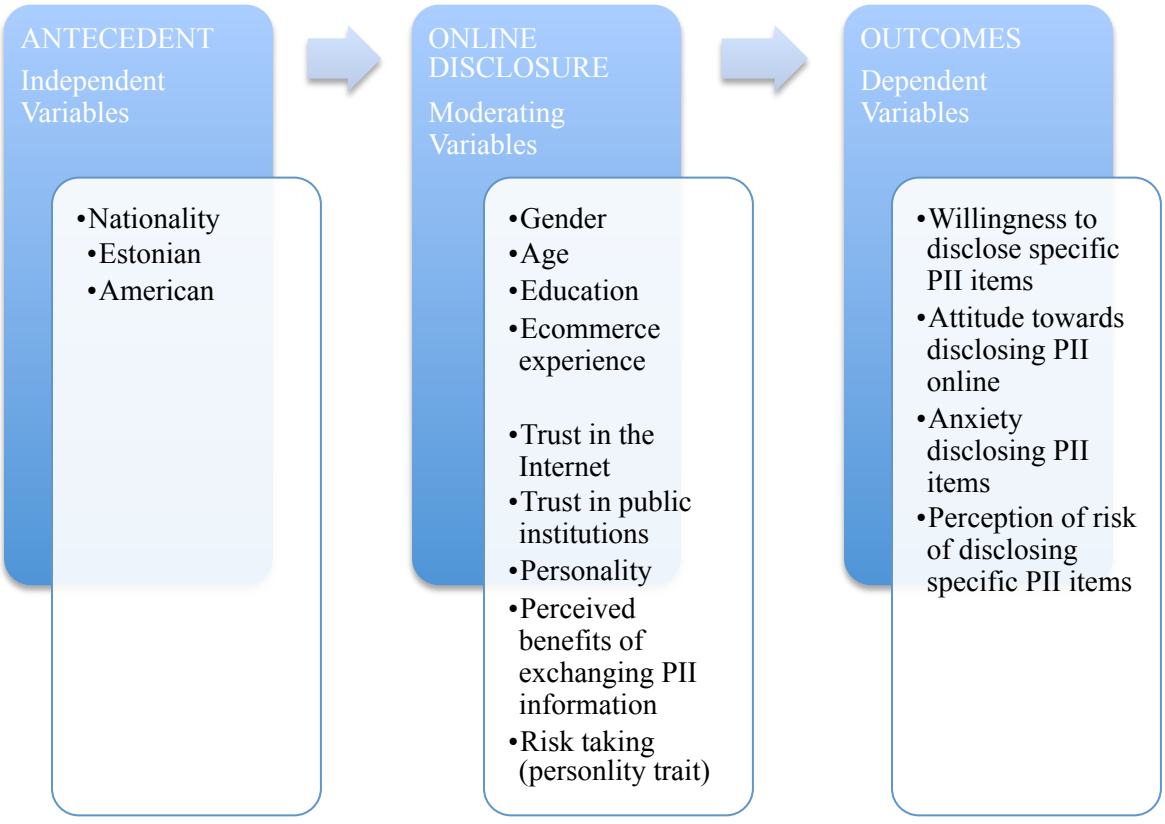


Figure 2.1: Study Framework

INDEPENDENT VARIABLE

Nationality

The independent variable in this study is *nationality*, defined here as differences in patterns of behaviors between people residing in one country (nation-state) versus another. More generally, nationality has been defined as "the collective identity that the people of the nation acquire by identifying with the nation" (p. 19). Essentially, nationality is a form of group identity (Oommen, 1997).

This study follows numerous other studies focused on cross-national comparisons. Cross-national and cross-cultural research in ecommerce has primarily shed light on differences in how ecommerce is adopted and utilized across the globe. For example, in a comparison of online shoppers in the United States and Saudi Arabia, Brosdahl and Almousa (2013) found that American shoppers had a more positive attitude toward ecommerce purchases, as well as greater intention to shop online. Comparing shoppers in the United States and South Korea, Choi and Geistfeld (2004) posited that cultural values served as antecedents to perceived risk, subjective norm, and perceived self-efficacy. In studying differences in ecommerce habits of French and American teenagers, Gentina, Butori, Rose, and Bakir (2013) found that French teens' purchasing behaviors were influenced by social assimilation, where American teens were influenced by distinctiveness and uniqueness. Additionally, Capece, Calabrese, Di Pillo, Costa, and Crisciotti (2013) identified cultural factors such as power distance and individualism as the main cultural factors affecting ecommerce adoption in Italy.

As ecommerce adoption increases globally, it is vital to understand how nationality affects ecommerce usage. In addition, it is important to continue to expand ecommerce studies beyond the US, since cultural characteristics of ecommerce in the US are not necessarily the

same in other countries. Understanding how American companies define and relate to different cultural characteristics and patterns of online behaviors across national and cultural boundaries is important for businesses that seek to expand their ecommerce into international markets. Gefen and Heart (2006) underscore the necessity of studying additional nations and cultures, as virtually "all ecommerce trust is based on studies in the US" (p. 18). Most importantly, Gefen and Heart (2006) posit that national culture as a variable must be utilized in studies exploring ecommerce.

Estonia

A comparison of the United States and Estonia certainly provides strong contrasts. Estonia is one of the most advanced nations in the world in terms of Internet usage, serving as a strong example of a society whose citizens are in constant digital connection. Table 2.1 provides a statistical profile of Estonia compared to the United States.

Although Estonia is small in population (1.3 million) and area (17,413 square miles) (VisitEstonia.com, 2014a), the country has a disproportionately large global impact on digital lifestyles and technological innovations, thus serving as a good contrast to the US. Estonia possesses five main attributes that underscore its importance globally and serve as solid rationale for the current study: advanced standing in technological systems, advanced government legislation and regulations, a culture that is collectivist and long-term oriented, high level of citizen proficiency with the Internet, and a distinct aversion to risk.

Table 2.1
National comparisons of United States and Estonia

Characteristic	United States	Estonia
Population	316,668,567	1,266,375
Total area (sq. miles)	3,794,100	17,463
Gross domestic product ($)	15.660 trillion	24.690 billion
GDP per capita ($)	49,800	19,100
Labor force	154,900,000	688,000
Unemployment rate (%)	8.20	17.50
Population below poverty line (%)	15	19
National government annual budget ($)	2.465 trillion	7.851 billion

Source: Countryreports.org (2014a, 2014b)

Advanced technological systems

Estonia's technological systems are advanced. The country provides nearly ubiquitous Wi-Fi coverage (Horvitz, 2008), and has already set in place plans for the 2015 completion of a fiber-optic network that will span the entire nation (Estonian Ministry of Foreign Affairs, 2010). Estonia, the birthplace of Skype, is considered a digital pioneer (VisitEstonia.com, 2014b), and it was the first country to allow online voting in a general election (A.A.K., 2013). The country is considered one of the most wired and technologically advanced in the world (Freedom House, 2014). In addition to its advanced technological systems, Estonia has the fifth highest number of mobile phones per capita, with 1,500 cellular phones for every 1,000 citizens (VisitEstonia.com, 2014b). Recently, Estonia built and now uses the world's first nationwide electric vehicle (EV) charging network for hybrid and electric vehicles (ABB, 2013). Through the most technologically advanced digital identification system in the world (E-estonia.com, 2014a), citizens can view many personal records online, including their educational records, medical records, current and previous addresses, full employment history, and traffic offences (Herlihy, 2014). Estonia is a small country with big technology.

Tallinn, Estonia's capital, further demonstrates how this country of advanced technology provides a glimpse into digital societies of the future. Tallinn's transportation system relies heavily on the country's advanced technology and Internet systems. To ride the local bus system (free to all residents), one must purchase a 2 Euro (~$2.75) smart card that is waved in front of a sensor on the bus (Nelson, 2013). When mailing a package at the local post office, residents use their cellphones to request a code in order to open a locker. Once their package is placed in the locker, the package begins its journey (Nelson, 2013). For parking, residents text the local parking authority with their car identification number and the parking lot's numeric identifier (Nelson, 2013). Through a digital billing system, residents pay for parking through electronic charges on their cellular phone bill. Technology is a constant feature of life in Tallinn and throughout Estonia.

Advanced legislation and regulations

Another significant feature of technological society in Estonia can be seen in recent advances in the country's legal system regarding technology and the Internet. Estonia has adopted advanced legislation and regulations, and established one of the world's first comprehensive privacy policies dealing with personal data (Privireal, 2005). As the majority of the world struggles to develop and implement privacy policies, Estonia's privacy legislation has evolved along with technology and the Internet. As an EU member nation, Estonia advises the EU on both its General European Data Protection Regulation and its Data Protection Law Enforcement Directive, whose goals are to expand digital privacy rights and help regulate how personal information is processed within the EU.

The Estonian government was the first fully digital government, labeled the "first paperless government" (Woodard, 2003) in which all government activities are conducted in an

online environment (Estonian Information System's Authority, 2006). Recently, the Estonian and Finnish governments completed the world's first digitally signed international agreement, which governs e-services between the two neighboring countries (Friedman, 2013). Because of its advanced legislation, regulation, and technological systems, Estonia produces the highest number of tech startups per capita in Europe and is ranked first in the world for Internet freedom (Keefer, 2012). Showcasing the advanced regulatory processes in Estonia, citizens can formally register a business online in only 18 minutes (Herlihy, 2014). Even more than Americans, Estonians count on the digital universe to complete transactions of all kinds, from paying for a bus ride, to voting and conducting business. Estonia may be a small country, but it is a big player in the digital world, a potential model for other countries in the future.

Culture

Compared to the US, Estonia possesses unique, contrasting cultural traits that serve as important aspects in this study. Hofstede identified a series of 6 cultural dimensions that can be used to distinguish nations and regions of the world. Hofstede's (2011) cultural dimensions, are based on underlying cultural values and mores, including *power distance* (PDI), *individualism versus collectivism* (IDV), *masculinity versus femininity* (MAS), *uncertainty avoidance* (UAI), *long-term versus short-term orientation* (LTO), and *indulgence versus restraint* (IND). Using Hofstede's criteria to analyze cultural differences between Estonia and the US reveals a number of striking differences.

Estonia's main cultural differences from the US can be categorized primarily along the dimensions of indulgence versus restraint (IND), masculinity versus femininity (MAS), long-term versus short-term orientation (LTO), and individualism versus collectivism (IND) (see Table 2.2). Hofstede (2014a) labels Estonia as an individualist society. Yet with a score of only

60 out of 100 (where 100 is highly individualistic) it is a country that readily identifies culturally as both European and Nordic. The country can thus be seen as a *weak* individualistic society, whereas the United States, with a score of 91, is a *strong(er*) individualist society. Because its citizens are driven by a sense of modesty and fairness, Estonia is considered, in Hofstede's terms, a *feminine* society, and does not readily boast about accomplishments (Hofstede, 2014a). A society whose perspective is future-oriented, Estonia would be labeled a long-term oriented culture, where the United States showcases a historically short-term perspective. Lastly, Estonia is a restrained society that "suppresses gratification of needs and regulates it[self] by means of strict norms" (Hofstede, 2014b, para. 6). In contrast, the United States is a self-indulgent nation that "allows relatively free gratification of basic and natural human drives related to enjoying life and having fun" (Hofstede, 2014b, para. 6). The strong differences in self-image and historical perspective between these two societies thus make them good candidates for comparison.

Table 2.2
Cultural dimensions comparison: US and Estonia

Cultural Dimension	United States	Estonia	Difference
Power Distance (PDI)	40	40	0
Individuals vs. collectivism (IDV)	91	60	29
Masculinity vs. femininity (MAS)	62	30	32
Uncertainty avoidance (UAI)	46	60	-14
Long-term vs. short-term orientation (LTO)	26	82	-56
Indulgence vs. restraint (IND)	68	16	52

Source: Hofstede (2014a, 2014b)

Internet and technology proficiency

Belonging to one of the most digitally connected societies in the world (Estonia.eu, 2014; Freedom House, 2014), Estonia's citizens are rated as highly proficient Internet users. Estonians fully embrace technology, even seeing it as an important part of their nation's cultural independence (Mansel, 2014). While Estonia is the 132nd smallest country in the world, it is ranked as 30th in the highest percentage of citizens that are Internet users (VisitEstonia.com,

2014b). The majority of Estonians engage in online banking, with 99.6% of bank transactions being conducted online (Estonian Information System's Authority, 2006). Consistent with this level of proficiency in Internet usage, 95% of Estonians filed their taxes online in 2013 (E-estonia.com, 2014b). Citizens of this small Baltic country embrace technology throughout life, beginning at early age. Indeed, most Estonian children are introduced to computer programming by age seven (Olson, 2014).

Aversion to risk-taking

Despite their technical acumen, Estonian citizens are generally averse to risk taking. Although some evidence exists to show that Estonians are willing to engage in some risk-taking behaviors (Kaasik, Andersson, & Horte, 1998), researchers like Hofstede (2014a) argue that Estonians are "careful about taking risks, preferring to reflect on problems for an extended period of time. Therefore, Estonians do not like to be rushed into making decisions" (para. 4). Estonians' natural tendency to avoid risk may have been reinforced by events such as the cyber-attacks that rocked the nation in 2007.

As a result of these cyber-attacks, notable in part because they represented the first time a country was attacked on every digital front and its government retaliated (Davis, 2007), Estonians have ample reason to be risk-aversive regarding online disclosure of personal information. These cyber-attacks may play a vital role in understanding how Estonians make decisions regarding online risk-taking versus risk aversion. Moreover, because the Estonian government communicated directly with its citizens about the severity and reach of the attacks as they unfolded, the attacks served to engender greater trust between citizens and government. This sense of trust has become a foundation of Estonia's advanced e-service industry (E-estonia.com, 2013).

Technology is widely embraced by the Estonian people (Rooney, 2013). As we have seen, it is even seen as an important part of the country's political and cultural independence (Mansel, 2014). But what are the impacts of this digitally connected culture on individuals' self-disclosure and privacy practices online? Shaped by post-Soviet economic and political transformations, Estonia provides a rare opportunity to explore how technology has influenced and shaped individuals' perceptions and inclinations toward collecting and revealing personal information.

This researcher was not aware of literature, available in English, which investigates a digitally connected society and its impact on disclosure of personal information, particularly during ecommerce transactions. Because Estonia is a digital pioneer, many countries around the globe have looked to the country as a model for constructing technology infrastructure, implementing comprehensive privacy policies, and securing e-government solutions.

DEPENDENT VARIABLES

The four dependent measures in this study are (1) willingness to disclose specific PII items, (2) attitude toward disclosing PII online, (3) anxiety about disclosing PII items, and (4) perception of risk of disclosing specific PII items.

Willingness to disclose specific PII items

For this study, the main variable of interest is *willingness to disclose specific PII items,* which is defined as an individual's openness to the idea of providing specific personal information in the context of ecommerce transactions. In general, willingness is defined as being "inclined or favorably disposed in mind" or "prompt to act or respond" (Merriam-Webster, 2014a). Willingness represents a necessary but not sufficient condition for *behavioral intent*, or "a person's subjective probability that he will perform some behavior" (Fishbein & Ajzen, 1975,

p. 288). However, willingness is probably the lowest-order component of behavioral intention, and does not necessarily suggest that the individual has seriously considered the action or actually plans, needs, wants, or is committed to taking a specified action.

Behavioral intent can go beyond mere willingness. It has been defined by Warshaw and Davis (1985, p. 214) as "the degree to which a person has formulated conscious plans to perform or not perform some specified future behavior." Willingness thus has lower predictive value than behavioral intent, which explains why behavioral intent is more used in consumer research. This stress on the difference between willingness and behavioral intent in decision making draws upon Fishbein and Ajzen's theory of reasoned action (see below for the discussion of attitude toward disclosure of PII in general). Rather than looking at specific actions that might be undertaken in response to a request or after exposure to a promotional message, however, the main focus of this study is on general readiness to disclose different types of information.

Expressed willingness to provide PII items online can be an indicator of an individual's personal disclosiveness. Initial exploration into differences among how individuals engage in general self-disclosure can be attributed to Lewin (1935; 1936), who investigated openness between Germans and Americans. Wheeless (1978) described disclosiveness as the tendency, on average, to disclose private information to others across various contexts. He defined disclosiveness as an individual's general openness, noting that some people are more predisposed to openness than others (Wheeless, 1976). To clarify the relationship between disclosiveness and self-disclosure, disclosiveness is a *characteristic* or *personality trait* of an individual, whereas self-disclosure is the *process* through which information is disclosed. Among consumers, willingness to disclose varies based on the purposes for which the information will be used (Goodwin, 1991). An individual's willingness to disclose may be solely determined in some

situations by weighing the perceived benefits and costs of disclosure (Altman, 1973). Additionally, individuals may be more willing to disclose to companies they already have relationships with or to companies that are perceived to be well known (Olivero & Lunt, 2004).

In studies of disclosiveness online, consumers are more willing (exhibit higher disclosiveness) to disclose information in a business-related social network, such as LinkedIn, versus in a private social network such as Facebook (Schaar, Valdez, & Ziefle, 2013). The trait of disclosiveness is positively related to a person's level of disclosure online: an individual high in disclosiveness is more likely to disclose online than an individual with low disclosiveness (Taddicken, 2014). The sensitivity of information requested on a website significantly impacts willingness to disclose (Metzger, 2007). Further, cultural differences in willingness to disclose exist and have been cited (Gupta, Iyer, & Weisskirch, 2010).

This study examines willingness to disclose particular items indentified as personally identifying information, positing that people are normally willing to routinely disclose certain (more public) items (such as name or email), but reluctant to provide more sensitive, less readily available facts about themselves (such as credit card numbers). Marketers commonly ask for a variety of facts about an individual, and understanding people's predispositions toward disclosing particular information can inform the data collection process.

Attitude toward disclosing PII online

As alternatives to willingness to disclose PII, this study sought to examine attitude toward disclosing PII as well as anxiety attendant to making such disclosures.

An attitude is "a learned predisposition to respond in a consistently favorable or unfavorable manner with respect to a given object" (Fishbein & Ajzen, 1975, p. 6). Rokeach (1968) defined an attitude as "a relatively enduring organization of beliefs around an object or

situation predisposing one to respond in some preferential manner" (p. 112). Alternatively, the attitude construct can be viewed as a "psychological tendency that is expressed by evaluation of a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993, p. 1). Further definitions exist (Dillard, 1993; Ledbetter, 2009). Attitude is the cornerstone of a widely used social science theory: the theory of reasoned action. Posited by Fishbein and Ajzen (1975), this theory presents a model for predicting behavior. It contains three main constructs: attitude, subjective norm, and behavioral intent.

Measuring attitude toward an activity, such as disclosing information, is a reasonably reliable indicator of a person's predisposition toward taking an action, although it falls short of measuring behavioral intent (Fishbein & Ajzen, 1975). Research has explored attitude effects in the context of *attitudes toward online self-disclosure* (OSD), which is defined as "the extent to which an individual feels more comfortable when sharing private information in online contexts" (Ledbetter, Broeckelman-Post, & Krawsczyn, 2011, p. 226). As a first step toward validating this construct, Ledbetter (2009) developed an instrument to measure online communication attitudes. The measuring online communication attitude instrument (MOCA) addressed both cognitive and affective beliefs of communicating online, using five dimensions: self-disclosure, apprehension (of communicating online), miscommunication (online communication inhibits shared understanding), social connection (contact with an individual's network is facilitated by online communication), and ease (appreciation of joy and utility provided by online communication).

The notion that attitude toward online self-disclosure can predict communication was substantiated by Caplan (2007), who associated negative attitude toward online self-disclosure with low communication competency. Self-disclosure was found to be inversely associated with relational closeness, Facebook communication (Ledbetter et al., 2011), and the amount of daily

talk, both over the phone and face-to-face (Ledbetter et al., 2011). In a related study, Mazer and Ledbetter (2012) concluded that online communication attitudes, specifically those of self-disclosure and social connection, positively predict compulsive and excessive Internet use.

Overall, attitude toward online disclosure in general is a useful measure for assessing the likelihood that users will engage in online disclosures of personal information, serving as an alternative measure for purposes of this study. Moreover, it is intuitive that individuals with a positive attitude toward disclosing personal information online are more likely to be willing to disclose various specific PII items and are less likely to perceive risks in doing so.

Anxiety disclosing PII items

Because of the potential risks and uncertainty about the prospective outcomes and consequences of disclosing personally identifying information, users can become anxious, creating in them a state of psychological *anxiety*. The American Psychological Association defines anxiety in its *Encyclopedia of Psychology* (Kazdin, 2000) as "an emotion characterized by feelings of tension, worried thoughts and physical changes like increased blood pressure." People with disorders of anxiety will typically have recurring intrusive thoughts or concerns, and they may avoid certain situations out of worry. They may also have physical symptoms such as "sweating, trembling, dizziness or a rapid heartbeat" (American Psychological Association, 2014a, para. 2).

Being anxious is the opposite of being psychologically comfortable. The idea of comfort is an important concept in studies concerning self-disclosure. Much of the literature that attempts to conceptualize *comfort* has originated in the realm of healthcare, which most often defines the concept as "a state of comfort" (Siefert, 2002, p. 16) that is "multi-dimensional, meaning different things to different people" (Hamilton, 1989, p. 32). Comfort has been examined in the

field of ergonomics (Branton, 1969), psychotherapy (Parloff, Kelman, & Frank, 1954), and psychology (Pineau, 1982).

Pineau's (1982) study, which used an open-ended question that asked respondents to define comfort, reported four common themes: personalization, space, warmth, and freedom of choice. Moreover, Kolcaba (1991) asserted that the construct of comfort consists of four concepts: physical, psycho-spiritual, environmental, and social. Several researchers have also identified a number of individual characteristics associated with comfort, including feeling at ease (Morse, 1983) and being in control. Further, it is necessary to interpret comfort as either a noun or a verb, and either an outcome or a process (Kolcaba, 1992). *Comfort level* is defined in the nursing literature as "contented enjoyment in physical or mental well-being brought about by lessening perception of discomfort or pain" (Flaherty & Fitzpatrick, 1978, p. 353).

Building on these definitions of comfort, researchers have explored the construct of comfort (or the lack of anxiety) as it pertains to self-disclosure. Specifically, the Distress Disclosure Index (DDI), a scale for measuring comfort as self-disclosure, was developed by Kahn and Hessling (2001). The DDI measures the extent to which an individual is comfortable (lacks anxiety) talking with other individuals about personally distressing information. In one of the few relevant studies, Wei, Russell, and Zakalik (2005) explored the relationship between self-disclosure and social self-efficacy as mediators of attachment and loneliness in college freshman. Researchers Wei et al. (2005) reported that comfort with self-disclosed feelings of distress served to mediate attachment avoidance (the fear of intimacy or dependence on others).

Clearly, for online users to be comfortable disclosing personally identifying information to the fullest extent, they must be free of anxiety, stress, fear, or worry about related risks. Understanding the degree to which online disclosure engenders comfort versus anxiety provides

an alternative measure to assess users' propensity to provide personal information in an ecommerce situation.

Perception of risk of disclosing specific PII items

Risk, defined as "the probability of harm occurring due to some hazard" (Trumbo, 2012, p. 93), is a major concern for consumers, and consumers continually weigh relative risk during the online purchase of goods and services. The literature has identified five basic types of consumer-related risk, including physical, psychological, social, financial, and functional/performance risks (Jacoby & Kaplan, 1972). Consumers may perceive experience a multitude of risks when disclosing online, especially in ecommerce.

Many dangers can arise through disclosure of personal information online, including identity theft, deceptive phishing schemes, and discrimination, to name a few. The largest concern faced by consumers is identity theft. In 2012, identity theft cost the average victim $365, leading to over $21 billion in total losses for the year. When searching for victims, identity thieves look for specific information including usernames and passwords, phone numbers, utility account numbers, social security numbers, and bank account numbers (Anderson, 2013). Due to the sensitivity of the aforementioned PII items, this study will explore the perceived risk of disclosing these very items.

Other types of data, including demographic and health information, can be misused to discriminate against individuals through profiling (Rindfleisch, 1997). Phishing, a technique that involves extracting personal information from an online user by posing as a legitimate website, is yet another threat to consumers (Downs, Holbrook, & Cranor, 2007). In addition to phishing, an estimated 130 million software programs exist that were created solely for the purpose of stealing personal information (Anderson, 2013).

In addition to these possible risks, it is generally believed that consumers associate different levels of risk with the disclosure of particular personal facts. Importantly, the perception of possible risks do not necessarily correspond to the actual risk and may be overstated or understated. Understanding the perceived riskiness associated with each disclosure of particular PII items can be useful.

Within the arena of consumer behavior, the concept of *perception of risk* was first introduced by Bauer (1960) who stated that consumer behavior could be seen as a process of risk taking, and this risk-taking behavior may influence the conversion of consumers to buyers. Soon thereafter, perception of risk was redefined as the overall amount of uncertainty experienced by a purchaser during a transaction (Cox & Rich, 1964). It has been suggested that perception of risk generates anxiety that influences the process of consumer decision making (Taylor, 1974). Mayer et al. (1995) defined risk perception as involving the "trustor's belief about likelihoods of gains or losses outside of considerations that involve the relationship with the particular trustee" (p. 726). Another common definition is "the buyer's subjective assessment of the consequences of making a purchasing mistake" (Murphy & Enis, 1986, p. 31).

Consumers must constantly balance the benefits (lower costs and time savings) and disadvantages (exposing personal data, increasing chances of identity theft) as they navigate the process of purchasing a product online. Building on the definition of perceived risk from Kim, Ferrin, and Rao (2008), this study will define perception of risk of PII items as consumers' beliefs about a potential negative outcome from divulging specific PII items during ecommerce transactions.

Perception of risk is an important issue in ecommerce and particularly in providing personal information. When purchasing online, consumers are not able to interact with the seller

the same way as in face-to-face purchases. Online purchasing is a process in which the buyer is detached from the seller and does not provide the same multi-sensory experiences (including non-verbal cues) found when shopping in-store. Similarly, automated online systems and miscues can unintentionally create doubts and eliminate opportunities to identify and overcome buyers' objections. Because of this, consumers can regard ecommerce transactions as having a higher probability of risk. Perceived risks can take various forms in an online environment, including hazards or losses pertaining to product quality, delivery, billing and the potential misuse of the information provided to facilitate the transaction (the focus of this study).

Enhancing willingness to provide personally identifying information by reducing consumer perceptions of risk is critical to emarketers because individuals who perceive high risk are less likely to complete purchases. Several studies have found negative impacts on shoppers' attitude toward shopping that stem from the negative effects of risk perception (O'Cass & Fenech, 2003; Shih, 2004), and perceived risks of online shopping ultimately have a negative effect on ecommerce adoption (Van der Heijden, Verhagen, & Creemers, 2003).

Importantly, research has shown that people's perceptions of risk vary by country, culture, and other factors. In a study comparing risk perceptions in online shopping among Americans and Saudi Arabians, Americans reported less perceived risk than Saudi Arabians for all dimensions of risk measured by the study (Brosdahl & Almousa, 2013). The authors concluded that differences in perceptions of risk might be explained by cultural differences, as well as by overall Internet adoption and proficiency. Similarly, Park, Gunn, and Han (2012) found differences in Korean versus American respondents involved in online purchases, with the latter having a higher tendency to trust. Additionally, the study found that while the relationship of trust between perceived risk (an important part of conducting purchases) is critical in the

United States, it is not important in South Korea. These and other studies suggest that perception of risk varies by country, suggesting that ecommerce retailers need to target their efforts to address different cultural perceptions.

The disclosure of PII items online provides both benefits and risks: disclosing may benefit the customer in some circumstances (for example, the ability to download and redeem money-saving coupons); however, there are significant concerns with disclosing PII online. It is common for many websites to reuse personal information obtained during website visits, to share information with affiliates, or to sell the information to third-parties. The consumer is not always aware of this free flow and exchange of information. The Federal Trade Commission (2000b) reported that 99% of websites collect personal information from individuals browsing their web sites. It is safe to say that consumers are not always aware of the extent to which their information is shared, or how easily identifiable they are online. Even when technologies anonymize data, individuals are still identifiable. For example, anonymous information as simple as Netflix viewing patterns can be reverse engineered to identify the individual (Ohm, 2010).

MODERATING VARIABLES

Gender

Gender, defined here simply as the sex of the online user, is a potential explanatory or confound variable in this study. Contradictions abound in the literature regarding whether males or females disclose more about themselves to others, either in-person or online (Levesque, Steciuk, & Ledley, 2002; Sprecher & Hendrick, 2004; Wheeless & Grotz, 1976). In the context of online communication, females have been shown to be more aware of their online disclosure actions, to disclose more online than males, and to disclose more honest statements online compared to males (Punyanunt-Carter, 2006). Comparing gender disclosure in online social

networks and the application of privacy settings, Walrave, Vanwesenbeeck, and Heirman (2012) found that female adolescents better protected their online privacy compared to males, disclosing less information and instituting more access restrictions to their online profiles. Moreover, female teenagers were less willing to disclose contact information online (email, phone number, address) than teenage males, and males were less likely than teen females to disclose profile data, such as gender, name, and age (Walrave & Heirman, 2012).

Age

Age also has been identified as a significant factor in disclosure. Growing evidence suggests that young adults disclose more information online compared to older users (Nosko, Wood, & Molema, 2010; Walrave et al., 2012). Nosko et al. (2010) showed a negative relation between age and disclosure: as age increases, self-disclosure decreases. In online social networks, adolescents disclose more personal information and set less strict privacy controls than do adults (Walrave et al., 2012). These lower levels of self-disclosure among older users might be explained by reduced familiarity with and trust of technology, but it is equally likely that older users are more wary of disclosing private information (Bucur, Renold, & Henke, 1999). Older users might have greater assets to protect (including wealth and reputation), be more familiar with cases of identity theft, other risks, or simply be wiser.

Education level

Education level is defined as the participant's highest level of formal education or school completed. More educated individuals presumably are exposed to a greater understanding of social problems and business activities and might have a more sophisticated appreciation for how information can be used (and misused) by others. As a result, they might be *more cautious*. On the one hand, more sophisticated users also might have a better understanding of why certain

types of personally identifying information might be requested to facilitate transactions and collect marketing intelligence. These users could thus be *more willing* to provide information. More educated users are thus likely to be more deliberative and discriminating concerning both the amount and the nature of the personal data they disclose to others, especially to strangers.

Ecommerce proficiency

Experience in using ecommerce, or the extent to which an individual positively rates their proficiency or competency in shopping online, is an important attribute that can affect engagement in ecommerce. One's self-assessment of competency in using ecommerce reflects frequency, familiarity, and overall confidence with using online shopping technology. Importantly, users who are more experienced with the web are more likely to shop online (Corbitt, Thanasankit, & Yi, 2003). Through increased proficiency in using the Internet, individuals are less likely to be concerned with associated risks (Dutton & Shepherd, 2006). Further, it can be assumed that this holds true for ecommerce as well: the greater the proficiency in using ecommerce, the fewer the concerns about perceived risks associated with ecommerce, which leads to an increase in the individual's ecommerce usage. A high level of acceptance and engagement will presumably be exhibited by a greater propensity to share the kind of personally identifying information that is required to complete ecommerce transactions.

Trust

Trust is a broad concept that has been explored across many disciplines. A conventional usage defines trust as a "belief that someone or something is reliable, good, honest, effective, and so forth." (Merriam-Webster, 2014b). Mayer et al. (1995) defined trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or

control that other party" (p. 712).

Trust is important in ecommerce at several levels. One level is trust in the emarketer, or the specific organization to whom the information is provided. Trust in this context can be a function of the organization's reputation (important for a new customer) or the user's past experiences with the organization, either in making purchases offline or online. Because this study sought to focus on cross-national comparisons, identifying purchasing situations involving specific or hypothetical organization was not practical, this study opted to examine the degree to which people trusted the Internet and organizations and institutions in general.

Trust in the Internet

A clear relationship exists between trust and perceived risk in conducting purchases (Park et al., 2012). Trust is a vital component of interaction for any Internet user, including both Estonians and Americans. Trust is important in conducting online transactions. Research confirms that the more a consumer trusts, the lower the perceived risk of purchasing (Pavlou, 2003). Additionally, trust has a reciprocal relationship with online disclosure: information disclosure increases the impression of an individual's trustworthiness, which results in reciprocal disclosure by the other individual when conversing (Henderson & Gilding, 2004).

Trust has been explored in many different purchasing contexts, including users' relationships with market researchers (Moorman, Deshpandé, & Zaltman, 1993) and buyer-seller relationships (Doney & Cannon, 1997). Trust is extremely important to consumers during online purchases and acts as an antecedent of perceived risk (Pavlou, 2003). The more a consumer trusts a website or online vendor, the lower the perceived risk of completing a transaction with the vendor.

Trust in the Internet in general has been explored in the context of *cybertrust*, or "trust in the Internet and related information and communication technologies" (Dutton & Shepherd, 2006, p. 433). Trust may be undermined online, and in ecommerce transactions in particular, due to lack of the kind of physical cues that are used by consumers to detect deceit in physical encounters (Wallace, 2001). Further, individuals who are more trusting in general may be more inclined to trust the Internet than less trusting persons (Rose, 2003). Moreover, trusting individuals are more likely to shop online (Uslaner, 2004).

Dutton and Shepherd (2006) define two major dimensions of online trust: *net confidence,* having confidence both in Internet technology and the individual(s) being communicated with, and *net risk,* the perception of and exposure to risks while online. Distrust in the Internet is cited as a major reason for failing to use the Internet regularly (Dutton & Shepherd, 2006). Therefore, lack of trust in the Internet may be a major determinant of whether or not someone is willing to engage in ecommerce. Additionally, those more experienced in Web usage tend to have a higher level of trust in ecommerce (Corbitt et al., 2003).

An individual's trust in ecommerce is actually influenced by three sources: the reputation of ecommerce in general, the consumer's previous online experiences, and the nature of the specific ecommerce site (Corbitt et al., 2003). *Trust in the Internet* will be defined as an individual's confidence (or lack thereof) in using the platform, or online website, especially for purchasing products or services.

Trust in institutions

A separate approach to measuring trust is exploring the people's view of public, social, or government institutions. Trust in institutions can be defined as an individual's beliefs regarding the character and trustworthiness of public entities, including hospitals, schools,

businesses, and government institutions. Trust, in general, is an important aspect of communication, whether interpersonally or online with a digital merchant.

To further understand trust and its implications for disclosure, this study sought to understand the degree to which people were trusting of three types of organizations that might be involved in conducting ecommerce transactions, and organizations and institutions in general. Businesses are obviously involved in ecommerce to promote their services. However, various other organizations, including governments, engage in ecommerce-type activities to facilitate transactions, such as the payment of taxes and requests for government services.

Trust in government institutions has been measured by Torney-Purta, Barber, and Richardson (2004) who investigated trust levels in adolescents from multiple countries. Torney-Purta et al. (2004) found that a threshold level of trust in government institutions allows individuals to explore and initiate their civic and political participation. One study investigated the relationship between institutional trust and consumer-perceived risk: as institutional trust increased, perceived risk decreased (Salam, Rao, & Pegels, 2003). By lowering perceived risk in ecommerce, institutional trust is a critical element for increasing ecommerce and its maturity (Salam et al., 2003). Trust levels vary between European national entities and the European Union, and some of these differences in trust levels are driven by country-level corruption levels (Arnold, Sapir, & Zapryanova, 2012).

Personality

Disclosiveness can vary by individual and various personality traits. This study sought to account for possible individual differences that might be found within the two populations by examining personality traits.

The American Psychological Association (2014b) defines *personality* as "individual differences in characteristic patterns of thinking, feeling, and behaving" (para. 1). Further, in various situations, one's personality influences behaviors and cognitions (Ryckman, 2012). Many authors have attempted to measure personality, and two recent efforts to measure personality have been developed: the Neo Personality Inventory (Costa & McCrae, 1985) and the Big Five Inventory (John, Donahue, & Kentle, 1991). The Big Five Inventory (BFI) contains five dimensions (neuroticism, extraversion, openness, agreeableness, and conscientiousness), that when combined, describe an individual's personality. Neuroticism reflects a tendency toward experiencing psychological distress, with high levels of neuroticism being associated with a sensitivity to threat. Extraverts tend to be sociable, outgoing, and able to have positive emotions. Openness (to experience) is demonstrated by an individual's willingness to try new things, and naturally be curious. Individuals demonstrating agreeableness reflect trust, cooperation and sympathy. Lastly, conscientiousness reflects an individual who is organized and diligent.

Development of the personality traits research had its origins in the work of Klages (1932), who suggested that analysis of language would assist in the understanding of personality. From Klages' suggestion, Baumgarten (1937) examined personality terms occurring in the German language. The analysis of personality terms continued through the identification of hundreds of personality traits and then through multiple replications of factor analysis (Digman, 1990), including Fiske (1949), Cattel (1957), Norman (1963), and Tupes & Christal (1992), theorists proposed the five main domains of personality. Two popular scales have been developed from the work of these trait theorists, and many researchers currently use either the NEO Five-Factor Inventory (NEO-FFI) or the BFI scale. In its modern form, the BFI scale is a 44-item scale measuring the five personality traits, while the Neo Five has 60-items.

The BFI personality traits have been studied extensively and, in more contemporary research, have been used to predict general online behavior. When investigating the relationship of personality to social media use, Correa, Hinsley, and de Zúñiga (2010) found that extraversion and openness were positively related to social media use. Those high in neuroticism have been found to use the Internet to avoid loneliness (Butt & Phillips, 2008), demonstrate a strong interest in using the Internet for communication (Wolfradt & Doll, 2001), and post accurate information of themselves on online profiles (Amichai-Hamburger, Wainapel, & Fox, 2002). Extraverts have been shown to belong to more groups on Facebook than introverts (Ross et al., 2009), and constantly use social media to grow their network of friends (Correa et al., 2010). Those high in openness or agreeableness are less inclined to self-disclose on social networks (Loiacono, Carey, Misch, Spencer, & Speranza, 2012). Conscientiousness has been shown to be negatively related to Internet use (Butt & Phillips, 2008). This non-use of the Internet by those high in conscientiousness may be explained by the Internet being perceived as a distraction to the individual's daily tasks (Ross et al., 2009).

Perceived benefits of exchanging PII information

Marketing has been described as an *exchange process* involving transactions where, among other things, two parties believe it is appropriate or desirable to deal with one another. Kotler (1988) defines exchange as "the art of obtaining a desired product from someone by offering something in return" (p. 6). In general, marketers provide products or services to benefit the purchaser, who in turn provides consideration, including but not limited to payments and the provision of information to facilitate the transaction and/or benefit the seller.

Providing personal information in exchange for benefits or incentives is a common practice in online marketing. In exchange for their email address, individuals may be offered

discounts on future purchases of a good or service in exchange for personal information perceived as an economic or social benefit. The result is a perceived benefit of exchanging PII information. Individuals are motivated to disclose online for many reasons (relationship building, etc.), including these economic motivations, which this study focuses on primarily.

Research suggests that consumers are enticed by offers and actually respond positively to revealing personal information in exchange for specific benefits, including information, entertainment, and financial value (Milne & Gordon, 1993). Additionally, consumers may provide personal information due to their desire for perceived individualized attention from companies (Graeff & Harmon, 2002). When consumers perceive that disclosure benefits exceed disclosure risks, they are more likely to disclose personal data (Milne & Culnan, 2004). Liebermann and Stashevsky (2002) found that perceived benefits of information disclosure is vital for consumers in deciding whether or not to disclose personal information on websites. Understanding how consumers perceive potential benefits versus risks can shed light on the important question of what motivates people to disclose personally identifying information and under what conditions they might do so.

For this study, four types of potential ecommerce benefits were identified: opportunity benefits, bargain likelihood benefits, purchase benefits, and privacy expectation benefits. *Opportunity benefits* characterize the purchase of a product online as providing an opportunity for an upside gain or positive outcome. *Bargain likelihood benefits represent* the likelihood of obtaining a good deal or purchasing a product at an advantageous price while shopping online. *Purchase benefits* involve value propositions for customers in exchange for providing some personal information (e.g. providing greater merchandise selection, better customer service,

tailored product offerings, special discounts). *Privacy expectation benefits* are conditions or guarantees desired in exchange for providing information.

Opportunity benefits and bargain likelihood benefit were adapted from the work of Jarvenpaa, Tractinsky, and Saarinen (1999) in their study examining the role of trust in ecommerce in cross-national settings. In the study, the authors explored risk perception and its relationship with trust and Internet usage, found that citizens of Israel were reportedly less experienced in web usage, but exhibited higher trust and lower risk perception than Australians.

Purchase benefits and privacy benefits arose from the work of Phelps, Nowak, and Ferrell, (2000) and Sheehan and Hoy (2000), later adapted by Gupta, Iyer, and Weisskirch (2010). Control over information, short-term transactional relationships, and long-term relationships were found to influence consumers' privacy concern (Sheehan & Hoy, 2000). Control over information presented several scenarios where individuals received unsolicited emails from companies, as well as situations where the personal information was sold. Consumers place varying importance on control over their personal information, and the level of control necessary for the information affects their privacy concern. Shopping benefits were measured as potential consequences and benefits and included increase in advertising mail, decrease in advertising mail, future shopping time and effort savings, and greater future merchandise selection. In addition, shopping benefits affect consumer purchase intentions: consumers are willing to make trade-offs when exchanging personal information for shopping benefits (Phelps et al., 2000).

Risk taking as a personality trait

Everyone takes risks in their everyday lives. Some people are quite willing to take risks that pertain to certain activities, but not to others. Trimpop (1994) defines risk-taking as "any

consciously, or non-consciously controlled behavior with a perceived uncertainty about its outcome, and/or about is possible benefits or costs for the physical, economic or psycho-social well-being of oneself or others" (p. 9). Similarly, Ferguson, Valenti, and Melwani (1991) define risk taking as "a tendency to engage in behaviors that the actor understands have some likelihood of resulting in a punishment or in the loss of a reward" (p. 196). Risk-taking individuals tend to throw caution to the wind. These individuals can be categorized as *risk-takers* rather than *risk-avoiders.* They are more likely or more willing than others to take risks on a regular basis across a variety of situations. Psychologists suggest that risk-taking can actually be considered a personality trait. Some individuals are simply predisposed to risk-taking, while other are not. The predisposition to take risks can even be explained by biological mechanisms (Zuckerman, 1988).

Although the Internet poses a variety of risks, the premise of its inclusion in this study is that risk-taking in general is a personality trait that can impact a person's decision to self-disclosure online. Risk-takers are posited to be more likely to ignore or discount concerns or threats posed by sharing personally identifying information online, while risk-avoiders are more likely to focus on the potential hazards or losses that may stem from ecommerce transactions. Being risk-avoidant personality, on the other hand, could lead a person to accentuate perceived risks and thus shy away from sharing personal data.

HYPOTHESES

The main purpose of this study is to examine the influence of nationality (country of residence) on the likelihood that people will disclose personally identifying information during ecommerce transactions. Specifically, the study uses survey research to explore how Estonians and Americans may differ in their online disclosure behaviors. Based on Estonia's unique position as a leader in Internet adoption and use, combined with the country's five unique

national attributes (as described earlier), Estonians would be expected to be more favorable toward the disclosure of PII on each of the four dependent variables in this study. This assumption provides the basis for the seven major testable hypotheses outlined here:

H1: *Estonians will be more willing than Americans to disclose specific PII items.*

Estonia's advanced, sophisticated approach to using the Internet to conduct everyday transactions has required its citizens to become accustomed to sharing and seeking personal information online. Moreover, a European Commission survey ranked Estonia as one of the more carefree nations in the EU in terms of citizens' willingness to publish personal information online (European Commission, 2011). For instance, 47% of Estonians reported that disclosing personal information online is not a major issue for them. Estonia also scored second highest of any EU country, behind Denmark, in terms of level of comfort in disclosing personal information online. This study posits that, due to their carefree nature in providing personal information, Estonians will be more likely to disclose specific PII items than Americans.

H2: *Estonians will be less likely to disclose PII items based on perceived benefits received in exchange for providing information compared to Americans.*

Broadly stated, the United States is an indulgent nation (Hofstede, 2014b) in which material goods are an outward sign of success and power. This indulgent nature transfers to the online realm where Americans have become accustomed to expecting benefits ("What's in it for me?"), such as discounts, free products or services or other incentives, in exchange for providing personal information. By contrast, Estonia is a more restrained society that "suppresses gratification of needs" (Hofstede, 2014a, para. 6). Supporting the concept of the United States as an indulgent, incentive-seeking society, a recent study noted that Americans were more willing (44% of responsdents) than the global average (41%) to provide personal information in

exchange for free products or services (SDL, 2014). By comparison, in a similar study, 32% of Estonians were willing to disclose personal information in exchange for free services online (European Commission, 2011). In comparing loyalty programs versus free products in exchange for personal information, Americans are more willing to provide personal information in exchange for loyalty programs (49%) than for free products (41%) (SDL, 2014). Meanwhile, Estonians consistently cite trust as an issue relevant to ecommerce (Cinite, Kumar, & Kumar, 2008; Inselberg, 2013). Estonians, therefore, may be more cautious in general when disclosing PII in exchange for benefits of various types. .

H3: *Willingness to disclose will be positively related to a) extraversion, b) openness, c) conscientiousness, and d) agreeableness, and e) negatively related to neuroticism.*

Research using the Big Five Inventory (BFI) suggests these five traits are related to willingness to disclose personally identifying information. Because extraverts have been shown to belong to more groups on Facebook than introverts (Ross et al., 2009), and constantly use social media in order to grow their network of friends (Correa et al., 2010), a positive relationship should exist between extraversion and willingness to disclose. Similarly, neuroticism should demonstrate a negative relationship with willingness to disclose, as neurotics focus on posting accurate information about themselves on online profiles (Amichai-Hamburger et al., 2002). This preoccupation with accuracy might reduce their need for disclosing overall, as they only want to disclose in opportunities where they can ensure the legitimacy of the information. Individuals demonstrating agreeableness should be willing to disclose so to keep their public persona of being agreeable. Lastly, conscientiousness should be positively related to willingness to disclose as disclosing online would help to perpetuate their sense of being organized and diligent in their online communications and purchases.

H4: *Willingness to disclose is positively related to a) trust in the Internet and b) being a trusting person more generally, as evidenced by trust in organizations and public institutions.*

Willingness to disclose is predicted to be positively related to how much trust people demonstrate in the Internet and in organizations and public institutions in general. Trust is a major determinant for shopping online as it lowers perceived risk (Pavlou, 2003; Salam et al., 2003), and should increase an individual's willingness to disclose personal information.

H5: *Estonians will demonstrate a more positive attitude toward disclosing online in general than Americans.*

Estonia is considered one of the most technologically advanced countries in the world, so that Estonians can be generally seen as adept users of technology (Freedom House, 2014). Estonians also are reported to be relatively comfortable disclosing personal information (European Commission, 2011). Based on these findings, Estonians are posited to have more positive attitude toward disclosing online than Americans.

H6: *Estonians will exhibit less anxiety about disclosing information online than Americans.*

This author posits that Estonians are more conditioned to disclosing PII items online than Americans, and thus the idea of providing personal data will result in lower levels of psychological anxiety for them. In comparison, it is anticipated Americans will be more anxious disclosing PII items online. Highlighting Americans' anxiety with the presence of their personal information online, a study discovered that 88% of Americans have taken steps to remove or mask personal information online (Rainie, Kiesler, Kang, & Madden, 2013). On the other hand, 47% of Estonians report that "disclosing personal information online is not a big issue" (European Commission, 2011, p. 30).

H7: *Estonians will have lower perception of risks related to disclosing specific PII items than Americans.*

Due to their relatively carefree nature toward disclosing personal information online and their reported high level of comfort in providing PII items online (which can be attributed to their high level of adoption of online banking, voting, and digital medical records), Estonians are predicted to have a lower perception of risks than Americans when disclosing specific PII items. A higher percentage of Estonians (85%) bank online compared to Americans (51%) (Estonian Review, 2012; Fox, 2013). Estonians are adept at online voting and are used to their health information being digitally recorded. Further, Estonians file their taxes online (95% of taxpayers) at a higher rate than Americans (70%) (E-estonia.com, 2014b; Murphy, 2011). As research has concluded, differences in perceived risk are influenced by overall Internet adoption and proficiency (Brosdahl & Almousa, 2013). Also due to their familiarity with having personal information stored online, as well as to the continual retrieval and updating of personal information, Estonians are predicted to report a lower perception of risk of specific PII items than Americans.

CHAPTER THREE:

METHODOLOGY

To investigate the questions outline in Chapter 2, this study conducted a cross-national online survey of residents in the United States and Estonia. Chapter 3 presents the methods and procedures used to investigate disclosure of PII during ecommerce transactions. This study was conducted in keeping with a human subject protocol approved by Colorado State University's Institutional Review Board (See Appendix A).

PARTICIPANTS

Sampling and Recruitment

Individuals over age 18 in both the United States and Estonia were recruited using quota sampling to complete the online survey administered through Qualtrics, a major online survey research service.

United States. Participants in the United States were recruited through Amazon's Mechanical Turk, or "Mturk," described as a "marketplace for work that requires human intelligence" (Amazon Mechanical Turk, 2014, para. 1). According to the operator, the "service gives businesses access to a diverse, on-demand, scalable workforce and gives workers a selection of thousands of tasks to complete whenever it's convenient" (Amazon Mechanical Turk, 2014, para. 1). The Mturk ecosystem labels individuals as either "workers" or "requesters." Requestors are clients who post a "Human Intelligence Task" (HIT) for workers to complete. Workers (further referred to as participants) volunteer and are incentivized to complete HITs according to compensation or other incentive levels set and paid for by the requester. Thus, the system essentially uses a quota system where tasks remain open until fully subscribed.

Surveys completed using Mturk are not randomized but rely on quota sampling. However, mounting evidence suggests Mturk is "a valid means of collecting data" (Mason & Suri, 2012, p. 4). Furthermore, Mturk sample have been found to be a valid venue in which to conduct research: the resulting samples are both more diverse than typical Internet samples and significantly more diverse than American college samples (Buhrmester, Kwang, & Gosling, 2011). Importantly, the data obtained through Mturk are thought to be as reliable as traditional survey research methods (Buhrmester et al., 2011), and the platform allows researchers to overcome barriers related to research costs, including recruitment and access to non-student adult pools (Berinsky, Huber, Lenz, & Alvarez, 2012). A recent study indicated that Mturk participants do not conduct HITs merely for monetary gains: only 13% report using Mturk primarily for earning income, while 40% do so for entertainment, and 67% of US participants report it as a fruitful way to spend time (Paolacci, Chandler, & Ipeirotis, 2010). In addition, Mturk participants have been found to be more representative of the US population than participants recruited through university pools, or Internet samples in general (Paolacci et al., 2010). Overall, the Mturk platform provides three key advantages: ready participant pool access, low cost, and pool diversity (Mason & Suri, 2012). With regard to non-response error, Mturk participants presented less error than Internet convenience samples acquired through other means (Paolacci et al., 2010).

Participants in the United States were recruited Mturk participants. Based on the literature and suggestions of other Mturk researchers, participants had to qualify to complete the task, and these criteria included the participant having a HIT approval rate of greater than or equal to 95%, and the number of completed HITs approved were greater than or equal to 1,000, as basis for the quality of their work. A detailed description of the steps for United States survey

participants follows (see Figure 3.1): Participants locate the HIT either through a keyword search (using keywords such as "survey, demographics, ecommerce, online shopping, academic, research, study, short, social science, science") or by browsing through a list of HITs. Once a participant locates an assignment, the HIT search interface displays detailed information about the work assignment, including the requester's name, HIT expiration date, incentive level (aka "Reward"), time allotted, description of the HIT, keywords, and qualifications of the requested workers. The title of the HIT created by the researcher was worded such that participants would be interested in completing the survey, but not primed about the topic of the study or could engage in self-selection, specifically those interested in privacy. The HIT was titled "Sharing Online Information in Ecommerce." Upon clicking the title of the HIT, participants were provided with detailed information about the survey hosted on Qualtrics.com (See Appendix B). Upon clicking a link, participants were redirected to the Qualtrics website, where they reviewed the Informed Consent statement (see exhibit in Appendix A), and completed the survey (See Appendix C). At the end of the survey, participants were redirected to the Mturk website. After completing the HIT, participants were paid once their submitted work was approved by the researcher.

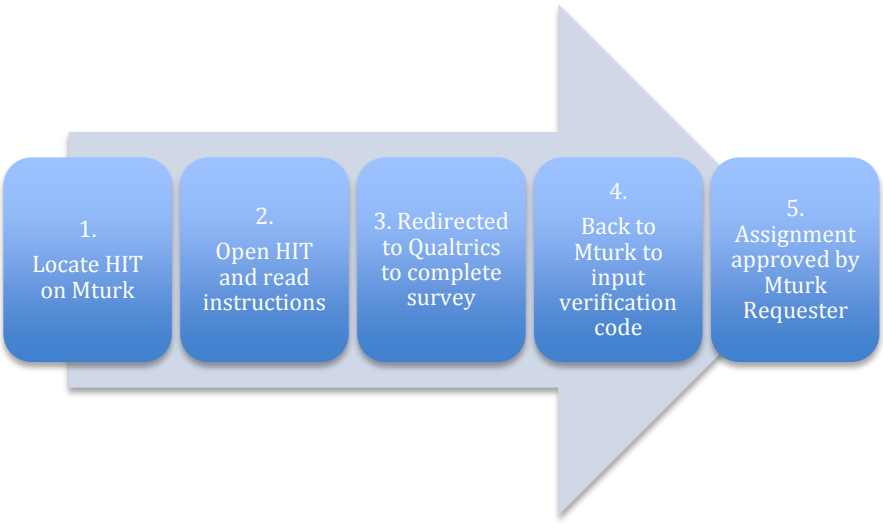


Figure 3.1: US survey workflow

To ensure that participants had experience with ecommerce, a filter question at the beginning of the survey required participants to designate if they had or had not purchased a good or service online: *Have you purchased at least one product or service online?* Participants who selected "*No*" were redirected to the end of the survey and were not compensated. To ensure participants were residents of the United States, a participant requirement was set that required respondents to be located in the United States. Participants were also required to designate their residency in the United States in a second filter question at the beginning of the survey. The options were, "United States" and "Other." Participants who selected "*Other*" were redirected to the end of the survey and were not compensated.

The incentive for the survey (US$1.50) was determined based on incentive levels for similar HITs in the Mturk marketplace, as well as recommendations from the literature.

Estonia. To recruit participants in Estonia, a web panel was recruited through a market research firm, Klaster Uuringukeskus. The market research firm recruited 297 participants over 18 years of age from their existing web panel participants, who started the Estonian version of

the online survey hosted on Qualtrics.com. Estonian participants were obtained by the researchers via an email and could respond via a survey link. After clicking the survey link, participants were redirected to the Qualtrics website, where they were provided with the Estonian version of the Informed Consent statement (see Appendix D) and the Estonian language survey (see Appendix E). The sample obtained by the market research firm represented a random sample of its web panel recruits but was not necessarily a random sample of the Estonian population.

To ensure that Estonian participants were experienced with ecommerce, the same filter questions as the English survey were utilized. At the beginning of the survey, participants were required to confirm if they had or had not purchased a good or service online: *Have you purchased at least one product or service online?* Participants who selected "*No*" were redirected to the end of the survey and were not compensated. To ensure that participants were residents of Estonia, participants were also required to designate their residency in Estonia in a second filter question at the beginning of the survey. Options were "*Estonia*" and "*Other*." Participants who selected "*Other*" were redirected to the end of the survey and were not compensated.

PROCEDURES

Survey administration, format, and translation

The study was administered using an online survey hosted through Qualtrics, in which participants completed 107 close-ended survey items (108 for Estonians--with an additional "Trust in EU" item).

A translation service provider was utilized to translate the survey into Estonian. A web search for "Estonia translation" directed the researcher to providers recommended and used by

the Estonian government, who were then contacted regarding translation costs and quality standards. Wiedemanni Translation Bureau, the selected translation provider, was selected based on its competitive bid, as well as for its high quality assurance in translating the instrument. This company is one of a few companies that met the European standard for translation services, EN 15038:2007, and was the first to receive this certification in Estonia (Wiedemanni Translation Company, 2014a).

Translation of the instrument was completed in four stages: (1) translation by a native-speaking Estonian, (2) editing by second native-speaking Estonian, (3) final proofreading by a project manager, and 4) an analysis using industry-standard translation software to ensure "terminological coherence of translated text" (Wiedemanni Translation Company, 2014b). Reverse translation was not used due to potential problems in literal re-translation (Dillman, 2009). Indeed, when conducting cross-national research, experts argue that direct translation of words should not be the focus, but rather accurate translation of concepts is more important in conveying accurate messages across languages (Harkness, 2003; Harkness, Van de Vijver, & Johnson, 2003).

Pilot Study

Prior to administration of the full survey, and subject to IRB approval, several scales were pretested and a full pilot test using students enrolled in summer courses at Colorado State University was conducted to check the instrument design and to correct problems related to question confusion, wordiness, or any other issues. Students involved in the pilot test were offered extra credit, as determined by their instructor. Alterations were made to the survey instrument based on issues arising from the pilot test.

An in-class pre-test (N=54) was performed of the "Anxiety levels disclosing PII items" and the initial BFI-10 personality scale (Rammstedt & John, 2007) considered for in the study. The "Anxiety levels disclosing PII items" scale was found to not be reliable (α=0.64). However, one item "I enjoyed providing the information" was found to have a poor fit, and scale reliability increased (α=0.80) with its exclusion. The personality scale (BFI-10) was found to have both validity and reliability problems, and only the pair of items measuring the personality trait of extraversion demonstrated sufficient reliability (α=0.76). Due to the poor results of the BFI-10 personality scale and in the full pilot study that followed, the scale was later replaced.

The pre-test version of the full survey was conducted on Qualtrics (n=87), an online survey platform, between June 8-10, 2014 to examine the reliability and validity of the survey instrument. To obtain a diverse sample, including adults similar to Mturk workers, pretest participants were recruited from various sources, including from a link posted on social media platforms, emails sent to CSU faculty, and students from multiple online sections of JTC 300. Instructors gave the author permission to recruit their students to participate, and the instructors provided bonus points for students who participated. In total, 87 participants completed the 91-item online survey, which included six demographic questions and the IRB informed consent statement. The resulting gender split was 36% male and 64% female, with an age range from 19 to 65 years old. Each scale was tested using factor analysis and reliability analysis. Only minor changes in the items were required, except for replacement of the BFI-10.

OPERATIONALIZATIONS

Independent variable

Nationality was confirmed in the separate surveys administered to residents either of the United States or Estonia. As outlined in the section on sampling and recruitment, United States

or Estonian nationals who resided in any other country (and might have been away from their native countries for varying periods of time) and all residents of other countries were excluded.

Dependent variables

Except as noted, the dependent variables and most of the moderating variables were measured using a 7-point Likert-type scale, where a negatively valenced response = 1 and a positively valenced response = 7 for consistency purposes.

Willingness to disclose specific PII items was measured by asking participants to rate their willingness to disclose each of 17 items of personal information on a 7-point Likert-type scale of 1=not willing and 7=very willing. The 17 items of personally identifying information included name, home address, home phone number, work address, work phone number, email address, date of birth, credit card number, annual income, credit history, medical history, age, marital status, Twitter handle, Facebook profile, Skype username, and PayPal account. These items were adapted from a study by Gupta et al. (2010) that explored differences in willingness to disclose between residents of the United States (α=0.88) and India (α=0.87). Gupta et al. (2010) based this scale on the work of Phelps et al. (2000) and Sheehan and Hoy (2000).

Attitude toward disclosing PII online was measured using a self-developed scale adapted from several extant general attitude scales (Hallahan, 1999). Participants were asked to complete the statement "*I would describe providing information online as*:" using 7-point semantic differential scales anchored by the following bipolar adjectives/phrases: *risky/safe*, *trustworthy/untrustworthy*, *unreliable/reliable*, *bad/good*, *unimportant/necessary*, and *worthless/valuable*. In an effort to reduce possible demand effects, half of the items were randomly reversed to mix the pattern of positive versus negatively valenced items appearing only on the right or left.

Anxiety levels disclosing PII items were measured using a self-developed 7-item, 7-point Likert scale. Participants were provided with the statement: *"Think back to a time when you were completing an information request form online, such as when you were purchasing a product or making a reservation for a hotel or restaurant. For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.*" The statements with which people were asked to agree or disagree included: *I felt uncomfortable providing the information; It wasn't stressful at all; I enjoyed providing the information; I didn't feel intimidated; I was uncertain about providing information; I was anxious about being asked for my information; I would have preferred to not provide all the information;* and *I was relaxed without any worries.*

Perception of risk of disclosing specific PII items was measured by asking participants to respond to the statement "*When purchasing goods or services online, people are asked to provide personal information in order to complete the purchase. Please indicate the level of risk you perceive involved in sharing each of the following types of personal information online where 1= very risky and 7 = not risky.*" The 17 items of personal information were the same as those used to measure willingness to disclose and included name, home address, home phone number, work address, work phone number, email address, date of birth, credit card number, annual income, credit history, medical history, age, marital status, Twitter handle, Facebook profile, Skype username, and PayPal account. The question stem and 7-point scale were adapted from Treiblmaier and Chong (2011) who measured perceived risk of personal information using similar items to create a reliable scale (α=0.83).

Moderating variables

Demographic questions were among the first questions participants answered, including gender, age, and education level. Gender was measured as three radio buttons in which participants indicated the biological sex with which they identified as *male*, *female*, or *other*. Participants indicated their age by typing in their age in years. Education was measured with participants selecting highest level completed from six choices displayed as radio buttons: *some high school, high school*, *some college*, *college degree*, *some graduate school*, and *graduate school*. In the Estonian survey, the most comparable nomenclature was used, based on the corresponding years of education completed.

Ecommerce experience was measured as a one item, 7-point Likert scale in which participants were asked to respond to the following statement: "*Ecommerce is the buying and selling of goods and services on the Internet. Choose the number that best reflects your proficiency or experience with purchasing goods or services online.* " The scale was measured as 1=Beginner and 7=Expert. This item was adapted from Treiblmaier and Chong (2011), which measured Internet experience. Participants with no ecommerce experience whatsoever were presumably eliminated from the sample through the filter question at the beginning of the survey.

Trust was measured using separate scales for trust in the Internet and trust in institutions.

Trust in the Internet was measured using a 4- item, 7-point Likert scale. The statement used was: "*The following questions ask your opinions about using the Internet. For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree*." The statements included: *The Internet is a safe environment in which to exchange information with others; the Internet is a reliable environment in which to conduct business transactions or personal purchases; Internet merchants are*

dependable, and *the Internet can be trusted.* The scale was adapted from Dinev and Hart (2006), and the scale had a satisfactory reliability of α=0.91 when used previously. Dinev and Hart (2006) constructed the scale based on work by Cheung and Lee (2002) and Lee and Turban (2001).

Trust in institutions was operationalized using a 4 item, 7-point Likert-type scale for American participants, and a 5-item, 7-point Likert type scale for Estonian participants. The Estonian participants rated one additional public institution, the European Union, which mutually governs the nation alongside the Estonian government. Participants were provided the statement "*The following questions are about your opinions of various public institutions. For each of the following statements, please indicate the extent to which you disagree or agree where 1 = never and 7 = always. How much of the time can you trust each of the following institutions?*" Participants rated four items, including: *the national government, the local government, local businesses,* and *international businesses*. The scale was adapted from Torney-Purta, Barber, and Richardson (2004) who measured trust in government-related institutions and reported an α=0.78.

Personality was operationalized using a 20-item, 7-point Likert-type scale measuring five dimensions of personality that together described an individual's personality: extraversion, neuroticism, openness to experience, agreeableness, and conscientiousness (McCrae & John, 1992). Although the Big Five Inventory (BFI-44) created by John et al. (1991) has been successfully used in repeated studies, various attempts have been made to shorten the original 44 item scale (Gosling, Rentfrow, & Swann Jr, 2003; Rammstedt & John, 2007). After the pilot study where the BFI-10 scale suggested by Rammstedt and John (2007) proved unreliable, a 20-item scale was constructed by the researcher. Items were selected that were believed to most

cogently represent the core construct for each of the five factors and each item scored high in reliability in the analysis of the items comprising the BFI as reported by Schmitt et al. (2007).

These five principal factors that emerged were validated (see results for Hypothesis 3) and labeled using the original Big Five dimensions (John et al., 1991). The five personality traits were each measured using 4-item, 7-point Likert scales with the question stem: "*How well do the following statements describe your personality? I see myself as someone who…*." For neuroticism, participants responded to (I see myself as someone who…) *is relaxed, handles stress well*; *gets nervous easily*; *worries a lot*; and *can be tense*. When responding to openness, participants rated the items (I see myself as someone who…) *is inventive*; *has an active imagination*; *is curious about many different things*; *is original,* and *has new ideas*. For extraversion, participants rated the items (I see myself assomeone who…) *is talkative*; *is outgoing, sociable*; *is reserved*; and *is shy, inhibited*. To measure conscientiousness, participants responded to the items (I see myself as someone who…) *does a thorough job*; *does things efficiently*; *tends to be disorganized*; and *tends to be lazy*. Finally, participants responded to items measuring agreeableness: (I see myself as someone who…) *is generally trusting*; *is considerate and kind to almost everyone*; *tends to find fault with others*; and *likes to cooperate with others*.

Perceived benefits of exchanging PII information was measured using four different sets of items intended to measure: opportunity benefits, bargain likelihood, purchase benefits, and privacy expected benefits.

The measures of perceived benefits, *opportunity benefits* and *bargain likelihood*, were measured using two sets of 7-point semantic differential scales. The question bank began with the following statement: "*This set of statements is about purchasing goods or services from online merchants. Think about your previous experience purchasing goods or services online in*

general. For each of the following pairs of adjectives, select the number that best describes your feelings:" Opportunity benefits was measured by one set of semantic differential scales based on the statement, "*How would you characterize the decision of whether to buy a product from an online retailer?*" Items in this subscale were anchored by the following pairs of bipolar adjective/phrases: *significant opportunity/significant risk, high potential for loss/high potential for gain,* and *very positive situation/very negative situation*. Bargain likelihood was the second set of semantic differential scales, and was based on the statement, "*What is the likelihood of finding a bargain by purchasing a good or service online*?" and was anchored by the following pairs of bipolar adjectives/phrases: *very unlikely/very likely, probable/not probable,* and *happens all the time/never happens*. The opportunity benefits index contained three items, all originating from Jarvenpaa et al. (1999). The fourth item from the original Jarvenpaa et al. (1999) scale was utilized for the bargain likelihood index, with two additional semantic differential response pairs being added to the original single item to construct an index that could be factor analyzed and exposed to reliability analysis.

Purchase benefits and *privacy expectation benefits* were operationalized by asking participants to respond to the following statement: "*Websites sometimes offer a coupon or discount in exchange for providing personal information such as your email or phone number. Below are some benefits that may be offered in exchange for your personal information. For each of the following statements, please indicate your level of willingness to provide information to companies, with 1 = not willing and 7 = very willing.* Responses to the statements were based on a 7-point Likert-type scale where 1=not willing and 7=very willing. Both indices originated as a single index used by Gupta et al. (2010). Purchase benefits included the item statements: *Company tailors their product offerings to my tastes; Company sends me special discounts on*

merchandise; It will help me save time when I make my next purchase from the same site; I can get better customer service from the company; It will provide a greater merchandise selection. Privacy benefits expected were measured by five statements: *The company website clearly states how my personal information will be used*; *The company website clearly states how my personal information will be used; The company website lets me know that they respect my privacy rights; I always know the purpose of the information being collected; I have a choice in whether my personal information should be disclosed to a third party; At any time, I can delete or edit my personal information.*

Risk taking as personality trait was operationalized using a 5- item, 7-point Likert scale. Participants were provided the statement: "*The following questions are about you and your personality. For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.*" The scale included the following items: *I often act on the spur of the moment; I quite enjoy taking risks; I'm willing to take some risks; I'm an adventurous person;* and *I welcome new and exciting experiences*. The scale was adapted from Ferguson et al. (1991) in which the authors measured adventurous risk taking (Cronbach α=0.90).

DATA ANALYSIS

The data from both the American and Estonian surveys hosted on Qualtrics were combined and edited in Excel and then downloaded into a consolidated SPSS database for analysis. Scale items reversed in the questionnaire were recoded so that all scale items were consistent in direction (positive=7, negative=1). Demographic information was reported and analyzed using cross tabulations. To determine reliability, Cronbach alpha was computed and examined for each of the potential scales (Cronbach, 1951). Only in cases where necessary,

certain items were removed to improve the scale's reliability. Once sufficient reliability was established, indices of the variables were created by computing means and standard deviations. The basic statistical test for the seven major hypotheses in the study involved Student t-tests comparing the mean values for Estonians and Americans. In addition Cohen's d was computed as an indicator of effective size. Cohen's d demonstrates the standardized difference between two means and is expressed in standard deviation units (Gliner, Morgan, & Leech, 2009). The effects of the moderating variables were analyzed using correlations employing Pearson r product-moment coefficients (two tailed, unless noted) and hierarchical multiple regression. In hierarchical multiple regression, independent variables are entered in blocks (steps) in an order specified by the researcher (Boduszek, 2013). Each subsequent block of independent variable is examined in how it adds to the prediction of the DV after controlling for previously entered IVs, and then each block and the overall model are assessed (Boduszek, 2013). Key measures in the analysis included the change resulting in the amount of variance explained with the addition of each block ($R^2\Delta$) and the resulting beta (β) representing the standardized coefficient that allows assessing which of the dependent variables had the greatest effect on the dependent variable. The tables presenting the analyses for the hierarchical multiple regression are based on tables suggested by Nicol and Pexman (2010, p. 120). In keeping with the custom in social science research, findings were deemed statistically significant if there was less than a 1 in 20 probability that the results obtained were obtained by chance ($p \leq .05$).

CHAPTER FOUR:

FINDINGS

As stated in Chapter 1, the purpose of this study was to examine the effect of nationality on disclosure of personally identifying information, also known as personal data, during ecommerce transactions, and specifically, how Estonians and American may differ in their online disclosure behaviors. This chapter profiles the study's participants and then reports the descriptive and inferential statistics used for testing the hypotheses pertaining to willingness to disclose, attitude toward disclosure, anxiety about disclosure, and perceived risks of disclosure.

DESCRIPTION OF PARTICIPANTS

A total of 554 people were initially recruited to participate in the study – 257 in the United States and 297 in Estonia. Of the 257 prospective American participants, all agreed to the IRB Informed Consent statement, one reported having no ecommerce experience, one reported residing outside the United States, and 7 were removed due to substantially incomplete responses. Among the 297 Estonians, 9 did not agree to the IRB Informed Consent statement, 26 had not previously purchased a product online, 4 did not reside in Estonia, and 33 were removed due to substantially incomplete surveys. This netted 248 US and 225 Estonian responses for data analysis. The participants are profiled in Table 4.1.

Gender

Of the 248 US participants, 121 (49%) were male and 126 (51%) were female, with one participant not reporting gender. The gender split for the Estonian sample was 80 male (36%) and 145 females (64%). Thus, the important differences in the gender for the two countries were found (χ^2=8.69, 1df, p≤.003).

Table 4.1
Descriptive Statistics of Participants

Characteristic	United States (n=248)		Estonia (n=225)	
	n	%	n	%
Gender				
Male	121	49	80	36
Female	126	51	145	64
Total (χ^2= 8.69, 1 df, p≤.003)	247	100	225	100
Age (years)				
Mean (t=-2.75, 470 df, p≤.006)	36.26	--	39.60	--
Range	20-82	--	19-83	--
Median	32	--	38	--
Median Split of Age				
34 and younger	137	55	99	44
35 and older	111	45	125	56
Total (χ^2=5.744, 1 df, p≤.021)	248	100	224	100
Education level				
Some High School	1	0.4	23	10
High School	30	12	85	38
Some College	81	33	38	17
College Degree	96	39	39	17
Some Graduate School	12	5	9	4
Graduate School	28	11	31	12
Total (χ^2=85.74, 5 df, p=.000)	248	100	225	100
Education Split of Holding College Degree				
High school or some college	112	45	146	65
College degree or higher	136	55	79	35
Total (χ^2=18.51, 1 df, p=.000)	248	100	225	100
Ecommerce experience				
1 Beginner	1	0.4	13	6
2	1	0.4	13	6
3	5	2	26	12
4 Neutral	9	4	81	36
5	63	26	38	17
6	124	50	42	19
7 Expert	44	18	12	5
Total (χ^2=85.74, 5 df, p=.000)	247	100	225	100
Mean (SD) (t=12.91, 470 df, p=.000)	5.75	(0.93)	4.30	(1.48)

Age

The mean age of the US participant was 36.26 (SD=11.71), while the mean age of the Estonian participant was three years older, 39.60 years of age (SD=14.65, t=-2.75, 470df, $p \leq .006$). The age range of US participants was from 20 to 82 years of age, while the Estonian range was 19-83 years of age, with median ages of 32 for the US and 38 for Estonia. To facilitate the regression analysis using dummy variables with values of 0 and 1, and based on an overall median=34 years, participants were collapsed into two age-based groups: those age 34 and younger (dummy variable value=0) and those age 35 and older (dummy variable value=1). Using this median split procedure, 55% of US participants were 34 or younger, and 45% were 35 or older. In Estonia, 44% were 34 or younger, and 56% were 35 or older.

Education

The two groups revealed important differences in education patterns, with the American sample having higher completed education levels overall. In the US, 1 (0.4%) had some high school, 30 (12%) completed high school, 81 (33%) attended some college, 96 (39%) completed a college degree, 12 (5%) some graduate school, and 28 (11%) completed a graduate degree. In Estonia, 23 (10%) had some high school, 85 (38%) completed high school, 38 (17%) had some college, only 39 (17%) completed a college degree, 9 (4%) attended some graduate school, and 31 (14%) completed graduate school. To facilitate the analysis, similar to age, participants were collapsed into two groups based on whether they held a college degree or not. Participants with only high school or some college (dummy variable value=0) were sorted from those who held at least a college degree (dummy variable value=1). For the resulting measure, 45% of Americans had some completed some high school or some college, while 55% had a college degree or higher. In contrast, Estonia had a larger proportion of non-degreed participants with only high

school or only some college (65%), and a lower percentage of participants who had completed a college degree or higher (35%).

Ecommerce experience

Participants were asked to rate their ecommerce experience on a 7-point scale, where 7=expert and 1=beginner. At a statistically significant level, Americans were more experienced with ecommerce (M=5.75) than their Estonian counterparts (M=4.30; t=12.91, 470df, p=.000).

In summary, Estonian participants were older, more likely female, completed less education, and reported less ecommerce experience than American participants. As will be detailed later, the differences in education levels (completion versus non-completion of a college degree) and ecommerce experience proved to be especially important confounds in understanding the participants' inclination to disclose personally identifying information. Age confounded certain findings.

WILLINGNESS TO DISCLOSE

Willingness to disclose personally identifying information was a major focus and provided the basis for the first four hypotheses in the study. Results were analyzed primarily using the 17-item list of specific PII items for which participants were asked to indicate their willingness to disclose the information on a 7-point scale, where 7=very willing to disclose and 1=not willing to disclose PII items.

Descriptive Statistics for Willingness to Disclose

The 17 items to which participants were asked to rate their willingness to disclose and their views about perceived riskiness of disclosure were exactly the same and thus are summarized here together to facilitate analysis. Each was first subjected to separate factor analyses using principal component analysis with Varimax rotation and Kaiser Normalization.

Because the resulting underlying factors followed the same general pattern, the factor analysis results are presented on a consolidated basis in Table 4.2. Details pertaining to perceived riskiness will be discussed as part of Hypothesis 7.

Table 4.2
Consolidated Factor Analysis Results for Willingness to Disclose (WD) and Perceived Risks of Disclosing (PR) Specific PII items

	Factor Loading				
Item	I	II	III	IV	V
Contact Information index					
Name (WD)	.78				
Name (PR)	.71				
Home address (WD)	.86				
Home address (PR)	.81				
Email (WD)	.74				
Email (PR)	.57				
Credit card number (WD)	**.77**			.24*	
Credit card number (PR)	.43*			**.68**	
PayPal account (WD)	.64			.45*	
PayPal account (PR)	.35*			**.60**	
Online Account information					
Twitter handle (WD)		.86			
Twitter handle (PR)		.89			
Facebook account (WD)		.88			
Facebook account (PR)		.89			
Skype username (WD)		.85			
Skype username (PR)		.89			
Life History information					
Date of birth (WD)			**.73**	.22*	
Date of birth (PR)			.32*	**.65**	
Marital status (WD)			.70		
Marital status (PR)			.79		
Age (WD)			.82		
Age (PR)			.85		
Financial/Medical History information					
Income (WD)				.68	
Income (PR)				.56	
Credit History (WD)				.79	
Credit History (PR)				.84	
Medical History (WD)				.72	
Medical History (PR)				.76	
Work-Related information					
Work address/Employer (WD)	.13*				.86
Work address/Employer (PR)	**.72**				
Work Phone (WD)	.07*				.90
Work Phone (PR)	**.70**				

Factor Analysis Summary Statistics					
Willingness to Disclose Specific PII Items					
Eigenvalue	5.67	3.33	1.61	1.27	1.06
% variance explained	33.3%	19.0%	9.5%	7.4%	6.2%
Cumulative variance explained	33.3%	52.4%	61.8%	69.3%	75.6%
Perceived Risks of Disclosing Specific PII Items					
Eigenvalue	6.55	2.44	1.31	1.94	--
% variance explained	38.5%	14.3%	7.7%	11.4%	--
Cumulative variance explained	38.5%	52.8%	60.5%	71.9%	--

Note: Boldface indicates highest factor loadings

As can be seen in Table 4.2, four factors emerged when perceived risks of disclosing specific PII items were analyzed, while 5 factors emerged for willingness to disclose. The difference was that the two items related to disclosing work-related information (address and phone number) were perceived as different from information related to disclosing one's own personal information – but *only* for willingness to disclose. These two items aligned with disclosing one's own personal information when it came to perceived riskiness.

The four factors that emerged were labeled: *contact information* used in transactions (name, home address, home phone, and email, credit card number), *online account information* (Twitter handle, Facebook account, Skype user name), *life history information* (date of birth, marital status, age), and *financial/medical history* (income, credit history, medical history). The fifth factor was named *work-related information* (work address, work phone).

Beyond differences discerned for work-related information, three other items loaded between or across factors. Participants appeared to treat credit card numbers and PayPal account information as basic information used to facilitate a transaction when judging willingness to disclose (factor I). However, their perceptions of the attendant risks for both of these payment information systems more closely aligned with the perceived risk of disclosing other financial or medical history (factor IV). In a similar way, participants appeared to be willing to provide date of birth as if it were comparable to other life history information (factor III), but their perceptions

of the related risk acted more in concert with the perceived risk of disclosing payment information and/or other financial or medical information (factor IV).

In addition to analyzing overall willingness to disclose (and perceived riskiness) based on all 17 items, based on the factor analysis, it was determined that is possible to treat the four clusters of items as separate dependent variables (see discussion in Hypothesis 7) by creating sub-indexes for contact information, online account information, life history information, and financial/medical information. In addition, the disclosure of work-related information was treated as a separate variable because of its potential application in business-to-business e-commerce and because attitude toward providing work information might differ from personal information. Finally, it was decided to treat disclosure of payment information (credit card and PayPal account information) as a sixth and separate variable in light of the keen interest in this specific topic and public concerns about identify theft and payment fraud. Overall, the factor analysis model for willingness to disclose accounted for 75.6% of the total variance.

To create indices to be used in the analysis, separate reliability analyses were then conducted on all 17 items and on each of the six sets of data as summarized in Table 4.3. The resulting Cronbach alphas demonstrated sufficient reliability (Cronbach α's ranged from .79 to .95). Notably, the principal index selected for use item the study (overall willingness to disclose index composed of all 17 items of personal data) was found to be reliable (Cronbach α =.87).

Overall, as shown in Table 4.3, participants were most willing to disclose contact information (M=5.15), and least willing to disclose financial/medical history information (M=2.10). Individuals were second most willing to disclose life history information (M=4.16), followed by payment information (3.77), work-related information (M=2.98), and online account information (M=2.53).

Table 4.3

Consolidated Summary of Indices Results for Willingness to Disclose and Perceived Risks of Disclosing Specific PII Items

Willingness to disclose (WD) (*1=not willing, 4=neutral, 7=very willing)*
Perceived risk of disclosing (PR) (*1=very risky, 4=neutral, 7=not risky)*

	Overall		US		Estonia					
Measure	*M*	*SD*	*M*	*SD*	*M*	*SD*	*df*	*t*	*p*	*Cohen's d*
Willingness to disclose index (WD)	**3.54**	**1.02**	**3.70**	**.905**	**3.37**	**1.11**	**448**	**3.45**	**.002**	**.33**
Perceived risk of disclosing index (PR)	**3.52**	**1.08**	**3.71**	**1.01**	**3.31**	**1.12**	**447**	**4.01**	**.000**	**.38**
Contact information index (WD)	**5.15**	**1.39**	**5.38**	**1.21**	**4.90**	**1.53**	**464**	**3.81**	**.000**	**.35**
Contact information index (PR)	**4.21**	**1.42**	**4.43**	**1.38**	**3.97**	**1.45**	**466**	**3.51**	**.000**	**.32**
Name (WD)	5.59	---	5.81	---	5.34	---	---	---	.001	---
Name (PR)	4.62	---	4.81	---	4.41	---	---	---	.007	---
Home Address (WD)	4.90	---	5.38	---	4.37	---	---	---	.000	---
Home Address (PR)	3.80	---	4.16	---	3.40	---	---	---	.000	---
Home Phone (WD)	4.46	---	4.46	---	4.46	---	---	---	.968	---
Home Phone (PR)	3.84	---	3.95	---	3.71	---	---	---	.123	---
Email (WD)	5.69	---	5.85	---	5.51	---	---	---	.011	---
Email (PR)	4.61	---	4.80	---	4.40	---	---	---	.011	---
Online account information index (WD)	**2.53**	**1.70**	**2.59**	**1.76**	**2.46**	**1.63**	**468**	**.833**	**.405**	**.08**
Online account information index (PR)	**3.36**	**1.64**	**3.64**	**1.66**	**3.05**	**1.57**	**467**	**3.92**	**.000**	**.37**
Twitter handle (WD)	2.62	---	2.84	---	2.39	---	---	---	.008	---
Twitter handle (PR)	3.44	---	3.80	---	3.04	---	---	---	.000	---
Facebook account (WD)	2.57	---	2.60	---	2.25	---	---	---	.627	---
Facebook account (PR)	3.29	---	3.52	---	3.04	---	---	---	.002	---
Skype username (WD)	2.41	---	2.35	---	2.48	---	---	---	.432	---

	Overall		US		Estonia					
Measure	*M*	*SD*	*M*	*SD*	*M*	*SD*	*df*	*t*	*p*	*Cohen's d*
Skype username (PR)	3.34	---	3.57	---	3.07	---	---	---	.001	---
Life history information index (WD)	**4.16**	**1.71**	**4.12**	**1.72**	**4.20**	**1.70**	**464**	**-.510**	**.610**	**.05**
Life history information index (PR)	**4.20**	**1.59**	**4.30**	**1.52**	**4.09**	**1.69**	**464**	**1.44**	**.151**	**.13**
Date of birth (WD)	4.19	---	3.96	---	4.45	---	---	---	.008	---
Date of birth (PR)	3.84	---	3.64	---	4.06	---	---	---	.015	---
Marital status (WD)	3.68	---	3.83	---	3.52	---	---	---	.111	---
Marital status (PR)	4.21	---	4.61	---	3.76	---	---	---	.000	---
Age (WD)	4.62	---	4.61	---	4.63	---	---	---	.939	---
Age (PR)	4.56	---	4.69	---	4.41	---	---	---	.089	---
Financial/Medical history index (WD)	**2.10**	**1.28**	**2.08**	**1.24**	**2.13**	**1.33**	**468**	**-.436**	**.663**	**.04**
Financial/Medical history index (PR)	**2.77**	**1.46**	**2.91**	**1.44**	**2.61**	**1.47**	**468**	**2.29**	**.023**	**.21**
Income (WD)	2.43	---	2.60	---	2.25	---	---	---	.024	---
Income (PR)	3.09	---	3.53	---	2.60	---	---	---	.000	---
Credit history (WD)	2.12	---	1.99	---	2.26	---	---	---	.053	---
Credit history (PR)	2.58	---	2.61	---	2.55	---	---	---	.682	---
Medical history (WD)	1.78	---	1.67	---	1.90	---	---	---	.057	---
Medical history (PR)	2.65	---	2.62	---	2.68	---	---	---	.711	---
Work-related information index (WD)	**2.98**	**1.81**	**2.96**	**1.81**	**3.00**	**1.81**	**469**	**-.205**	**.838**	**.02**
Work-related information index (PR)	**3.29**	**1.72**	**3.42**	**1.79**	**3.14**	**1.62**	**469**	**1.81**	**.072**	**.16**
Work address (WD)	3.04	---	3.07	---	3.00	---	---	---	.688	---
Work address (PR)	3.27	---	3.42	---	3.09	---	---	---	.041	---

	Overall		US		Estonia					
Measure	*M*	*SD*	*M*	*SD*	*M*	*SD*	*df*	*t*	*p*	*Cohen's d*
Work phone (WD)	2.92	---	2.85	---	2.99	---	---	---	.430	---
Work phone (PR)	3.30	---	3.42	---	3.18	---	---	---	.148	---
Payment information index (WD)	**3.77**	**1.83**	**4.60**	**1.55**	**2.84**	**1.68**	**463**	**11.75**	**.000**	**1.09**
Payment information index (PR)	**2.79**	**1.58**	**3.21**	**1.65**	**2.31**	**1.37**	**463**	**6.43**	**.000**	**.59**
Credit card number (WD)	3.87	---	4.80	---	2.84	---	---	---	.000	---
Credit card number (PR)	2.46	---	2.87	---	2.00	---	---	---	.000	---
PayPal account (WD)	3.66	---	4.39	---	2.85	---	---	---	.000	---
PayPal account (PR)	3.11	---	3.56	---	2.60	---	---	---	.000	---

Hypothesis 1 – Nationality Effects on Willingness to Disclose

Hypothesis 1 stated Estonians would be more willing than Americans to disclose specific PII items. H1 was not supported; instead, significant results in the *opposite* direction were found, suggesting Americans – not Estonians – are more willing to disclose personal data.

Table 4.3 summarizes the t-test comparisons between Americans and Estonians for the overall willingness to disclose index, as well as for the six sub-indices. Americans (M=3.70, SD=.905) are more willing to disclose the 17 items of PII than Estonians (M=3.37, SD=1.11; t=3.45, df=448, p≤.002). Overall, this difference in willingness to disclose can be attributed to differences in willingness to disclose contact information (US M=5.38, Estonia M=4.90, t=3.81, df=464, p=.000) and differences in willingness to disclose payment information (US M=4.60, Estonia M=2.84, t=11.75, df=463, p=.000), while differences for the remaining 4 sub-indices (online account information, life history information, financial/medical history, and work-related information) were not statistically significant.

To investigate how well the demographic variables (education level, gender, age and ecommerce experience) predict willingness to disclose, a hierarchical multiple regression was conducted using the 17-item willingness to disclose as the dependent measure. In Step 1, nationality was entered as a predictor variable. When nationality alone was considered, it significantly predicted willingness to disclose, (β = -.161, p≤ .001, R^2 = .024). However, as indicated by the R^2=.024, only 2% of the variance in willingness to disclose could be explained by knowing the participants' nationality. In Step 2, the addition of education, gender, and age did not significantly improve the prediction because none were significant. In Step 3, the addition of ecommerce experience was significant in predicting willingness to disclose (β= .211, p≤ .001, adjusted R^2 = .031), *eliminating the significant effect of nationality.* With the final step's

combination of predictors, ecommerce experience had the highest beta (β =.21, p≤.001), while education (β =-.094, p≤.001) remained significant in predicting willingness to disclose. But together, the addition of ecommerce experienced explained only an additional 3.1% of the variance, and the variables included in Step 3 accounted for only 6% of the variance. This suggests factors other than demographics are important to consider (see Hypotheses 2-4).

Table 4.4
Hierarchical Multiple Regression Model for Willingness to Disclose Index 17 PII items

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.024***	.026***
Nationality	-.327	.095	-.161***		
Step 2:				.035**	.009
Nationality	-.370	.098	-.182***		
Education	-.189	.097	-.093		
Gender	.012	.097	.006		
Age	. 035	.095	.017		
Step 3:				.06***	.031***
Nationality	-.158	.111	-.078		
Education	-.192	.096	-.094***		
Gender	-.003	.096	-.001		
Age	.114	.096	.056		
Ecommerce Experience	.151	.039	.211***		

*p≤ .05; **p≤.01; ***p≤ .001

The results in Table 4.4 were further analyzed by splitting the file and analyzing the same regression results for the United States and Estonia separately – a technique subsequently used for analysis and referred to as a "split file regression analysis." In this procedure, by necessity, nationality had to be removed from the regression model. For the United States, ecommerce experience had no effect on willingness to disclose (β =.065, p≤.316), but the completion of a college degree did. Individuals without a degree were more willing to disclose PII than participants with a degree (β =-.134, p≤.039). For Estonia, no difference was found for any of the demographic variables, but greater ecommerce experience positively influenced willingness to disclose. Individuals with greater experience were more willing to disclose PII (β =.248, p≤.001).

Thus, the two variables impact willingness to disclose differentially in the US and Estonia – a consideration important in analyzing H2-H4.

Hypothesis 2 – Impact of Perceived Benefits on Willingness to Disclose

Hypothesis 2 stated Estonians were less likely to disclose PII items based on perceived benefits received in exchange for providing information compared to Americans. H2 was supported.

Four different, but related measures were used in order to measure perceived benefits of exchanging PII information, including characterizing the purchase of a product online as benefit opportunity, the likelihood of finding a bargain while shopping online, purchase benefits (value propositions [i.e., greater merchandise selection, better customer service, tailored product offerings, special discounts] for customers in exchange for providing some personal information), and exchanging PII for certain privacy guarantees expected while shopping.

The opportunity benefits index and bargain likelihood indices were adapted from Jarvenpaa et al. (1999) which measured general risk perception of shopping on the Internet. Reliability analysis demonstrated adequate Cronbach alphas for both the opportunity benefits index (Cronbach α=.78) and bargain likelihood (Cronbach α=.85) index as replicated from their original source. Although the purchase benefits and privacy benefits expected index originated as a single index used by Gupta et al. (2010), factor analysis was conducted on the ten original items, and revealed two underlying dimensions. These were labeled *purchase benefits* (Eigenvalue=3.979, accounting for 39.90% of variance) and *privacy benefits expected* (Eigenvalue=3.619, 36.17% of variance). Separately, the 10-items split into two factors accounted for 75.98% of the total variance.

A correlation analysis showed that the four benefits indices were all highly correlated at the p=.000 level (except for one at the p≤.038 level). Although the researcher considered developing a single "benefits" super-index, a factor analysis of all the benefits-related items in Table 4.5 confirmed that they properly fell into the four categories shown and thus should be best analyzed separately. The factor analysis (table not provided) explained 75% of variance. Separate reliability analyses were conducted on each of the four sets of data, as summarized in Table 4.5, with the resulting Cronbach alphas all demonstrating sufficient reliability (Cronbach α's ranged from .78 to .90).

Table 4.5 presents the t-tests for the two countries for participants' perceptions about the four potential ecommerce benefits. For the opportunity benefits index, when asked "How would you characterize a decision of whether to buy a product from an online retailer?" Americans (M=5.18, SD=.996) were more positive than Estonians (M=4.40, SD=1.10) about perceptions regarding potential benefits of shopping online (t=8.46, df=469, p=.000). Americans (M=5.92, SD=.962) were significantly more positive then Estonians (M=5.12, SD=1.20) on the bargain likelihood index when asked "What is the likelihood of finding a bargain by purchasing a good or service online?" (t=7.95, df=463, p>.000). For the five scenarios that comprised the purchase benefits index, Americans (M=4.38, SD=1.42) were significantly more willing than Estonians (M=4.08, SD=1.52) when asked "I am willing to give my information to online companies if…" (t=2.24, df=468, p≤.026). Continuing the trend, Americans (M=5.41, SD=1.41) scored significantly higher than Estonians (M=4.23, SD=1.38) when considering privacy benefits (t=9.1, df=466, p=.000).

Table 4.5
Perceptions of Potential Ecommerce Benefits

Measure	United States		Estonia		df	t	p	Cohen's d
	M	SD	M	SD				
This set of statements is about purchasing goods or services from online merchants. Think in general about your previous experiences purchasing goods or services online. For each of the following pairs of adjectives, select the number that best describes your feelings: (1=negative, 4= neutral, 7=positive)								
How would you characterize a decision of whether to buy a product from an online retailer?								
A. Opportunity benefits index	**5.18**	**.996**	**4.40**	**1.10**	**469**	**8.46**	**.000**	**.74**
Significant opportunity/Significant risk	5.08	---	4.31	---	---	---	.000	---
High potential for loss/High potential for gain	5.15	---	4.36	---	---	---	.000	---
Very positive situation/Very negative situation	5.32	---	4.55	---	---	---	.000	---
What is the likelihood of finding a bargain by purchasing a good or service online?								
B. Bargain likelihood index	**5.92**	**.962**	**5.12**	**1.20**	**463**	**7.95**	**.000**	**.74**
Very unlikely/Very likely	6.09	---	5.43	---	---	---	.000	---
Probably/Not probable	5.93	---	5.06	---	---	---	.000	---
Happens all the time/Never happens	5.75	---	4.92	---	---	---	.000	---
Websites sometimes offer coupons or discounts in exchange for providing personal information, such as your email address or phone number. Below are some benefits that might be received in exchange for your personal information. For each of the following statements, please indicate your level of willingness to provide information to companies where 1 = not willing and 7 = very willing. (1=not willing, 4=neutral, 7=very willing)								
I am willing to give my information to online companies if:								
C. Purchase benefits index	**4.38**	**1.42**	**4.08**	**1.52**	**468**	**2.24**	**.026**	**.20**
The company tailors their product offerings to my tastes.	3.86	---	3.75	---	---	---	.112	---
The company tailors their product offerings to	4.90	---	3.99	---	---	---	.908	---

my tastes.								
It will help me save time when I make my next purchase from the same site.	4.53	---	4.29	---	---	---	.243	---
I can get better customer service from the company.	4.34	---	4.08	---	---	---	.262	---
It will provide a greater merchandise selection.	4.28	---	4.18	---	---	---	.096	---
D. Privacy benefits expected index	**5.41**	**1.41**	**4.23**	**1.38**	**466**	**9.10**	**.000**	**.85**
The company website clearly states how my personal information will be used.	5.26	---	4.08	---	---	---	.000	---
The company website lets me know that they respect my privacy rights.	5.19	---	3.93	---	---	---	.000	---
I always know the purpose of the information being collected.	5.30	---	3.78	---	---	---	.000	---
I have a choice in whether my personal information should be disclosed to a third party.	5.54	---	4.37	---	---	---	.000	---
At any time, I can delete or edit my personal information.	5.75	---	4.99	---	---	---	.000	---

Correlational analysis showed that willingness to disclose was positively related to all four benefits identified in the study: perceived purchasing benefits (r=.448), privacy expectation benefits (r=.381), opportunity benefits (r=.263) and likelihood of obtaining a bargain (r=.173, all p=.000). To investigate how well the variables measuring perceptions of potential ecommerce benefits predict willingness to disclose, a hierarchical multiple regression was performed using willingness to disclose as the dependent measure. This followed the same procedure used in testing Hypothesis 1, but omitted gender and age in Stage 2 because these were not significant in predicting willingness to disclose. In Step 1, nationality was entered as the predictor variable. When nationality alone was considered, it again significantly predicted willingness to disclose in favor of the United States (β = -.144, $p \leq .01$, R^2 = .021). In Step 2, education level (β=-.098, $p \leq .05$) and nationality (β=-.161, $p \leq .001$) were both statistically significant in predicting disclosure. The second model accounted for an increase of less than 1% of the variance versus step 1 ($R^2\Delta$=.09, $p \leq .05$). In Step 3, nationality, education (β=-.098,$p \leq .05$) and ecommerce experience (β=.168, $p \leq .01$) produced significance, and again, nationality was no longer significant. (These results followed the same pattern discerned for Hypothesis 1: When the files were split and separate regression analyzes are conducted for each nation, the education effect can be explained by Americans with lower education being more willing to disclose; while the ecommerce experience effect can be attributed to a positive relationship between ecommerce experience and willingness to disclose among Estonians.)

The final model, Step 4, introduced the four ecommerce benefits measures and was statistically significant (R^2=.236, $p \leq .001$). The four ecommerce benefits variables accounted for an additional 18.5% of the variance, raising the total variance explained by the model to 23.6%. Among the four ecommerce benefits variables however, two were statistically significant

predictors of willingness to disclose in exchange for ecommerce benefits: opportunity benefits (β=.111, p≤.01) and purchase benefits (β=.352, p≤.001). Notably, nationality remained non-significant. When separate regressions were conducted by nationality, slightly different results were obtained. For Americans, the effect of education was preserved (β=100, p≤.040) along with purchase benefits (β=.485, p=.000), but opportunity benefits were not significant (β=.079, p≤.227). Meanwhile, for Estonians, none of the four benefits were significant, although opportunity benefits approached the significance level (β=142, p≤.065). Moreover, the effects of ecommerce experience became nonsignificant among Estonians (β=.118, p≤.088).

Table 4.6
Hierarchical Multiple Regression Model Willingness to Disclose on Benefits Exchange

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.021**	.021**
Nationality	-.292	.096	-.144**		
Step 2:				.030***	.009*
Nationality	-.326	.097	-.161***		
Education	-.198	.097	-.098*		
Step 3:				.051***	.021**
Nationality	-.158	.111	-.078		
Education	-.199	.096	-.098*		
Ecommerce experience	.120	.039	.168**		
Step 4:				.236***	.185***
Nationality	-.033	.111	-.016		
Education	-.161	.087	-.080		
Ecommerce experience	.042	.037	.059		
Opportunity benefits	.104	.049	.111**		
Bargain likelihood	.049	.044	.056		
Purchase benefits	.242	.043	.352***		
Privacy benefits	.040	.045	.059		

*p≤ .05; **p≤.01; ***p≤ .001

Hypothesis 3 – Impact of Personality on Willingness to Disclose

Hypothesis 3 investigated the relationship of the personality traits found in the Big Five Inventory (BFI) -- neuroticism, openness, extraversion, conscientiousness, and agreeableness -- to willingness to disclose personally identifying information. H3 was partially supported.

Table 4.7
Factor Analysis of the 5 Personality Variables

	Factor Loading				
	I	II	III	IV	V
Item	Neuroticism	Openness	Extraversion	Conscientiousness	Agreeableness
Is relaxed	.69				
Gets nervous easily	.82				
Worries a lot	.84				
Can be tense	.78				
Is inventive		.78			
Active imagination		.79			
Curious		.69			
Original, new ideas		.78			
Is talkative			.82		
Is outgoing, sociable			.79		
Is reserved (R)			.74		
Is shy (R)			.78		
Does a thorough job				.74	
Does things efficiently				.71	
Tends to be disorganized (R)				.80	
Tends to be lazy (R)				.77	
Is generally trusting					.68
Is considerate and kind					.77
Tends to find fault (R)					.50
Likes to cooperate					.75
Factor Analysis Summary Statistics					
Eigenvalue	5.13	2.65	2.21	1.75	1.35
% variance explained	25.6%	13.3%	11.4%	8.7%	6.7%
Cumulative variance explained	25.6%	38.9%	49.9%	58.6%	65.4%

As described in the Methods chapter, each of the five personality traits was measured using 4-item scales – presented in an intermixed bank of 20 items on the survey. A confirmatory factor analysis of all 20 items (Table 4.7) resulted in the expected 5 factors, with all items loading on the proper factor as (Schmitt et al.,2007, p. 186). After six iterations, each of the 20 items loaded on the single factor with a loading of .500 or higher (except for one item, *Tends to Find Fault with Others*, which loaded at .495). The 5-factor model accounted for 65.4% of the total variance in the 20 items.

Based on the factor analysis, separate reliability analyses were conducted on each of the five sets of items as summarized in Table 4.8. Except for one scale (agreeableness index), the resulting Cronbach alphas for other indices all demonstrated acceptable reliability (Cronbach α's ranged from .79 to .84).

Table 4.8 also summarizes the t-tests between Americans and Estonians for the BFI personality scales, which reveal significant differences in personality dimensions between the two countries: the sampled Estonians (M=4.20, SD=1.05) are more extraverted than the sampled Americans (M=3.62, SD=1.45) (t=-4.85, df=465, p=.000). Estonians (M=3.84, SD=1.19) were significantly higher in neuroticism than Americans (M=3.40, SD=1.51; t=-3.47, df=462, $p \leq .001$). The indices for openness and conscientiousness were also statistically significant. In contrast to Estonia, Americans demonstrated more openness (M=5.21, SD=1.22) than Estonians (M=5.00, SD=.945 t=2.09, df=462, $p \leq .037$), and scored higher in conscientiousness (M=5.53, SD=1.12) than Estonians (M=4.80, SD=.989; (t=-3.47, df=462, $p \leq .001$). Agreeableness was the one personality factor in which there was no significant difference between participants in the two countries, an issue that might be accounted for by the low reliability of the index among the Estonian sample (Cronbach α=.56).

Table 4.8
Five Personality Scales

(1 = strongly disagree, 4=neutral, 7 = strongly agree)

I am someone who…	United States		Estonia					
Measure	M	SD	M	SD	df	t	p	Cohen's d
Extraversion index	**3.62**	**1.45**	**4.20**	**1.05**	**465**	**-4.85**	**.000**	**.46**
…is talkative	3.59	---	4.33	---	---	---	.000	---
…is outgoing, sociable	3.80	---	4.94	---	---	---	.000	---
…is reserved (R)	3.20	---	3.20	---	---	---	.996	---
…is shy, inhibited (R)	3.91	---	4.33	---	---	---	.007	
Openness index	**5.21**	**1.22**	**5.00**	**.945**	**462**	**2.09**	**.037**	**.19**
…is inventive	4.90	---	5.14	---	---	---	.057	---
…has an active imagination	5.25	---	4.96	---	---	---	.031	---
…is curious about many different things	5.63	---	5.35	---	---	---	.019	---
…is original, has new ideas	5.08	---	4.54	---	---	---	.000	---
Neuroticism index	**3.40**	**1.51**	**3.84**	**1.19**	**462**	**-3.47**	**.001**	**.32**
…is relaxed, handles stress well (R)	2.92	---	3.45	---	---	---	.000	---
…gets nervous easily	3.44	---	3.64	---	---	---	.206	---
…worries a lot	3.59	---	4.30	---	---	---	.000	---
…can be tense	3.67	---	3.96	---	---	---	.054	---
Conscientious index	**5.53**	**1.12**	**4.80**	**.989**	**467**	**7.40**	**.000**	**.69**
…does a thorough job	5.96	---	5.29	---	---	---	.000	---
…does things efficiently	5.76	---	4.89	---	---	---	.000	---
…tends to be disorganized (R)	5.15	---	4.72	---	---	---	.004	---
…tends to be lazy (R)	5.26	---	4.33	---	---	---	.000	---
Agreeableness index	**5.01**	**1.14**	**5.08**	**.830**	**469**	**-.797**	**.426**	**.07**
…is generally trusting	4.48	---	5.21	---	---	---	.000	---
…is considerate and kind to almost everyone	5.64	---	5.25	---	---	---	.000	---
…tends to find fault with others (R)	4.71	---	5.08	---	---	---	.009	---
…likes to cooperate with others	5.21	---	4.77	---	---	---	.000	---

H3 predicted that willingness to disclose would be positively related to a) extraversion, b) openness, c) conscientiousness, and d) agreeableness and e) negatively related to neuroticism. Partial support for H3 can be evidenced in the correlational analysis, which showed, as predicted,

that the 17-items willingness to disclose index was positively related to two personality traits: openness (r=.109, p≤.022), and agreeableness (r=.149, p≤.002) and negatively related to neuroticism (r=-.115, p≤.015). However, significant correlations were not found between willingness to disclose and extraversion (r=.013, p≤.077, n.s.) or between willingness to disclose and conscientiousness (r=.087, p≤.067, n.s.).

To further investigate how well the five personality variables predict willingness to disclose, hierarchical multiple regression was used as in H1 and H2, substituting the 5 personality factors in Step 4. An analysis using the same split-file procedure used previously showed the same general confound reported for willingness to disclose pertaining to education and experience: Americans without a degree appeared to be more willing to disclose and Estonians with more ecommerce expertise appeared to be more willing to disclose. Although the entire model in Step 4 was statistically significant (p≤.001), the addition of personality traits explained an additional 3.3% (p≤.05) of the variances, and the 8 variables accounted for 8.8% of the variance. Only two items in Step 4 were statistically significant predictors of willingness to disclose: ecommerce experience (β=.163, p≤.01) and agreeableness (β=.154, p≤.01). As with H1 and H2, the effect of nationality became nonsignificant (β=.-093, n.s.). Importantly, a regression analysis by nationality revealed that agreeableness only had an effect within the American sample (β=.217, p≤.002) but not among Estonians (β=.118, p≤.156). Meanwhile willingness to disclose was only explained by ecommerce experience among Estonians (β=.236, p≤.001), but not Americans (β=.014, p≤.833).

Table 4.9
Hierarchical Multiple Regression Model for Willingness to Disclose: Effects of Personality Traits

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.020**	.023**
Nationality	-.302	.095	-.152**		
Step 2:				.031***	.008
Nationality	-.335	.097	-.168***		
Education	-.187	.097	-.094		
Step 3:				.055***	.024***
Nationality	-.157	.110	-.079		
Education	-.193	.096	-.097*		
Ecommerce experience	.126	.039	.179***		
Step 4:				.088***	.033*
Nationality	-.186	.115	-.093		
Education	-.203	.095	-.102		
Ecommerce experience	.115	.039	.163**		
Extraversion	-.008	.040	-.011		
Openness	.075	.047	.083		
Neuroticism	-.014	.037	-.020		
Conscientious	-.039	.049	-.043		
Agreeableness	.152	.051	.154**		

*p≤ .05; **p≤.01; ***p≤ .001

Hypothesis 4 – Impact of Trust on Willingness to Disclose

H4 predicted willingness to disclose based on the 17-item index was positively related to a) trust in the Internet and b) being a trusting person more generally, as evidenced in trust in institutions. H4 was supported, although findings suggest differences in trust levels between Americans and Estonians.

The first trust measure, trust in the Internet, was a five-item index adapted from Dinev and Hart (2006). The index was not subjected to factor analysis but showed high reliability (Cronbach α=.88), as shown in Table 4.10. Interestingly, there is a significant difference between the US (M=4.76, SD=.996) and Estonia (M=3.81, SD=1.10), with Americans reporting higher trust in the Internet (difference = .955; t=9.91, df=470, p=.000).

Table 4.10
Trust in the Internet

(1=strongly disagree, 4=neutral, 7=strongly agree)

	United States		Estonia					
Measure	M	SD	M	SD	df	t	p	Cohen's d
Trust in the Internet index	**4.76**	**.996**	**3.81**	**1.10**	**470**	**9.91**	**.000**	**.91**
The Internet is a safe environment in which to exchange information with others.	4.34	---	3.75	---	---	---	.000	---
The Internet is a reliable environment in which to conduct business transactions or personal purchases.	5.21	---	4.04	---	---	---	.000	---
Internet merchants are dependable.	5.07	---	3.78	---	---	---	.000	---
The Internet can be trusted.	4.42	---	3.65	---	---	---	.000	---

The second trust measure investigated in H4b was the trust in institutions index adapted from 4 items used by Torney-Purta et al. (2004) and shown in Table 4.11. The items were not subjected to factor analysis but demonstrated good reliability as an index (Cronbach α=.80). In contrast to Americans, who were more favorable than Estonians toward the Internet, Estonians demonstrated significantly greater trust in institutions than Americans (Estonians M=4.33, SD=1.01; Americans M=4.04, SD=.982; t=-3.10, df=466, $p \leq .002$). Notably, participants in both countries were most trusting of local businesses and least trusting of the national governments. Of particular note, Americans (M=3.54) were significantly lower in their trust of national government compared to Estonians (M=3.95,$p \leq .002$). Estonians were also more favorable toward international businesses compared to Americans (US M=3.79, Estonian M=4.58, p=.000).

Using a separate item not included in the 4-item index, Estonians were asked to report their trust in the European Union, the regional governing body responsible for various economic and political policies, including many Internet policies to which Estonia must adhere. While the

score for trust in the EU (M=4.28) was higher than Estonians' views of both local government (M=4.14) and Estonian national government (M=3.95), it was lower than their views of local businesses (M=4.66) or international businesses (M=4.58).

Table 4.11
Trust in Institutions

(1=never, 4=sometimes, 7=always)

	United States		Estonia					
Measure	M	SD	M	SD	df	t	p	Cohen's d
Trust in institutions index	**4.04**	**.982**	**4.33**	**1.01**	**466**	**-3.10**	**.002**	**.29**
National government	3.54	---	3.95	---	---	---	.002	---
Local government	4.00	---	4.14	---	---	---	.254	---
Local businesses	4.83	---	4.66	---	---	---	.084	---
International business	3.79	---	4.58	---	---	---	.000	---
The European Union*	---	---	4.28	---	---	---	---	---

*(Estonia only)

Support for H4 was evident in a correlational analysis that showed, as predicted, the 17-items willingness to disclose index was positively related to both trust in the Internet (r=.336, p=.000), and trust in institutions (r=.201, p=.000) as well as the trust in EU item (relevant for Estonian participants) (r=.222, p≤.001).

A preliminary analysis of trust in institutions showed no significant differences among participants across the study based on gender, education, or age. Similarly, no differences were found in trust in the internet based on gender (Males M= 4.42, Females M=4.22, t=1.82, 469df, p≤.069). However, trust in the Internet differed significantly based on age: Younger participants (M=4.43) were more trusting of the Internet than older participants (M=4.19, t=2.25, 469df, p≤.025). Significant differences in trust of the Internet also were detected based on education. Participants with a college degree (M=4.43) were more trusting than those without a college degree (M=4.21, t=-2.14, 470df, p≤.033).

To formally test H4, and to understand the role of trust in tandem with the significant demographic variables identified in the study, hierarchical multiple regression was performed (Table 4.12) in the same manner as in H1, H2, and H3, substituting trust in the Internet and trust in institutions in Step 4. (Because gender and age did not have a significant effect on willingness to disclose, these were omitted from the analysis although both are possible confounds in understanding trust.) The entire model in Step 4 was statistically significant. The addition of the two trust items explained an additional 9.6% ($p \leq .001$) of the variance and the five variables together accounted for 15.9% ($p \leq .001$) of the variance. The model suggests four items as statistically significant predictors of willingness to disclose when taking trust into account: education ($\beta = -.099$, $p \leq .05$), ecommerce experience ($\beta = .136$, $p \leq .01$), trust in the Internet ($\beta = .235$, $p \leq .001$), and lastly, trust in institutions ($\beta = .177$, $p \leq .001$). Similar to H1, H2, and H3, differences based on nationality became nonsignificant ($\beta = -.044$, n.s.) in Step 4. This suggests that trust, in fact, is a possible factor in willingness to disclose.

Table 4.12
Hierarchical Multiple Regression Model for Willingness to Disclose: Effect of Trust in the Internet and Trust in Institutions

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.028***	.028***
Nationality	-.340	.095	-.168***		
Step 2:				.034***	.006
Nationality	-.368	.096	-.182***		
Education	-.161	.097	-.079		
Step 3:				.063***	.029***
Nationality	-.168	.109	-.083		
Education	-.163	.095	-.081		
Ecommerce experience	.140	.038	.198***		
Step 4:				.159***	.096***
Nationality	-.089	.109	-.044		
Education	-.201	.091	-.099*		
Ecommerce experience	.097	.038	.136**		
Trust in the Internet	.209	.047	.235***		
Trust in Institutions	.178	.047	.177***		

*p≤ .05; **p≤.01; ***p≤ .001

When a split-file regression was performed, the effects of trust were corroborated in both countries. The effects of education were significant in the US (US β=-152, p≤.015; Estonia β=-.921, p≤.349) and the effects of ecommerce experience were significant in Estonia (US β=.005, p≤.941; Estonia β=.186, p≤.008).

Summary of Hypotheses Related to Willingness to Disclose (H1-H4)

From the results in H1-H4, 7 variables were identified that appear to have important value in explaining willingness to disclose. These included education, ecommerce experience, opportunity benefits, purchase benefits, agreeableness, trust in the Internet and trust in institutions. To examine their possible impact, separate regression analyses were performed to identify the differences between the US and Estonian in predicting willingness to disclose 17 items of PII (Table 4.13). A preliminary run showed that opportunity benefits and agreeableness were not significant in either nation, and so these were eliminated from the analysis. The regression model for the United States (R^2=.279, p≤.001) found both education (β=-.120, p≤.05) and purchase benefits (β=.453, p≤.001) were significant predictors in willingness to disclose. For Americans, individuals who have less education are more willing to disclose, whereas those who perceive more purchase benefits are more willing to disclose. For Estonians, four variables were significant predictors of willingness to disclose the overall 17 PII items. The regression model (R^2=.255, p≤.001) showed that trust in institutions (β=.133, p≤.05), trust in the Internet (β=.214, p≤.01), ecommerce experience (β=.134, p≤.05), and purchase benefits (β=.299, p≤.001) all significantly predicted an individual's willingness to disclose. However, education was not significant (β=-.040, n.s), as it was in the US model. The combination of all four variables in the model accounted for 27.9% of the total variance in United States (p≤.001) and 25.5% of the total variance in the Estonia (p≤.001).

Table 4.13
Summary Regression Models for Willingness to Disclose, United States and Estonia

Country and predictor variable	*B*	*SE B*	*ß*	*R*	R^2
US				.528	279***
Trust in Institutions Scale	.099	.055	.107		
Trust in the Internet	.033	.060	.037		
Ecommerce Experience	.020	.057	.021		
Purchase Benefits	.288	.039	.453***		
Education	-.217	.102	-.120*		
Estonia				.505	.255***
Trust in Institutions Scale	.146	.072	.133*		
Trust in the Internet	.216	.068	.214**		
Ecommerce Experience	.101	.049	.134*		
Purchase Benefits	.218	.046	.299***		
Education	-.093	.143	-.040		

*p≤ .05; **p≤.01; ***p≤ .001

For both countries, purchase benefits were the largest significant positive predictor of willingness to disclose (US β=.453, Estonia β=.299, both p≤.001). Secondary to purchase benefits for Estonians, trust in the Internet was the next largest positive predictor of an individual's willingness to disclose 17 items of PII.

ATTITUDE TOWARD DISCLOSING INFORMATION

Hypothesis 5 – Attitude toward disclosing information online in general

As an alternative measure to willingness to disclose 17 specific PII items, this study included attitude toward disclosing information as a general measure of predisposition toward disclosure. Specifically, Hypothesis 5 predicted that Estonians would demonstrate a more positive attitude toward disclosing online in general than Americans. H5 was not supported. In fact, the results were in the opposite direction from the prediction.

Attitude toward disclosing personally identifying information online (PII) were measured utilizing a self-developed 7-item scale. After demonstrating reliability during pilot testing, the

same scale (Table 4.14) was administered to both Americans and Estonians. A confirmatory factor analysis showed that the items clustered into a single factor (Eigenvalue=4.27, accounting for 61% of the variance), and the resulting index demonstrated good reliability (Cronbach α=.89). When asked to rate seven adjective pairs for "I would describe providing information online as:" Americans (M=4.38, SD=.947) were significantly more positive in their attitude toward disclosing PII online in general than Estonians (M=3.55, SD=1.00, t=9.25, df=467, p=.000).

Table 4.14
Attitude Toward Disclosing Personally Identifying Information Online
(*1=negative, 4=neutral, 7=positive)*

	United States		Estonia					
Measure	M	SD	M	SD	df	t	p	Cohen's d
Attitude toward disclosing PII index	4.38	.947	3.55	1.00	467	9.25	.000	.85
Risky/Safe	3.89	---	3.21	---	---	---	.000	---
Trustworthy/Untrustworthy (R)	4.01	---	3.53	---	---	---	.000	---
Unreliable/Reliable	4.35	---	3.44	---	---	---	.000	---
Bad/Good	4.28	---	3.47	---	---	---	.000	---
Unimportant/Necessary	5.14	---	3.66	---	---	---	.000	---
Not valuable/Valuable	4.66	---	3.76	---	---	---	.000	---
Always willing/Never willing (R)	4.34	---	3.76	---	---	---	.000	---

A correlation analysis showed that attitude toward disclosure was positively related to willingness to disclose the 17 PII items (r=.487, p=.000).

To investigate how well the nationality and the demographic variables (education level, gender, age and ecommerce experience) predict attitudes disclosing PII online in general, a hierarchical multiple regression was computed using the 7-item attitude toward disclosing index as the dependent measure (see Table 4.15). In Step 1, nationality was entered as the predictor variable. When nationality alone was considered, it predicted attitude toward disclosure in

general (β = -.390, p≤ .001, R^2 = .152) and accounted for 15% of the variance (p≤.001). In Step 2, the addition of demographic variables produced a significant effect, however the increase in total variance explained was minimal (R^2 Δ=.016, p≤.05). Nationality (β =-.382, p≤.001) and age (β =-.121, p≤.01) were both significant predictors of attitude toward disclosing online in general in Step 2. The results suggested that Americans (versus Estonians) and younger individuals (age 34 and under; age 35 and over) had more positive attitude toward disclosing PII online in general. The addition of ecommerce experience in Step 3 also proved a significant positive predictor of attitude toward disclosing online (β= .246, p≤ .001), and nationality (β =-.260, p≤.001) was still significant in Step 3. Ecommerce experience accounted for an additional 4.3% (p≤.001) of the variance, and the five variables in Step 3 accounted for 21% of the total variance for the model (R^2=.211, p≤.001).

Table 4.15
Hierarchical Multiple Regression Model for Attitudes Disclosing Online in General

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.152***	.152***
Nationality	-.824	.090	-.390***		
Step 2:				.168***	.016*
Nationality	-.807	.093	-.382***		
Education	.009	.092	.004		
Gender	.097	.092	.046		
Age	-.255	.090	-.121**		
Step 3:				.211***	.043***
Nationality	-.550	.104	-.260***		
Education	.005	.090	.002		
Gender	.080	.090	.037		
Age	-.159	.090	-.075		
Ecommerce experience	.182	.037	.246***		

*p≤ .05; **p≤.01; ***p≤ .001

A split-file regression showed similar support for the importance of ecommerce experience on attitude toward the disclosure in both countries (US β=.151, p≤.019; Estonia β=.269, both p=.000). Of note, however, the effects of age appear to apply only in Estonia. The

effect of age in the US model was not significant (US β=-.005, p≤.937) but was significant in Estonia in favor of younger users (β=-.269, p=.000).

ANXIETY ABOUT DISCLOSING PERSONALLY IDENTIFYING INFORMATION

Hypothesis 6 – Anxiety over disclosing PII

Similar to attitude toward disclosure, the study considered anxiety related to disclosing information as an alternative measure to willingness to disclose. Hypothesis 6 stated that Estonians would demonstrate more confidence and exhibit less anxiety about disclosing information online than Americans. H6 was not supported because there was no significant difference between the groups.

Anxiety over disclosing personally identifying information (PII) was measured using a self-developed scale. The 7-item index was subjected to factor analysis, which revealed two underlying dimensions where all but two of the items loaded on a single factor (Eigenvalue=4.077, accounting for 58% of the variance). Two of the items (related to stress and intimidation) loaded into a second separate factor (Eigenvalue=1.077, representing 15% of the variance). When all seven items were tested for reliability, however, the resulting Cronbach α=.88 was virtually identical to the results for the 5-item version (α=.87). Absent a clear rationale for eliminating the two items from the scale, all seven items were retained to measure anxiety.

As displayed in Table 4.16, on average, Estonians (M=3.54, SD=1.19) and Americans (M=3.44, SD=1.29, were no difference in their levels of reported anxiety (difference=.10, t=.815, df=464, p≤.415).

Table 4.16
Anxiety Over Disclosing Personally Identifying Information Online

(1=strongly disagree, 4=neutral, 7=strongly agree)

	United States		Estonia					
Measure	M	SD	M	SD	df	t	p	Cohen's d
Anxiety disclosing PII index	3.44	1.29	3.54	1.19	464	-.815	.415	.08
I felt uncomfortable providing the information.	3.34	---	3.55	---	---	---	.143	---
It wasn't stressful at all. (R)	3.18	---	3.29	---	---	---	.455	---
I didn't feel intimidated. (R)	2.84	---	3.19	---	---	---	.014	---
I was uncertain about providing information.	3.49	---	3.47	---	---	---	.888	---
I was anxious about being asked for my information.	3.30	---	3.43	---	---	---	.378	---
I would have preferred not to provide all the information.	4.41	---	4.03	---	---	---	.019	---
I was relaxed without any worries. (R)	3.61	---	3.87	---	---	---	.085	---

To test if a statistically significant relationship was present between anxiety related to disclosing PII items, and other key variables, a series of correlations were computed. As expected, an individual's anxiety over disclosing PII was negatively related to willingness to disclose overall (r=-.324, p=.000) -- a relationship found in both countries (US r=-.228, Estonia r=.431, both p=.000). Anxiety was negatively correlated with attitude toward disclosure overall (overall r=-.460, Estonia r=-.499, US r=-.472, all p=.000). Anxiety was negatively, but only marginally related to risk taking as a personality trait overall (r=-.087, p≤.060). A country-level analysis confirmed the correlation was not significant for the US (r=-.058, p≤.373), but anxiety and risk-taking as a personality trait were negatively related among Estonians (r=-.166, p≤.014).

Table 4.17 summarizes the correlations between anxiety disclosing PII items and the 8 variables with significant correlations overall.

Table 4.17
Correlations of Anxiety with Key variables: US vs. Estonia.

Variable	Overall	US	Estonia
Opportunity benefits	-.310***	-.237***	-.408***
Bargain Likelihood	-.145**	-.072	-.206**
Privacy Benefits Expected	-.232***	-.292***	-.169**
Purchase Benefits	-.279***	-.294***	-.258***
Trust in the Internet	-.303***	-.364***	-.266***
Trust in Institutions	-.216***	-.238***	-.211**
Neuroticism	.171***	.211***	.103
Agreeableness	-.158***	-.216*	-.070

*p≤ .05; **p≤.01; ***p≤ .001

Exploring the overall correlation scores for the entire sample, trust in the Internet (r=-.303, p≤.001) and opportunity benefits (r=-.310, p≤.001) both demonstrated a relationship with anxiety disclosing PII. While the relationships between anxiety and the aforementioned variables were significant (p≤.001), the strength of the relationship is only "medium or typical" (Gliner, Morgan, & Leech, 2009, p. 252). As would be expected, except for neuroticism, the relationships are negative – anxiety is less as the other variables increase.

Further correlations were run between anxiety over disclosing PII and the other variables thought to be potential predictors of anxiety. Three personality variables were non-significant overall: extraversion (r= -.059, p≤.207), openness (r=-.004, p≤.93) and conscientiousness (r=-.067, p≤.150). However, 8 variables were found to be significantly correlated to anxiety across the sample or on a national basis. These included opportunity benefits, bargain likelihood, purchase benefits, privacy benefits expected, trust in the Internet, trust in institutions, and the personality traits of neuroticism and agreeableness. Opportunity benefits was negatively correlated with anxiety disclosing in the overall sample (r= -.310, p≤.001), and in the US (r= -.237, p≤.001) and Estonia (r= -.408, p≤.001). Bargain likelihood was significant, and negatively correlated to anxiety overall (r= -.145, p≤.01) and in Estonia (r= -.206, p≤.01).

Privacy benefits expected were negatively correlated with anxiety disclosing at a significant level for the overall sample (r= -.232, p≤.001), the US (r= -.292, p≤.001), and Estonia (r= -.169, p≤.001). Purchase benefits, trust in Internet, and trust in public institutions were each negatively correlated with anxiety at a significant level for the overall sample, and for both the US and Estonia.

Table 4.17 shows the correlations when run separately by nation. Of the eight variables found to be significant in relationship for the overall sample, one was not significant for the US (bargain likelihood r=-.303, n.s.) and surprisingly, the two personality traits of neuroticism (r=.103, n.s.) and agreeableness (r=-.070, n.s.) were not significant in Estonia. The largest significant correlation in the US related to anxiety was trust in the Internet (r=-.364, p≤.001), while opportunity benefits (r=-.408, p≤.001) was the largest significant correlation in Estonia. The significant positive relationship found was between anxiety and neuroticism, present in the US (r=.211, p≤.001), however it was not significant in Estonia (r=.103, n.s.).

Table 4.18 reports the hierarchical multiple regression analysis conducted to investigate the predictability of anxiety disclosing PII items based on ten variables, including demographics, the variables measuring potential ecommerce benefits, the personality trait of neuroticism, and the two trust scales (trust in the Internet, trust in institutions). As with the previous hypotheses, in Step 1, nationality (β =.044, n.s.) was entered as the predictor variable but , as expected from the t-test, Step 1 was not significant. In Step 2, gender (β =-.114, p≤.01) and age (β =.1137 p≤.01) were both significant predictors of anxiety disclosing PII items, Step 2 accounted for 3.1% of the variance (R^2=.031, p≤.01). The addition of ecommerce experience in Step 3 increased the variance accounted for by 1.5% ($R^2 \Delta$=.015, p≤.01), but gender (β =-.109, p≤.01), age (β =.112,

p≤.01), and ecommerce experience (β =-.145, p≤.01) were all significant predictors of anxiety disclosing.

The final model, Step 4, introduced six additional variables into the regression model, including three potential ecommerce benefit variables (the variable bargain likelihood was omitted after being found nonsignificant in prior regression), the personality trait of neuroticism, and the two trust scales (trust in the Internet, trust in institutions). The additional variables explained an additional 18% of the variance (p≤.001), and the 10 variables utilized in Step 4 together accounted for 22.7% of the total variance for the model (R^2=.227, p≤.001). Seven of the ten variables significantly predicted anxiety disclosing PII items: nationality (β=-.136, p≤.01), gender (β=-.127, p≤.01), age (β=.153, p≤.001), trust in the Internet (β=-.157, p≤.01), trust in institutions (β=-.101, p≤.01), the personality trait of neuroticism (β=.147, p≤.001), and opportunity benefits (β=-.188, p≤.001). The variable of opportunity benefits was the strongest predictor of anxiety disclosing (β=-.188), and trust in the Internet the second strongest predictor of anxiety disclosing.

When regressions were conducted to investigate predictors of anxiety separately in the US and Estonia using the same 9 variables (other than nationality), the resulting models were each statistically significant (both p≤.001) but differed in terms of the significant variables and the amount of variance explained (21% for the US and 30% for Estonia). For the US, trust in the Internet (β=-.225, p≤.01) and the personality trait of neuroticism (β=.183, p≤.01) were the two significant predictors, while gender (β=-.178, p≤.01), age (β=.155, p≤.01), and opportunity benefits (β=-.278, p≤.001) were the significant predictors of anxiety disclosing PII for Estonian participants. All others became nonsignificant.

Table 4.18
Hierarchical Multiple Regression Model for Anxiety Disclosing PII items

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.002	.002
Nationality	.100	.120	.044		
Step 2:				.031**	.029**
Nationality	.109	.120	.043		
Gender	-.289	.121	-.114**		
Age	.344	.119	.137**		
Step 3:				.047***	.015**
Nationality	-.066	.136	-.026		
Gender	-.277	.120	-.109**		
Age	.282	.121	.112**		
Ecommerce experience	-.133	.050	-.145**		
Step 4:				.227***	.180***
Nationality	-.343	.143	-.136**		
Gender	-.322	.111	-.127**		
Age	.385	.113	.153***		
Ecommerce experience	-.003	.049	-.003		
Trust in the Internet	-.175	.060	-.157**		
Trust in Institutions	-.126	.058	-.101**		
Neuroticism	.134	.041	.147***		
Opportunity benefits	-.222	.061	-.188***		
Purchase benefits	-.096	.055	-.111		
Privacy benefits expected	-.056	.057	-.068		

*p≤ .05; **p≤.01; ***p≤ .001

PERCEIVED RISK OF DISCLOSING PII ITEMS

Perceived risk of disclosing personally identifying information was the second major focus of this study and provided the basis for the concluding hypothesis. The results were analyzed using the 17-item list of specific PII items for which participants were asked to indicate their perceived risk (parallel items to those used to assess their willingness to disclose). Each of the 17 items were assessed on a 7-point scale, where not risky to disclose=7 (positive valence) and very risky to disclose=1 (negative valence).

Hypothesis 7: Perceived Risk of Disclosing PII items

Hypothesis 7 stated Estonians would have lower perception of risks related to disclosing of specific PII items than Americans. This hypothesis was not supported, as overall, *Americans* were found to have lower perceptions of risk based on the 17 PII items.

As described in H1, and Table 4.2 and Table 4.3 presented previously, the 17 items for this measure were treated as a single index and factor analyzed, resulting in 6 sub-indexes. The overall index measuring perceived risk of disclosing index was reliable (Cronbach α=.90), as were each of the sub-indices.

As presented in Table 4.19 (repeated from Table 4.3), Americans (M=3.71, SD=1.01) perceived significantly less risk in disclosing all the 17 PII items than Estonians (M=3.31, SD=1.12, t=4.01, df=447, p=.000). The difference between Americans and Estonians for the overall 17-item index can be attributed to significant differences in perceived risk for four of the sub-indices, presented from largest to smallest in terms of differences between the two countries: payment information (US M=3.21, Estonia M=2.31, difference=.907, t=6.43, df=466, p=.000), online account information (US M=3.64, Estonia M=3.05, difference=.588, t=3.92, df=467, p=.000), disclosing contact information (US M=4.43, Estonia M=3.97, difference=.458, t=3.51, df=466, p=.000), and financial/medical history information (US M=2.91, Estonia M=2.61, difference=.308, t=2.29, df=468, p$\leq$.023). Differences in perceived risk of disclosing work related information (US M=3.42, Estonia M=3.14, t=1.81, df=469, p=n.s.) and life history information (US M=4.30, Estonia M=4.09, t=1.44, df=464, p=n.s.) were not statistically significant.

Table 4.19

Perceived Risk of Disclosing PII Items

(*1=very risky, 4=neutral, 7=not risky)*

	Overall		US		Estonia					
Measure	*M*	*SD*	*M*	*SD*	*M*	*SD*	*df*	*t*	*p*	*Cohen's d*
Perceived risk of disclosing index	**3.52**	**1.08**	**3.71**	**1.01**	**3.31**	**1.12**	**447**	**4.01**	**.000**	**.38**
Contact information index	**4.21**	**1.42**	**4.43**	**1.38**	**3.97**	**1.45**	**466**	**3.51**	**.000**	**.32**
Name	4.62	---	4.81	---	4.41	---	---	---	.007	---
Home Address	3.80	---	4.16	---	3.40	---	---	---	.000	---
Home Phone	3.84	---	3.95	---	3.71	---	---	---	.123	---
Email	4.61	---	4.80	---	4.40	---	---	---	.011	---
Online account information index	**3.36**	**1.64**	**3.64**	**1.66**	**3.05**	**1.57**	**467**	**3.92**	**.000**	**.37**
Twitter handle	3.44	---	3.80	---	3.04	---	---	---	.000	---
Facebook account	3.29	---	3.52	---	3.04	---	---	---	.002	---
Skype username	3.34	---	3.57	---	3.07	---	---	---	.001	---
Life history information index	**4.20**	**1.59**	**4.30**	**1.52**	**4.09**	**1.69**	**464**	**1.44**	**.151**	**.13**
Date of birth	3.84	---	3.64	---	4.06	---	---	---	.015	---
Marital status	4.21	---	4.61	---	3.76	---	---	---	.000	---
Age	4.56	---	4.69	---	4.41	---	---	---	.089	---
Financial/Medical history index	**2.77**	**1.46**	**2.91**	**1.44**	**2.61**	**1.47**	**468**	**2.29**	**.023**	**.21**
Income	3.09	---	3.53	---	2.60	---	---	---	.000	---
Credit history	2.58	---	2.61	---	2.55	---	---	---	.682	---
Medical history	2.65	---	2.62	---	2.68	---	---	---	.711	---
Work-related information index	**3.29**	**1.72**	**3.42**	**1.79**	**3.14**	**1.62**	**469**	**1.81**	**.072**	**.16**
Work address	3.27	---	3.42	---	3.09	---	---	---	.041	---
Work phone	3.30	---	3.42	---	3.18	---	---	---	.148	---
Payment information index	**2.79**	**1.58**	**3.21**	**1.65**	**2.31**	**1.37**	**463**	**6.43**	**.000**	**.59**
Credit card number	2.46	---	2.87	---	2.00	---	---	---	.000	---
PayPal account	3.11	---	3.56	---	2.60	---	---	---	.000	---

To understand the nature of the risk perceived by participants in the study, correlations were computed between perceived risk of disclosing PII items and other key variables for all participants, and then separately for both the US and Estonia (Table 4.20).

Table 4.20
Correlation of Perceived Risk with Key Variables: US vs. Estonia.

Variable	Overall	US	Estonia
Opportunity benefits	.253***	.215***	.193**
Bargain Likelihood	.116*	.027	.088
Privacy Benefits Expected	.353***	.233***	.397***
Purchase Benefits	.361***	.295***	.406***
Trust in the Internet	.295***	.266***	.227***
Trust in Institutions	.108*	.098	.181**
Neuroticism	-.123**	-.057	-.152*

*p≤ .05; **p≤.01; ***p≤ .001

For the overall sample, significant correlations were found between perceived risk of disclosing PII items overall and opportunity benefits (r=.253, p≤.001), bargain likelihood (r=.116, p≤.05), privacy benefits expected (r=.353 ,p≤.001), purchase benefits (r=.361,p≤.001), trust in the Internet (r=.295, p≤.001), trust in institutions (r=.108, p≤.05), and neuroticism (r=-.123, p≤.01). All of the significant relationships found in the overall sample were positive in direction (except for neuroticism). Based on the direction of the response for perceived risk, where 7=not risky and 1=very risky, the lower the perceived risk, the greater the perceived opportunity benefits. Additionally, the greater the bargain likelihood, privacy benefits expected, purchase benefits, trust in the Internet, or trust in institutions, all result in a lower perceived risk of disclosing.

The separate correlations for the US and Estonian found that four variables were significant in the US, and six in Estonia. For Americans, there is a significant relationship between perceived risk of disclosing and opportunity benefits (r=.215, p≤.001), privacy benefits

expected (r=.233, p≤.001), purchase benefits (r=.295, p≤.001), and trust in the Internet (r=.266, p≤.001). In Estonia, only bargain likelihood (r=.088, n.s.) was found not to be significantly related to perceived risk of disclosing.

Based on these correlations, a hierarchical regression analysis was performed to investigate how well these key variables predict perceived risk of disclosing. In Step 1, nationality was entered as the predictor variable, and it significantly predicted lower perceived risk of disclosing in the US (β = -.178, p≤ .001, R^2 = .032, p≤.001). In Step 2, the addition of education, gender, and age were nonsignificant. Ecommerce experience was added in Step 3, explaining an additional 1% (p≤.05) of the variance, although the model was significant (R^2=.045, p≤.01). Of the five variables in Step 3, only nationality (β = -.134, p≤ .01) and ecommerce experience (β = .114, p≤ .01) were significant predictors of perceived risk. In the final step, the addition of the two trust scales, the four ecommerce benefits, and neuroticism explained an additional 14% of the variance (R^2 change=.142, p≤.001), for a total of 18.7% of the variance (R^2=.187). Although the model was significant (p≤.001), only purchase benefits (β =.228, p≤ .001) was found to be a significant predictor of perceived risk of disclosing.

Regressions in which effects were analyzed separately for each nation found that none of the variables was significant in predicting perceived risk among Americans, but that purchase benefits was significant among Estonians only (β =.228, p≤ .001).

Table 4.21
Hierarchical Multiple Regression Model for Perceived Risk of Disclosing 17 PII items

Step and predictor variable	*B*	*SE B*	ß	R^2	ΔR^2
Step 1:				.032***	.032***
Nationality	-.380	.103	-.178***		
Step 2:				.035**	.004
Nationality	-.398	.105	-.187***		
Education	-.126	.105	-.059		
Gender	-.020	.104	-.009		
Age	-.021	.103	-.010		
Step 3:				.045**	.010*
Nationality	-.285	.119	-.134**		
Education	-.126	.104	-.059		
Gender	-.026	.104	-.012		
Age	.022	.105	.010		
Ecommerce experience	.085	.042	.114*		
Step 4:				.187***	.142***
Nationality	-.101	.130	-.047		
Education	-.123	.098	-.058		
Gender	-.052	.098	-.024		
Age	-.036	101	-.017		
Ecommerce Experience	.004	.043	.006		
Trust in the Internet	.095	.055	.100		
Trust in Institutions	.007	.053	.006		
Opportunity benefits	.106	.059	.106		
Bargain Likelihood	-.021	.050	-.022		
Privacy Benefits Expected	.069	.050	.098		
Purchase Benefits	.166	.049	.228***		
Neuroticism	-.049	.037	-.063		

*p≤ .05; **p≤.01; ***p≤ .001

CHAPTER 5:

DISCUSSION

The concluding chapter of this dissertation contains six sections: (a) hypotheses summary, (b) review of variables, (c) a further examination of willingness to disclose versus perceived risk, (d) implications for theory and practice, (e) limitations and future research, and (f) conclusion. Overall, significant differences were found between participants from the United States and Estonia concerning their willingness to disclose and the perceived risks associated with disclosing, within 17 items of PII and in other variables. Bolstering the findings of previous studies, this study showed that, regardless of the maturity or scope of the ecommerce market, individuals of different nationalities are willing to disclose information in exchange for certain shopping benefits. This study found that trust is especially important when shopping online, particularly when disclosing personal information.

HYPOTHESES SUMMARY

Table 5.1 summarizes the research findings on the seven hypotheses examined in this study. Overall, three of the hypotheses were supported or partially supported by the research, while four were rejected.

Table 5.1
Summary of Hypotheses Results

Hypothesis	Result of Statistical Analysis	Findings
H1: Estonians will be more willing than Americans to disclose specific PII items	Rejected based on t-test	*Americans* (M=3.70, SD=.905) are more willing to disclose 17 items of PII than Estonians (M=3.37, SD=1.11; t=3.45, df=448, p≤.002). Ecommerce experience (ß =.21, p≤.001), and education (ß =.094, p≤.001) were significant predictors of willingness to disclose.

H2: Estonians will be less likely to disclose PII items based on perceived benefits received in exchange for providing information compared to Americans	Supported based on regression	*Americans* (M=4.38, SD=1.42) were significantly more willing than Estonians (M=4.08, SD=1.52) to exchange PII for purchases benefits (t=2.24, df=468, p≤.026). Americans (M=5.41, SD=1.41) were significantly more willing than Estonians (M=4.23, SD=1.38) to exchange PII for guarantees of privacy protections while shopping (t=9.10, df=466, p=.000). Ecommerce benefits predicting willingness to disclose included opportunity benefits (β=.111, p≤.01) and purchase benefits (β=.352, p≤.001).
H3: Willingness to disclose will be positively related to a) extraversion, b) openness, c) conscientiousness, and d) agreeableness and e) and negatively related to neuroticism	Partial support based on correlation and regression	Willingness to disclose was positively related to two personality traits: openness (r=.109, p≤.022), and agreeableness (r=.149, p≤.002) and negatively related to neuroticism (r=.115, p≤.015). Significant correlations were not found between willingness to disclose and extraversion (r=.013, p≤.077, n.s.) nor conscientiousness (r=.087, p≤.067, n.s.).
H4: Willingness to disclose based on the 17-item index will be positively related to a) trust in the Internet and b) being a trusting person more generally, as evidenced in trust in institutions	Supported based on correlations	Willingness to disclose was positively related to both trust in the Internet (r=.336, p=.000), and trust in institutions (r=.201, p=.000). Regression found four items as statistically significant predictors of willingness to disclose: education (β=-.099, p≤.05), ecommerce experience (β=.136, p≤.01), trust in the Internet (β=.235, p≤.001), and trust in institutions (β=.177, p≤.001).
H5: Estonians will demonstrate a more positive attitude toward disclosing online in general than Americans.	Rejected based on t-test	*Americans* (M=4.38, SD=.947) were significantly more positive in their attitude toward disclosing PII online in general than Estonians (M=3.55, SD=1.00, t=9.25, df=467, p=.000). Nationality (β=-.260, p≤.001) had a significant effect on attitude toward disclosing online in general and those more experienced in ecommerce (β=.246, p≤.001) have a more positive attitude

		toward disclosing online.
H6: Estonians will exhibit less anxiety about disclosing information online than Americans.	Rejected based on t-test	No significant difference was found between the groups based on mean scores. Regression found predictors of anxiety disclosing include nationality (β=-.136, p≤.01), gender (β=-.127, p≤.01), age (β=.153, p≤.001), trust in the Internet (β=-.157, p≤.01), trust in institutions (β=-.101, p≤.01), the personality trait of neuroticism (β=.147, p≤.001), and opportunity benefits (β=-.188, p≤.001).
H7: Estonians will have lower perception of risks related to disclosing of specific PII items than Americans	Rejected based on t-test	*Americans* (M=3.71, SD=1.01) perceived significantly less risk in disclosing the 17 PII items than Estonians (M=3.31, SD=1.12, t=4.01, df=447, p=.000). Potential benefits pertaining to the purchase (β =.228, p≤ .001) were found to be a significant predictor of perceived risk of disclosing.

REVIEW OF STUDY VARIABLES

This study explored relationships between several important variables, and their effect on willingness to disclose and perceived risk of disclosing personal data. Among these variables were nationality, demographic variables (including ecommerce experience), perceived ecommerce benefits, personality traits, and trust (in the Internet, and in institutions). Additionally, attitude toward disclosure and anxiety disclosing served as alternative measures for measuring the dependent variables of disclosure during ecommerce transactions.

Nationality

Notably, the direction for all of the country-based hypotheses that were statistically significant were in the *opposite* direction of predictions. Although Estonians are ranked as a nation high in technological sophistication, the effect of the being more advance technologically

did not have the expected effect on willingness to disclose and perception of risk. Key factors, other than technological proficiency, seem to influence these differences. Despite its advancements, it appears that Estonia is not as developed as the US, at least in terms of participants' experience with ecommerce (the focus of the study) versus the use of the Internet more generally. However, an alternative explanation is that the Estonian sample might be more representative of that country's population, while than the Mturk panel as skewed in favor highly sophisticated ecommerce use versus the US population as a whole. Further, because Estonia is more technologically advanced, and knowledge about the regulation of its data practices is pervasive, citizens' awareness may be raised by government and other organizations, which may in turn stimulates Estonians' awareness and sensitivity to privacy concerns.

Importantly, education and ecommerce experience interacted with nationality to reveal important differences between the two samples when separate regression analyses were performed. The results showed that the American participants without a college degree were more willing to disclose, while Estonians with more ecommerce experience were more willing to disclose. The effect of age is important variable to consider as well. For Estonians, the younger the individual, the more positive their attitude toward disclosing. Younger individuals, or sometimes referred to "digital natives" (Prensky, 2001), have grown-up with technology infiltrating almost every conceivable aspect of their lives. As a result, younger individuals are thought to be more comfortable with technology (Windham, 2005). By being able to share information about themselves through a multitude of digital channels (i.e., Twitter, Facebook, Instagram, Snapchat, text messages, email), younger people might be more willing to disclose personal data, and have more positive attitudes providing their personal information.

Ecommerce Experience

Ecommerce experience was found to be an important predictor of willingness to disclose and perceived risk of disclosure. Those with more self-reported experience shopping online were found to be more willing to disclose, and perceived less risk in disclosing. Further, those higher in ecommerce experience held more positive attitude toward disclosing online. These findings support the idea posited by the author that ecommerce experience works in a similar fashion to Internet proficiency in general: the higher Internet proficiency, the more likely the individual is to shop online (Corbitt et al., 2003). This increased Internet proficiency then leads the individual to less likely be concerned with associated risks (Dutton & Shepherd, 2006). This same relationship between general Internet proficiency and willingness to disclose and perceived risk is apparent in ecommerce experience: the more a person shops online, that individual becomes more familiar with and accustomed to providing information to complete a transaction. They therefore become more willing to disclose information, and through constant disclosing of information, perceive less risk involved with disclosing.

Perceived Purchase Benefits

Of the four perceived purchase benefits, H2 found both opportunity benefits and purchase benefits to be positive predictors of willingness to disclose. The findings suggest that, to persuade consumers to disclose information, it is important for online shopping either to be characterized as an important opportunity or providing purchase benefits (i.e., greater merchandise selection, better customer service, tailored product offerings, special discounts). These findings support existing research, which has found both that individuals will disclose information when given a reason why to do so, such as in exchange for incentives (Milne & Gordon, 1993). For Americans, purchase benefits are significant positive predictors of

willingness to disclose, while perceived ecommerce benefits were not significant predictors of willingness to disclose for Estonians.

Perceived risk of disclosing and its relationship to perceived benefits were explored, and potential benefits pertaining to the purchase were found to significantly lower perceived risk of disclosing. The data suggest that when increased shopping values (such as purchase benefits) are present, those in the overall sample have lower perceived risk of disclosing. Based on these findings, people might be lured by purchase benefits, and therefore may ignore or subjugate concerns about risks. These findings are consistent with the literature, which found when consumers perceive disclosure benefits as exceeding the risks associated with disclosure, individuals are more likely to disclose personal information (Milne & Culnan, 2004).

Personality

Three personality traits (openness, agreeableness, and neuroticism) were found to be correlated with willingness to disclose, but openness and neuroticism were not significant in the regression analyses. In the hierarchical multiple regression analysis, the combination of ecommerce experience (β=.163, $p \leq .01$) and agreeableness (β=.154, $p \leq .01$) were statistically significant predictors of willingness to disclose. Based on the direction of the relationship, the more agreeableness a person demonstrates, the more willing the person is willing to disclose personal data. This suggests individuals who are agreeable may disclose more to seem personable and friendly or are more compliant to requests. While contradictions abound in the literature regarding the relationship between disclosure and openness (Loiacono, et al., 2012), this study found some evidence about the effect of openness but agreeableness might be a more important personality trait. As noted in the literature review, Wheeless (1976) labeled openness as disclosiveness, and Taddicken (2014) established that those higher in disclosiveness (or

openness) are more likely to disclose online compared to individuals low in disclosiveness. Previous research has demonstrated the negative relationship between neuroticism and willingness to disclose (Loiacono et al., 2012) – a finding corroborated in this study.

Trust – In the Internet and Institutions

Trust was measured as both trust in the Internet and trust in institutions. Both were found to be statistically significant predictors of willingness to disclose. The study's findings suggest that trust is a possible important factor in willingness to disclose, which supports literature that found a reciprocal relationship between trust and willingness to disclose (Henderson & Gilding, 2004; McKnight, Choudhury, & Kacmar, 2002). Research has demonstrated that those more inclined to trust in general are more inclined to trust the Internet (Rose, 2003). This view of trust would seem logical, since trust has been identified as a major determinant in individuals' completion of purchases (Pavlou & Chellappa, 2001), whether online or offline. Additionally, this study found trust in the Internet was negatively associated with perceived risk; higher trust in the Internet resulted in lower perceptions of disclosure risk. These findings support research demonstrating higher trust results in lower perceived risk (Pavlou, 2003; Salam et al., 2003).

Interesting, trust acts differently in the US and Estonia. While Americans demonstrated higher trust in the Internet, Estonians were shown to have higher trust in institutions. While technology is indeed a major component of Estonians' everyday lives, based on the sample, American participants exhibited more trust in the Internet. Where Estonians, based on their high technological adoption and high uses of digital infrastructure, were posited to hold high trust levels, surprisingly the results were the opposite. The lower level of trust in the Internet demonstrated by the Estonians may be explained historically or culturally as a result of previous Soviet occupations of the nation where citizens were subjected to extensive government

wiretapping and surveillance. It is possible that these negative feelings related to technology are still present.

The author was somewhat surprised by the lower levels of trust in the Internet demonstrated by the Estonians: trust has become vital in the acceptance of Internet-based services in the country, which allows for e-voting, e-banking, etc. The open communication between Estonia's government and citizens during the 2007 cyber-attacks that rocked the country led to an increase in citizen trust in government, opening the door to development of the country's expansive e-service industry (E-estonia.com, 2013). This Estonian e-services industry is built around a data exchange layer called the "X-Road," created in 2001, which facilitates data exchange among different secure databases and "enables secure Internet-based data exchange between the state's information systems" (Estonian Information System's Authority, 2013). Although it was expected that Estonians would place greater trust in the Internet than Americans, the study's results do not support this.

Regarding trust in institutions, it should be no surprise that Americans hold a low level of trust in institutions. With the U.S. Congress' approval ratings at all-time lows (Jones, 2014), this clearly affects the level of trust in national government among participants in the American sample. Similarly, many Americans are uncomfortable with "Big Business" and question corporations' obsession with profit and lack of corporate social responsibility (Steinhauser, 2014). Estonians, on the other hand, have higher trust in institutions. Estonia is continually ranked as one of the most democratic countries in the world, and one of the "free" journalistic nations; both may serve as indicators for why Estonians demonstrate more trust in institutions. Further work would be beneficial to differentiate how trust in government versus in trust business impacts ecommerce, since both types of institutions are encouraging customers and

citizens to conduct routine transactions online. Additionally, it would be useful in future studies to include *trust propensity*, or "a dispositional willingness to rely on others," (Colquitt, Scott, & LePine, 2007, p. 909) as another potentially valuable measure of trust. Further, Mayer, Davis, and Schoorman's (1995) integrated model of organizational trust, which encompasses benevolence, integrity, and ability as antecedents to trust, is another worthwhile trust measure for future research.

Attitude toward disclosing

In addition to measuring willingness to disclose 17 items of PII, attitude toward disclosure served as an alternative measure for measuring the dependent variables of disclosure during ecommerce transactions. From the study's results, nationality does have a significant effect on attitude toward disclosing online in general, at least nominally, and those more experienced in ecommerce have more positive attitude toward disclosing online. Participants in the American sample showed more positive attitude toward disclosing online than Estonians. Attitude toward disclosing were positively related to willingness disclose, which seems logical: individuals who perceive online disclosure as positive should be more willing to disclose.

Anxiety toward disclosing

As an alternative measure for willingness to disclose, the study also measured individual's anxiety related to disclosing information. For Americans, higher trust in the Internet and lower anxiety are associated, and neurotic individuals tend to be anxious. Younger Estonians will have less anxiety disclosing, and those perceiving a lack of clear opportunity benefits in ecommerce demonstrate higher anxiety. Additionally, the results found that seven variables were found to predict anxiety toward disclosing PII items: nationality, gender, age, both trust variables (trust in the Internet and trust in institutions), the personality trait of neuroticism, and opportunity

benefits. These results suggest that individuals who perceive shopping online as presenting positive shopping opportunities report less disclosure-related anxiety, and those with more trust in the Internet will have lower anxiety disclosing online. Additionally, those who have more trust in institutions will have lower anxiety levels in disclosing. Higher levels of trust have been previously explored in the literature, showing that higher levels of perceived risk, and in turn higher anxiety, lead to lower trust (Corbitt et al., 2003).

FURTHER EXAMINATION OF WILLINGNESS TO DISCLOSE VERSUS PERCEIVED RISK

The Relationship Between Willingness To Disclose And Perceived Risk

For this study, two major concepts were of particular interest: willingness to disclose personal information and perceived risk of disclosing the information. Willingness to disclose was operationalized as an individual's openness to the idea of providing specific items of personal information in the context of ecommerce transactions, and perceived risk of disclosing the information was measured as the level of concern or perceived potential for hazard or loss involved in disclosing the same information. These two variables, crucial for understanding disclosure in ecommerce transactions, were examined using the same 17-item scale of personal data items.

An important goal of this study has been to compare these two variables to determine how they are related. As a review, Table 5.2 provides a consolidated summary comparison of the main index scores and of the six PII underlying sub-indices for the two measures, which were previously reported in detail in Table 4.3. Table 5.2 lists them from most willing to disclose to least willing to disclose, and from least risky to most risky, respectively. In general, the comparisons reveal a similar pattern: contact information was the category of information

participants were most willing to disclose, with the least perceived risk. Financial/Medical history was the category people were least willing to disclose and was perceived as the most risky. Notably, although payment information was the second most willing-to-disclose category, it rated next to the bottom in terms of riskiness.

Where significant differences were detected between the two countries, people in the United States were generally more willing to disclose than Estonians, and perceived less disclosure risk. Estonians were less willing than Americans to disclose contact information (US M=5.38, Estonia M=4.90), and especially payment information (US M=4.60, Estonia M=2.84). Estonians also perceived the four categories of PII as more risky to disclose compared with Americans: Estonians were less willing to disclose contact information (Estonian M=3.97, US M=4.43), online account information (Estonia M=3.03, US M=3.64), payment information (Estonia M=2.31, US M=3.21) and financial/medical history (Estonia M=2.61, US M=2.91).

To analyze the relationship between the two constructs of willingness to disclose and perceived risk of disclosing, it was believed potentially useful to compare the scores for each individual. Conceptually, for each individual there is a *gap* between willingness to disclose and perceived risk for each of the underlying items for the overall index score and for each of the sub-index scores. This gap can be operationalized as the arithmetic difference between the two scores and computed by subtracting perceived riskiness from willingness to disclose. The result can be either positive (willingness to disclose exceeds the perceived risk) or negative (willingness to disclose is less than perceived risk). The result is a series of gap scores for each individual and in turn, those gap scores can be compared for Americans versus Estonians.

Table 5.2
Summary Comparison of Willingness to Disclose and Perceived Riskiness of Disclosure for Six PII Categories

	Willingness to disclose (WD) (*1=not willing, 4=neutral, 7=very willing)* Perceived risk of disclosing (PR) (*1=very risky, 4=neutral, 7=not risky)*					
Measure	Overall	US	Estonia	Difference	*t*	*p*
Willingness to disclose indices						
Index (17 items)	**3.55**	**3.70**	**3.37**	**.327**	**3.45**	**.001**
Contact Information	5.15	5.38	4.90	.486	3.81	.000
Payment information	3.77	4.60	2.84	1.76	11.75	.000
Life History	4.16	4.12	4.20	-.081	-.510	n.s.
Work-Related	2.98	2.96	3.00	-.034	-.205	n.s.
Online Account Information	2.53	2.59	2.46	.131	.833	n.s
Financial/Medical History	2.10	2.08	2.13	-.052	-.436	n.s
Perceived risk of disclosing indices						
Index (17 items)	**3.52**	**3.71**	**3.31**	**.403**	**4.01**	**.000**
Contact Information	4.21	4.45	3.97	.458	3.51	.000
Life History	4.20	4.30	4.09	.212	1.44	n.s.
Online Account Information	3.36	3.64	3.03	.588	3.92	.000
Work-Related	3.29	3.42	3.14	.285	1.81	n.s.
Payment Information	2.79	3.21	2.31	.907	6.43	.000
Financial/Medical History	2.77	2.97	2.61	.308	2.29	.023

Table 5.3 compares the willingness to disclose and perceived risk scores for the various index scores, but arranges the means presented in Table 5.2 by country, and then shows the computed difference between them, labeled as a *gap score*. Not surprisingly, the differences between willingness to disclose and perceived risk was not significant for either Americans or Estonians when only the 17-item index scores are considered. This might be expected as an artifact of averaging a large number of widely varying scores. In the US, willingness to disclose and perceived risk for the 17 items were virtually identical (willingness M=3.70, perceived risk M=3.71, difference=-.02, t=-.393, p≤.694). In Estonia, the gap was also slight (willingness M=3.37, perceived risk M=3.31, difference=.07, t=1.52, p≤.130). Importantly, however, statistical significant and potentially important differences were found for the specific types of information represented in the sub-indices.

Table 5.3
Gap Between Willingness to Disclose and Perceived Riskiness of Disclosure for Six PII Categories, By Country

	Willingness to disclose (WD) (*1=not willing, 4=neutral, 7=very willing)* Perceived risk of disclosing (PR) (*1=very risky, 4=neutral, 7=not risky)*				
Country and Index	WD	PR	Difference (Gap score)	*t*	*p*
United States					
Index (17 items)	3.70	3.71	-.020	-.393	.694
Contact Information	5.38	4.44	.931	11.22	.000
Payment Information	4.60	3.21	1.39	12.47	.000
Life History Information	4.12	4.30	-.179	-.180	.074
Work-Related Information	2.96	3.42	-.459	-4.21	.000
Online Account Information	2.60	3.63	-1.03	-9.25	.000
Financial/Medical History Info	2.08	2.90	-.841	-8.76	.000
Estonia					
Index (17 items)	3.37	3.31	.070	1.52	.130
Contact Information	4.90	3.93	.970	11.36	.000
Payment Information	2.84	2.30	.544	5.30	.000
Life History Information	4.21	4.10	.110	1.39	.167
Work-Related Information	3.00	3.14	-.145	-1.48	.140
Online Account Information	2.47	3.06	-.582	-6.47	.000
Financial/Medical History Info	2.13	2.60	-.468	-6.14	.000

The first subindex, contact information, included four items: name, home address, home phone, and email address. Participants from both countries rate willingness to disclose contact information higher (US M=5.38, Estonia M=4.90) than perceived risk (US M=4.44, Estonia M=3.93). The results were statistically significant for both countries (US difference =.931, t=11.22, p=.000, Estonia difference=.970, t=11.36, p=.000).

Payment information, the second sub-index, included credit card number and PayPal account, and followed the same pattern as the first sub-index: both Americans and Estonians reported higher willingness to disclose (US M=4.60, Estonia M=2.84) than perceived risk (US M=3.21, Estonia M=2.30), with results being statistically significant for each country (US difference=1.39, t=12.47, p=.000; Estonia difference=.544, t=5.30, p=.000).

For life history information (DOB, marital status, age), willingness to disclose (M=4.21) was higher than perceived risk (M=4.10) for Estonians, but not statistically significant (Estonia

difference=.110, t=1.39, p≤.167). The difference was not significant for Americans although the scores were reversed: Americans reported higher perceived risk (M=4.30) than willingness to disclose (M=4.12, difference=-.179, t=-.180 p≤.074).

Study participants from both countries reported work-related information as higher in perceived risk (US M=3.42, Estonia M=3.14) than willingness to disclose (US M=2.96, Estonia M=3.00). However the difference was only statistically significant in the US (US difference= -.459, t=-4.21, p=.000, Estonia difference=-.145, t=-1.48, p≤.140).

Online account information (Twitter, Facebook, and Skype accounts) was the fifth index examined between the US and Estonia for willingness to disclose and perceived risk. For both the US and Estonia, willingness to disclose was low and the perceived risk was higher. For the US participants: willingness to disclose M=2.60, perceived riskiness M=3.63, difference=1.03, t=-9.25, p=.000. For Estonians: willingness to disclose M=2.47, perceived riskiness M=3.06, difference=-.582, t=-6.47, p=.000. Overall, the US participants perceived disclosing online account information, such as Skype username, as less risky than Estonians, but the Estonians are more concerned about these information items (exhibiting a lower gap than in the US).

Financial/medical information included the items of income, credit history, and medical history. Both in the US and in Estonia these items were ranked higher in perceived risk (US M=2.90, Estonia M=2.60) than willingness to disclose (US M=2.06, Estonia M=2.13). For each country, the gap based on the difference in scores for willingness to disclose and perceived riskiness were statistically significant (US: difference=-841, t=-8.76, p=.000; Estonia: difference =-.468, t=-6.139, p=.000).

The results from the study perceive unique differences in how Estonians and Americans disclose information related to each of the sub-indices—findings that the researcher intends to examine more fully an a later secondary analysis.

Personal contact information: For both countries, information related to contacting an individual was rated highest in willingness to disclose. Name, home address, home phone number, and email are probably the most widely collected items of personal data in completing ecommerce purchases, so it would make sense that individuals are more conditioned to providing these items then other categories of personal data. Both countries showed a similar gap between willingness and perceived risk associated with contact information, so similarities are present in both countries related to disclosing of personal contact information.

Payment information: Similarities are present in the US and Estonia regarding disclosure of payment related information. While both countries rated payment information as more willing to disclose than perceived risk, both rated payment information risky to disclose. For Americans, payment information was the second most risky to disclose, while Estonians rated it the most risky. It seems that disclosing payment information is risky in both mature and burgeoning ecommerce nations, and marketers should rightfully ensure consumers of secure transactions.

Life history information: Of all the gap scores for either country, the difference of .110 between willingness and perceived risk in the Estonian score is the smallest of the calculated gap. Although they might be willing to disclose such items, Estonians might also struggle with balancing the potential risks of disclosing information associated with date of birth, marital status, and age.

Work-related information: Surprisingly, disclosure of work-related information (work address, work phone) is typically provided less willingly by the study participants than home-

contact information (home address, home phone). These responses suggest that consumers from both a mature (i.e., United States) and burgeoning ecommerce nation (i.e., Estonia) consider work-related personal data as sensitive information. Several explanations for this finding exist. Consumers are accustomed to providing home-contact information for online purchases, and typically have items shipped to home addresses rather than to work addresses, implying that, while online merchants can offer to ship products to work addresses, requiring consumers to disclose work-related information may jeopardize the sale, and/or alienate the consumer. Individuals may not want to ship items to their work address, especially sensitive items that may negatively impact others' perceptions. Others might be concerned about the prospect of third-party marketers or their affiliates contacting employers, or colleagues at work, or having messages intercepted at work, or being affiliated with activities that would be looked upon unfavorably by employers. Individuals from both countries may seek a work-life balance, and this includes separation of one's private home life from their work life.

Online account information: People in both countries perceive greater risk than willingness to disclose related to online account information, but are willing to disclose information. While individuals may be open to providing online account information, such as Facebook or Twitter profile, to friends or family, they may not be as willing to disclose the same information to businesses. Individuals typically use social networks for receiving and distributing personal information to family and friends, but not for receiving contacts from businesses or government. If businesses were to contact consumers through social networks, it may be seen as deluding trust, resulting in a negative perception of the business, and in effect, the consumer seeking to do business with another company. Notably, these findings provide clear and important implications for marketers in that they should carefully solicit consumer's online

account information, and that contacting consumers through these networks may alienate them and reduce trust in the marketer or merchant. It is recommended that if consumers are interested in interacting with marketers through their online accounts, the communication should be initiated by the consumer, and not by the marketer.

Financial/medical information: Importantly, while Estonian patients can access their digital health records from one file, the medical system in the US is a highly fragmented - medical providers and patients do not enjoy universal access. Income is a sensitive concept in the United States, and Americans are often hesitant to disclose their annual income. Medical history in Estonia is more readily disclosed, as Estonians are accustomed to the nation's system of digital healthcare file, while a higher percentage of the population banks online compared to Americans. People in both countries are increasingly wary about protecting their credit history, for fear of possible identity theft.

Conceptualizing the Willingness-Risk Gap: Online Disclosure Consciousness

A common thread seen throughout this study has been the prevalence of individuals who are willing to exchange personal data for purchase benefits (one of the four ecommerce benefits), or value propositions (i.e., greater merchandise selection, better customer service, tailored product offerings, special discounts) in exchange for providing some personal information. While shopping online, individuals must constantly navigate various "risk-sensitive activities" (Fife & Orjuela, 2012, p. 1), specifically as noted in the literature where the need or desire to disclose information might outweigh any perceived risk associated with disclosing (Milne & Culnan, 2004). For example, if an individual must disclose credit card information to complete a transaction, but the website does not seem trustworthy, the individual must balance the benefits of disclosing (obtaining the desired service or good) with the risk inherent in shopping on the

website (such as an untrustworthy vendor, a risky website where credit information may be leaked, or the potential for disclosure of personal information to a third party).

Several authors have attempted to conceptualize the idea of balancing or juggling the need to disclose information with perceived risks. The dilemma confronting users has been coined a *privacy paradox* (Barnes, 2006). Alternatively, when considered in the framework of cost-benefit analysis the idea has been referred to as *privacy calculus* (Dinev & Hart, 2006; Krasnova & Veltri, 2010). By contrast, others have described it as a *risk-benefit ratio* (Petronio & Durham, 2008).

Indeed, it seems that a paradox is present in online communication, specifically related to disclosing. If people sincerely perceive a level of risk when volunteering personal information to receive an online service, it is then argued that individuals would not involve themselves in this exchange (Fife & Orjuela, 2012). This notion of a *privacy paradox* (Barnes, 2006) where individuals state their intention to limit disclosure do the opposite by disclosing information, has been documented empirically (Norberg, Horne, & Horne, 2007; Yao, Rice, & Wallis, 2007; Youn & Hall, 2008). Scholars believe that the privacy paradox could be due to users' lack of awareness or literacy concerning privacy, however, the paradox has not fully been explained (Taddicken, 2014).

In the privacy calculus framework, a combination of factors (privacy concerns, perceived risk, trust, etc.) influence a user's decision to disclose information, and in turn, users consider the costs and benefits associated with the disclosure and respond appropriately. Behavioral intent to disclose results from a combination of factors. However these factors do not eliminate perceived privacy risk or concerns even when the individual favors disclosure (Dinev & Hart, 2006).

As posited in communication privacy management theory, individuals make decisions about disclosure based on a rules-based system (Petronio, 2002), ultimately attempting to minimize costs while maximizing rewards (Metzger, 2007). Risk-benefits ratio is one criteria individuals use in creating privacy rules or guidelines that dictate the ebb-and-flow of personal information (Petronio & Durham, 2008). CPM also states that privacy rules change such that as perceive risk associated with information increases, the likelihood it will not be disclosed increases (Metzger, 2007).

While these models and theories provide some rationale for investigating parts of online disclosure, they all possess some important omissions. First, many studies have failed to directly relate users' privacy concerns to their disclosure behaviors (Taddicken, 2014). Second, a weakness inherent in the frameworks lies in the identification of scenarios where willingness and perceived risk fluctuate. Third and last, these models deal with the problem as an abstraction and do not attempt to take into account *both* willingness to disclose *and* perceived risk, nor measuring specific disclosure items or categories of items empirically. As evidenced in this study, the contradiction between willingness and risk can vary by the specific information to be disclosed, and not all disclosure concerns are equally sensitive. For example, risk associated with name may not be as high as with date of birth, and this study provided clear delineations in measuring different categories of personal information.

As an alternative model, the gap between willingness and perceived risk suggested in this study might be conceptualized as *online disclosure consciousness*. In everyday parlance, consciousness can be defined as "the normal state of being awake and able to understand what is happening around you" (Merriam-Webster Dictionary, 2014c). Alternatively, online disclosure consciousness might be considered the ongoing salience or awareness of potential hazards or loss

situations and their consequences pertaining to sharing information. The premise is that individuals continuously weigh the benefits derived with the risks involved in disclosing information or managing their online privacy. In other words, with the possible exception of an impetuous act, people are wary about risks when making disclosure decisions. This constant cognitive balancing of risk and benefits is prevalent when shopping online and apparent when disclosing information (Dinev & Hart, 2006).

The disclosure consciousness model proposed here posits that individuals are indeed aware of their disclosure actions, and aware of the risks inherent in disclosing. The model argues that users' privacy/risk concerns can be directly related to their disclosure activities, and both can be measured empirically. Lastly, the model proposes that while individuals might cognitively process risk-benefit ratios in specific situations, they make decisions routinely and schematically (Fiske & Taylor, 2013, pp. 104-105) based on their knowledge stored in memory about comparable experiences and the resulting outcomes.

Conceptually, either willingness or perceived risk may override the other, and the resulting action is dictated by the overriding concern (i.e., willingness to disclose or perceived risk). If the individual's willingness-to-disclose score exactly equals her or his risk concern, they might be become stymied and decide to put off the decision to purchase and to further contemplate the benefits and costs of disclosing. Regardless of whether the gap is negative (perceived risk is greater than willingness) or positive (willingness is greater than perceived risk), an individual who is disclosure conscious will exhibit smaller difference in the gap between scores for willingness to disclose and perceived risk of disclosing. If the consumer's risk perception sufficiently outweighs the willingness or perceived benefits to disclose, he or she might decide not to disclose at all. However, if, over time, the consumer perceives that the

attendant risks are minimal and outweighed by the potential benefits, the individual will disclose information.

Applying Online Disclosure Consciousness to Compare Americans and Estonians

To examine online disclosure consciousness between participants in the two countries, the differences in the gap scores reported in Table 5.3 were analyzed using Student t-tests that compared the disclosure consciousness (gap) scores for the US and for Estonia. This analysis of "differences between differences" is reported in Table 5.4.

Table 5.4
Comparison Between US & EE Gaps Between Willingness to Disclose and Perceived Riskiness of Disclosure

	Willingness to disclose (WD) (*1=not willing, 4=neutral, 7=very willing)* Perceived risk of disclosing (PR) (*1=very risky, 4=neutral, 7=not risky)*				
Measure	US Gap	EE Gap	Difference	t	p
Index (17 items)	1.64	1.61	|.030|	0.28	.777
Contact Information	.931	.970	|.038|	0.32	.749
Payment Information	1.39	.544	|.844|	5.54	.000
Life History Information	-.179	.110	|.288|	-2.23	.026
Work-Related Information	-.459	-.145	|.314|	-2.13	.034
Online Account Information	-1.03	-.582	|.449|	-3.09	.002
Financial/Medical History Info	-.841	-.468	|.372|	-3.00	.003

These results from Table 5.4 are illustrated graphically in Figure 5.1, which depicts both the size of the gaps as well as the direction for the overall index measures as well as each of the 6 sub-indices. As explained in the legend for Figure 5.1, scores to the right of the center line indicate where willingness to disclose exceeded perceived risk. Scores to the left of the center line indicate where perceived risk is greater than willingness to disclose.

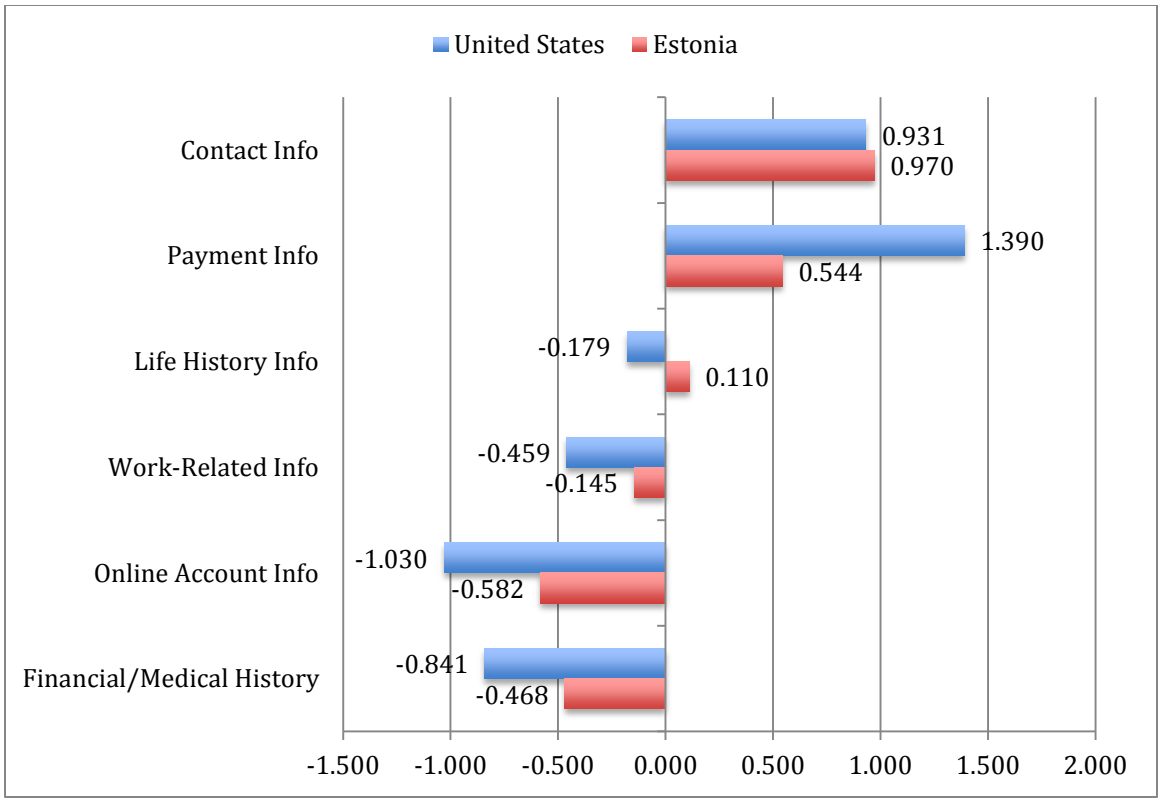


Figure 5.1
Gap Differences between Willingness to Disclose and Perceived Risk for US and Estonia

(Note: Scores to the right of the 0.00 line indicate willingness to disclose exceeds perceived risk. Scores to the left of the 0.00 line indicate perceived risk is greater than willingness to disclose. US = blue bar; Estonia = red bar)

The two items where both Americans and Estonians reported willingness to disclose scores *higher* than perceived risk scores, the difference in the gap scores was not significant for personal contact information (US gap=.931, Estonia gap=.970, difference=.038, p≤.749). However, for disclosure of payment information, the overall willingness to disclose scores were not only *higher* for the US compared to Estonia but the gap between willingness to disclose and perceived risk were also significantly *larger* (US gap=1.39, Estonia gap=.544, difference=.844, p=.000). This suggests that Americans and Estonians are comparable in their disclosure consciousness about personal contact information, but Estonians are more disclosure-conscious than Americans when disclosing payment information.

Notably, for the items for which perceived *risk* exceeded willingness to disclose, the same general pattern emerged: Overall, the gaps for Americans were significantly larger than for Estonians, for whom the two scores more closely corresponded. This finding suggests that Americans are less disclosure conscious, while Estonians might be more concerned about perceived risks, regardless of the level at which they were willing to disclose the specific types of PII.

Overall, as denoted by lower gap scores, Estonians demonstrated greater online disclosure consciousness than Americans on all five scales found to be significant. These included payment information (US gap=1.39, Estonia gap=.544, difference=.844, p=.000), life history information (US gap=-.179, Estonia gap=.110, difference=.288, p≤.026), work-related information (US gap=-.459, Estonia gap=-.145, difference=.314, p≤.034), online account information (US gap=-1.03, Estonia gap=-.582, difference=.449, p≤.002), and financial/medical history information US gap=-.841, Estonia gap=-.468, difference=.372, p≤.003).

Role of Risk-Taking as Personality Trait in Online Disclosure Consciousness

As a further way to examine risk perceptions, this study sought to consider adventurous risk-taking traits of individuals using an index of 5 items (Cronbach alpha=.88) as a possible predictor of both willingness to disclose and risk perceptions. As indicated in Table 5.8, participants were asked the degree to which they act on the spur of the moment, enjoy taking risks, are willing to take risks, consider themselves adventurous, and welcome new and exciting experiences. The results, however, were mixed.

Table 5.8 reports Estonian participants (M=4.60) were significantly higher in risk taking as a personality trait versus Americans (M=3.87, difference=-.728, t=-6.37, df=467, p=.000). These results were somewhat unexpected, but are consistent with characterizations of Estonians

as being willing to take risks. Risk taking might indeed be more prevalent among Estonians, functioning as a coping mechanism in a society that has been in transition for some time (Kaasik et al., 1998). However, the difference between the two groups could be an artifact of the composition or either the American sample (more experienced in ecommerce, more conscientious, less extraverted) or the Estonian sample (more female, older, less educated), or both. Interestingly, however, Estonians described themselves as both less open and more neurotic compared to Americans.

Table 5.8
Risk Taking as a Personality Trait

(*1=strongly disagree, 4=neutral, 7=strongly agree)*

	US		*EE*					
Measure	*M*	*SD*	*M*	*SD*	*df*	*t*	*p*	*Cohen's d*
Risk taking personality index	**3.87**	**1.32**	**4.60**	**1.14**	**467**	**-6.37**	**.000**	**.62**
I often act on the spur of the moment.	3.18	---	4.38	---	---	---	.000	---
I quite enjoy taking risks.	3.14	---	4.00	---	---	---	.000	---
I'm willing to take some risks.	4.33	---	4.74	---	---	---	.002	---
I'm an adventurous person.	3.94	---	4.74	---	---	---	.000	---
I welcome new and exciting experiences.	4.70	---	4.14	---	---	---	.001	---

Performing a correlation analysis, significant relationships were found between risk-taking as a personality trait and key variables. Although there was no relationship between risk-taking and perceived riskiness of disclosing the 17 items of personal data in the disclosure index (US r=.007, p≤.919; Estonia r=.063, p≤.368), risk-taking was positively related to willingness to disclose for the Estonians only (Estonia r=.141, p≤.043). Although a similar trend was evident for the American sample, the relationship fell short of statistical significance (US r=.141, p≤.079). Both Estonians and Americans demonstrated a positive relationship between risk taking and trust in the Internet (US r=.157, p≤.05, Estonia r=.175, p≤.01). Also, for both Americans and Estonians, risk-taking as a personality trait was positively correlated to the personality of

dimensions of extraversion (Overall sample r=.348, p≤.001, US r=.283, p≤.001, Estonia r=.350, p≤.001) and openness (Overall sample r=.301, p≤.001, US r=.296, p≤.001, Estonia r=.429, p≤.001). Interestingly, conscientiousness was negatively related to risk taking among Estonians, but not Americans (Estonia r=-.134, p≤.05; US r=-.011, p=.870). For Estonians, risk-taking was negatively correlated to anxiety (Estonia r=-.166, p=.014), but the association was not significant for Americans (US r=.111, p=.083). Surprising, while the privacy benefits index was not significantly correlated to risk taking for either group (US r=.071, p=.268, Estonia r=.114, p=.094), two items from the scale were found to be significantly positive correlated with risk taking as a personality trait for Estonians: "*I have a choice in whether my personal information should be disclosed to a third party*" (r=.144, p≤.05) and "*At any time, I can delete or edit my personal information*" (r=.199, p≤.01). Lastly, purchase benefits were positively correlated with risk taking for the Americans (r=.185, p≤.01) but were not statistically significant for the Estonians (r=.112, p=.097). No other significant relationships to risk-taking as a personality trait were found.

The results from the previous paragraph have some important implications. First, it seems that for both Americans and Estonians, individuals with higher trust in the Internet may be more likely to take risks. Further, risk-taking individuals in Estonia are more willing to disclose information. Regarding personality, extraverts and those labeled as being "open" are more likely to be risk takers, while conscientious individuals may take fewer risks. Consequently, Estonians who exhibit lower levels of anxiety disclosing personal data may be willing to take more risks.

IMPLICATIONS

The results of this study provide a potential starting point for further development of theory in an important research area that should prove to be of both theoretical and practical

interest to researchers, consumers, marketers and online merchants, and government policy makers alike.

Developing the Online Disclosure Consciousness Continuum Model

This study proposes the online disclosure consciousness continuum as an alternative to at least 3 other frameworks that have been suggested to describe the desire or need to disclose and concerns about risks. Although needing further development, the researcher proposes an online disclosure consciousness model that can be found in Figure 5.2. It treats online disclosure consciousness as a continuum anchored by two extremes. The two end anchors are *absolute willingness to disclose (AWD)* or *absolute perceived risk (APR).*

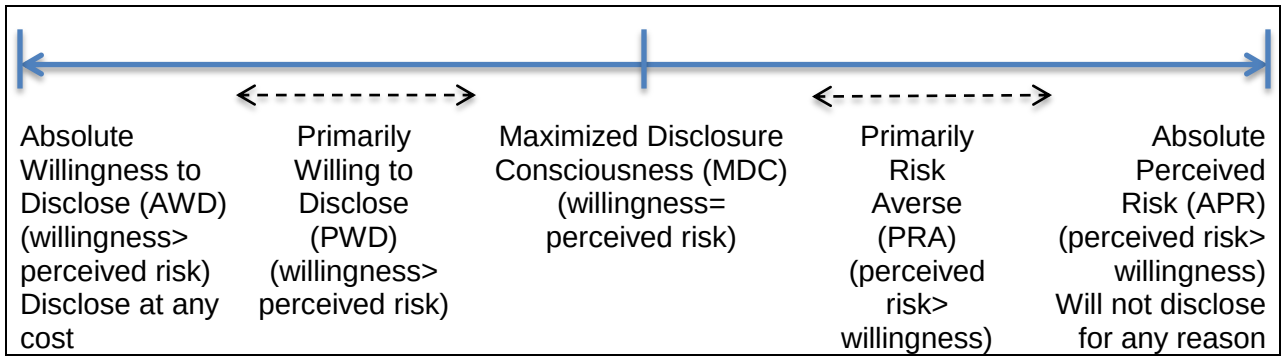


Figure 5.2
Online Disclosure Consciousness Continuum
Note: AWD (absolute willingness to disclose) is when willingness>perceived risk, and one will disclose at any cost without regard to risk. PWD, primarily willing to disclose, is when willingness>perceived risk but risks weigh heavily in the decision. MDC (maximized disclosure consciousness) is where willingness is offset by risk concerns. PRA (primarily risk averse) is when perceived risk>willingness and suggests the individual is especially cautious. APR (absolute perceived risk) is where perceived risk>willingness to disclose and an individual will not disclose for any reason.

In the first of five possible situations, represented on the left, an individual exhibits absolute willingness to disclose (AWD) with total disregard for risk. This left anchor of the continuum, AWD holds that an individual's willingness score completely outweighs the perceived risk. In this situation, the individual is either unaware of the risk in general or ignores

it entirely. Absolute willingness to disclose includes but is not limited to impetuous or impulsive acts of disclosure where the person behaves with reckless disregard.

The right anchor on the online disclosure consciousness continuum represents absolute perceived risk (APR), where the hazards or fear of loss precludes any intention to disclose. In the APR scenario, the potential discloser is either overwhelmed by the possible resulting risks, and disclosure is not even considered an option. If individuals continually experience APR scenarios, where perceived risk far outweigh willingness to disclose and constantly choose not to disclose, it could be considered neurotic, as many potential benefits arise from disclosure (i.e., development of self, friendships, greater freedom to communicate).

The midpoint in the model represents Maximized Disclosure Consciousness (MDC), where willingness and perceived risk equal each other, leaving the discloser unable to act.

The final two scenarios on the online disclosure consciousness continuum fall between absolute willingness to disclose and MDC, and absolute perceived risk and MDC. In the fourth situation, represented left of center of the continuum, an individual is primarily willing to disclose (PWD) or inclined to disclose. In the PWD situation, the willingness to disclose is not absolute and the conscious effort to weigh the benefits against the risks is at work. Importantly, this situation represents any situation where an individual initially believes willingness exceeds perceived risk and might be driven by temptation and the perceived benefits of an offer despite second thoughts pertaining to risks. Here, the individual is more cognitively aware of the inherent risks than in absolute willingness to disclose, but the decision to disclose is more difficult to complete. This scenario seems quite prevalent in the study, where willingness to disclose outweighed perceived risk, and therefore disclosure occurs.

The fifth and final scenario, primarily risk averse (PRA), represented on the right center of the continuum, is where the individual's perceived risks initially exceed benefits of disclosure. In the PRA scenario, perceived risk may outweigh disclosure and individuals might need to be convinced that disclosing is advantageous. Convenience or necessity of the disclosing act must overcome the greater perceived risk versus disclosure. For example, if an individual chooses to file taxes online, the risk associated with the information far outweighs the desire to disclose, but the individual will disclose anyway to complete a necessary task.

Of the five scenarios proposed for the online disclosure consciousness continuum, the author proposes that the two partial situations are most likely: PWD and PRA. Abstaining from disclosure altogether as in APR, may lead to serious consequences, as may full disclosure, as represented in AWD. While an individual experiences MDC at some point, it would seem logical at some time for a person to resolve mental deadlock by deciding either for or against disclosure. In this instance, an individual can move along the continuum choosing either PWD or PRA.

In the proposed ODC model, decisions are not static. The process of decision-making is dynamic and a person can move along the continuum, influenced by 1 or more of 3 factors: marketers' actions, personal experience, or external happenings.

In essence, marketers want individuals to move left on the continuum, ultimately disclosing information to facilitate a transaction. Marketers exert influence over an individual's decision on the continuum by offering benefits, enhancing trust, and lowering the perceived risks. However, there are situations where marketers might not encourage disclosure, such as when legal or security problems might result. Ultimately however, a marketer strives to offer such a compelling benefit it might coax an individual from the middle or right side of the continuum to the left. If the individual remains reticent, a marketer can simply increase benefits

promoted or reasons for disclosure (i.e., better customer service, tailored shopping experience, greater merchandise selection), or offer an incentive.

Personal events and experience also influence movement on the ODC continuum. Positive experiences encountered when disclosing personal data, for example, can bolster a person's confidence or self-efficacy or reduce a person's reluctance. Social pressures, such as a friend encouraging purchase of a "cool" product, or providing encouragement or assurance that disclosure is safe, might swing the individual in the direction of willingness to disclose. Conversely, if a friend or family member had a bad experience such as finding a travel site confusing or deceptive, the individual's willingness to disclose may be stymied or the individual might move right on the continuum and become overpowered with risk aversion.

Beside marketers' influence and internal activities, external developments can influence disclosure decisions. An individual might be perfectly willing to disclose personal data to purchase a product or service, but if the website is hacked and news about the incident is widely circulated, the individual might quickly decide not to disclose information because the risk is too great. Ongoing negative coverage of data breaches and warnings about the need to be concerned about privacy can pose barriers. On the other hand, popular events might prompt disclosure without much consideration of the risk, as witnessed by viral fundraising events for charity or disaster relief. Positive, societal events might lead people to support a worthy cause. Lastly, global events outside the control of any individual may dampen disclosure. Wars, economic downturns, spread of disease, and other gloomy global events might also dissuade consumers from disclosing due to perceived risk. Conversely, public health threats might influence people to disclose, such as signing up for emergency text message notifications about weather emergencies or public health outbreaks. Importantly, certain organizations such as privacy

advocates, actively discourage individuals from disclosing information and promote the importance of using extreme care in doing so. Essentially these organizations counteract marketers' actions and people's desires by influencing individuals to move to the right on the ODC continuum.

Implications for Theory

As a major focal point of this study, willingness to disclose was found to vary by individual and nationality. Willingness to disclose may be predicted by various factors, including education, ecommerce experience, perceived ecommerce benefits of opportunity benefits and purchase benefits, the personality trait of agreeableness, trust in Internet, and lastly, trust in institutions. Further, willingness to disclose was found to be positively correlated with attitude toward disclosing and was negatively related to anxiety.

This study provided a practical scale for measuring willingness to disclose, specifically opting to use a 17 items of personal data as a measure. The measure for willingness to disclose is not exhaustive, and additional items might be added in future studies. By demonstrating that personal information items can be split into six distinct categories (contact information, payment information, life history information, work-related information, online account information, and financial/medical information) this study created a reliable scheme for classifying different types of personal information. In future research, a priority will be to create a more efficient measure of willingness to disclose, perhaps focusing on or combining the two sets of measures that generated the most response, contact information and payment information.

This research demonstrated that personality can be a valuable concept for examining disclosure online based on the relationship among openness, agreeableness and neuroticism and willingness to disclose (H3) and the relationship between risk-taking as a personality trait and

conscientiousness. Contemporary researchers continue to seek quick but reliable methods for measuring personality. By using an ostensibly efficient 20-item personality scale adapted from the Big-Five Inventory (John et al., 1991), this study demonstrated a potentially useful set of indices for measuring personality. The study's findings show that the five dimensions of personality cross nationalities (with the exception of agreeableness for Estonia) and that the scale might provide a good instrument for measuring these dimensions.

Further, this study has helped shed light on what kinds of information individuals label as most and least risky. In areas where social media and technology change quickly, perceptions of what is private may also transform rapidly. This study provides contemporary insights into how people with different personality characteristics and nationalities differentiate private information. What constitutes *risky* personal information could be seen as a moving target, and this research provides up-to-date information on what type of information individuals in two different countries constitute as risky to be disclosed.

In addition to completing analyses of personality characteristics involved in risk analysis and disclosure, this study tested a framework to help identify explanatory variables for both willingness to disclose and perceived risk of disclosing PII. The explanatory variables identified included the importance of purchase benefits, trust (in both the Internet and public institutions), and the related roles of attitudes and anxiety related to disclosing. Looking ahead, further analysis of the data and refinement of the conceptual model will be beneficial for informing privacy theory.

The online disclosure consciousness continuum provides a potential theoretical contribution for understanding the cognitive processes involved in the balance of protecting versus disclosing personal information. Presented with the five scenarios in the continuum,

theorists may be able to further conceptualize disclosure processes. The model needs to be subjected to empirical testing, but provides a starting point for development of theory. The proposed online disclosure consciousness continuum model refines the theories of privacy paradox, privacy calculus, or communication privacy management and serves as a complimentary "piece of the puzzle" in understanding online disclosure. Specifically, one key advantage lay in its conceptualization of scenarios on the continuum of disclosing information.

Implications for Consumers

Consumers and their privacy concerns were an important focus of this study. Establishing a relationship between the marketer and the consumer is the foundation for completing purchases online. With this in mind, several implications emerge from this study for how consumers can protect their privacy while also obtain benefits while continuing or creating relationships with online marketers, retailers, or merchants. Specifically, it is important that shoppers educate themselves, understand the varying risk associated with different types of personal data, be aware of intrinsic factors affecting disclosure and perceived risk, and lastly, learn to recognize reputable and trustworthy merchants.

In light of the need among marketers to solicit personal information, consumers should be aware that marketers might in fact entice them through use of shopping benefits in order to collect personal information. Consumers must become familiar with the practices employed by marketers to encourage them to disclose personal information online. Shoppers should take precautions to prevent the unsolicited and undesired gathering of their information. Examples include reading privacy statements and employing ad-blocking technologies where necessary. Consumers have a responsibility to be an informed consumer, and organizations such as the Electronic Frontier Foundation and the Federal Trade Commission in the US conduct consumer

privacy education campaigns about how to protect personal information--and how to wisely disclose it online when appropriate.

Besides becoming informed about common online marketing practices, consumers should be aware of intrinsic factors that affect their willingness to disclose and perceived risk of disclosing. From the results of this study, personality traits affected both willingness to disclose and perceived risk of disclosing. Consequently, a consumer should know his or her personality and how it might affect disclosing online. For example, an open or agreeable person might be predisposed to sharing information and might need to take extra care. Conversely, those demonstrating neuroticism may not be as willing to disclose and might perceive more risk than really exists. By not disclosing, a neurotic person might miss out on benefits or opportunities.

Trust, in general, is a predictor of willingness to disclose and is important when consumers decide about making purchasing decisions online. Consumers should know and only disclose personal data to organizations they know and trust. Underscoring the importance and value of public privacy education programs, consumers should consult organizations that provide reviews of online merchants. In the United States, the Better Business Bureau (BBB) provides ratings and reviews for online merchants, and the organization provides similar reviews for many companies in the EU.

Implications for Practice

The findings of this study suggest some best practices that marketers should consider. These suggested best practices include requesting information wisely, offering attractive benefits in exchange for personal information, fostering trust with consumers, tapping consumer personality to target messages, and lastly, connecting with consumers through social media.

Requesting information wisely. Marketers should selectively choose which PII items they require to complete a transaction. In the United States, this study found financial and medical history information are perceived as being the most risky to disclose. It would benefit marketers and ecommerce sites to refrain from soliciting this type of information unless absolutely necessary, since the perceived risk of disclosing such information may actually discourage consumers from completing purchases. Conversely, marketers and ecommerce sites may find easier ways to solicit information, such as contact information, that is considered less risky in both the United States and Estonia.

Offering benefits or incentives in exchange for personal information was shown in this study to function as an important predictor of inclination to disclosure and possibly decreases the perceived risks of disclosing personal information. Willingness to disclose was positively related to all four ecommerce benefits presented (addressing privacy expectations, positioning online shopping as an opportunity, and promoting the likelihood of finding a bargain while shopping online). For Estonians, purchases benefits were a predictor of lower perceived risk of disclosing in general. The promotion of purchase benefits could greatly encourage individuals to disclose information.

Fostering trust. Online merchants who strive to be successful in encouraging disclosure of PII must foster an environment of trust. For both business and government, there are a plethora of tools to increase trust. Merchant endorsements that attest to or approve the site's business or disclosure practices include displaying emblems from entities such as the Better Business Bureau (BBB) or eTrust. In Estonia, practices for increasing consumer trust include assurances of buyer protection and secure shopping (European Consumer Center of Estonia, 2014), and consumers may also browse a black list of online stores not adhering to Estonian

government regulations for ecommerce (Tarbijakaitseamet, 2014). Merchants may also allay concerns by allowing money-back guarantees, offering trial periods for purchases, featuring testimonials from satisfied users, and listing company contact information for verification. Professional design, presentation, and credible content may also help decrease consumer concerns. It would greatly benefit online merchants, as well as government and public institutions engaged in ecommerce, to encourage such public trust, as this may directly translate into increased levels of transactions, which can make organizations more efficient and effective.

Tap insights about consumer personality. Using consumer personality traits to more effectively target product and service messages is another important component marketers should consider. This study found that openness and agreeableness were positively correlated and neuroticism was negatively correlated to willingness to disclose. Through data mining, marketers have a powerful mechanism for better identifying possible relevant, messages. By tailoring messages based on a consumer's personality, merchants might be able to further encourage disclosure during purchases. For example, consumers high in openness might be best reached using appeals that involve being open: suggest being creative or imaginative, original and inventive. In the same regard, to reach agreeable individuals, marketers might focus on attributes of products of service that stress being trusting, considerate to others, and cooperative. Motiving neurotics calls for messages that evoke calm, stress-free conditions.

Connecting with consumers via online accounts. This study found that consumers from two different countries rated online account information (Facebook, Twitter, and Skype accounts) as the second most risky information to disclose. Notably, these findings provide clear and important implications for marketers in that they should carefully solicit consumers' online account information, and that contacting consumers through these networks may annoy or

alienate them and reduce trust in the marketer or merchant. It is recommended that if marketers are interested in interacting with consumers through their online accounts, the communication should be initiated by the consumer, and not by the marketer.

Implications for Public Policy

Privacy protection is not a "one size fits all" proposition, so this study, along with future studies, can contribute to the process by fostering understanding of what personal data items are particularly important to individuals, and how concerns might vary by age, education, gender, and Internet usage. Such findings will help to further define privacy concerns, and in turn, provide insights into the development of policies aimed to protect privacy rights while maintaining free exchanges. Of particular note, policy makers should recognize that participants in this study highlighted the importance of having control over their personal information. In the privacy benefits expected index, the two most important privacy benefits in both the US and Estonia were "I have a choice in whether my personal information should be disclosed to a third party" and "At any time, I can delete or edit my personal information." It seems that regardless of nationality, having full control over one's personal information is of great importance, and a principle that regulators should make continue to strengthen through industry oversight and regulation.

Policy makers should continue to encourage the use of affirmative opt-in versus opt-out settings in online accounts. Typically, merchants and marketers apply an opt-in approach where the user's information is collected as a default policy. By requiring users to opt in only if they desire to do so, information is not collected. A user must purposefully change account settings so that marketers and other entities are allowed to gather and utilize personal information. From the results pertaining to privacy expectations, this study found that users having complete control

over their personal information is very important. By providing consumers with a choice whether to opt-in rather than opt-out, consumers are in full control of their personal information.

For policy makers in both the United States and the European Union, this study shed light on kinds of information consumers consider risky. Based on the demonstrated levels of riskiness associated with the 17 items of personal data, policy makers would be wise to consider the level of regulation needed to protect information considered especially risky. The need for closer examination of the use of various ecommerce benefits in exchange for disclosing information is also highlighted by the research, showing that many perceived benefits may be more effective marketing tools than information gathering practices that may serve to alienate customers and citizens.

While all participants in the study were at least 18 years of age, it would be useful to extend this study's framework to minors, specifically their willingness to disclose specific PII items (including items that might not be applicable to adults) and their perceptions of the attendant risks. It would be particularly important to investigate how marketers might use perceived shopping values or bargains (in the form of purchase benefits) or social opportunities to target minors. Estonia may not necessarily be representative of the European Union as a whole, but investigating that extremely high-tech nation's perceptions of privacy and risk could help shape policies for other EU countries struggling to define and protect consumers' personal information.

Finally, this study can help bridge the gap between the US and the EU in terms of shaping consumer data protection. Disagreements over the issue of international data protections and other consumer privacy issues could indeed undermine trade negotiations such as those currently being worked out through the Transatlantic Trade and Investment Partnership

(Erlanger, 2013). Understanding national differences in the perception of privacy and disclosure could prove valuable in working out mutually acceptable international solutions to privacy protection, while maintaining the openness necessary to the effective functioning of global markets.

This study might be useful in helping to increase usage of ecommerce not only in established markets, but also in emerging markets. In nations such as Estonia, where ecommerce is burgeoning, knowing how trust and perceived shopping values and bargains work together will be critical aspects of nurturing a continually expanding ecommerce marketplace. As other nations in the EU and around the world expand their usage of ecommerce -- a 50% increase in ecommerce is expected just in Europe by 2019 (Economist, 2014) -- governments, consumers, and online merchants must have a clear understanding of how to best encourage ecommerce adoption.

LIMITATIONS

This study had several limitations. First, the research used non-probability sampling to recruit enough participants from both the United States and Estonia. Even though purposive quota sampling was used, the reported demographics are skewed between the US and Estonia in the area of education. The profile of study participants thus might not be representative of the populations studied.

For future studies, ecommerce experience should be measured using a multi-item index to enhance the measure's validity. Important differences were found between the Estonian and American samples regarding the impact of experience as a predictor of willingness to disclose. This suggests that experience is a potential confound or explanatory variables that needs to be incorporated in future studies. The problem of examining ecommerce experience was

compounded in this study with the use of a single-item measure that combined the concepts of self-reported proficiency and experience and used a continuum that ranged from expert to beginner. These should be more properly separated. Other possible measures for experience include extent of ecommerce use, such as the number of ecommerce transactions completed in the past month. To the extent possible, research must more fully take into account factors such as usage, proficiency, self-efficacy, and the purposes for which ecommerce transactions are undertaken (such as personal versus business use). While these limitations may make it impossible to generalize from this study to the entire US or Estonian populations, the research nonetheless resulted in noteworthy findings that can inform and influence the direction and design of future studies, particularly for researchers interested in increasing understanding of how cultural differences help determine the mechanisms of disclosure and privacy in the Internet setting.

Improving the conceptualization and operationalization of perceived ecommerce benefits also would be beneficial for future studies. The benefits examined in this study are not exhaustive, and identifying and measuring additional ecommerce benefits could provide additional insights into the relationship between disclosing information and the use of various shopping benefits. Identifying additional scenarios where consumers exchange information while shopping (including referrals) would allow extension of the current benefits measures.

Going beyond these methodological limitations of the study, it seems clear that, in the international realm, translation can be an issue. The most qualified translation service provider in Estonia was retained to assure a high quality of translation, and one indicator of the success of the translation was evident in the similar Cronbach alphas for the indices within the Estonian population compared to the US participants. These suggest that the items were reasonably

comparable in perceived meaning and measured a single underlying construct.

Just as choosing a translation service, deciding on what recruitment service to use can be a complicated part of conducting research. The decision to use Amazon's Mturk for participants was both convenient and cost efficient for the purposes of this study. But because all but 16 Mturk participants rated themselves as above average in ecommerce experience, it is probable that the Mturk panel was not representative of the general US population in terms of ecommerce proficiency – an important moderating variable in the study. Additionally, the Estonian sample was recruited from within a pool of registered web panel participants and might not have been representative of the general Estonian population.

Other variables, such as personality, were measured with an adapted version of the BFI scale, which may present some issues of reliability on at least one dimension. The adapted BFI scale proved reliable except for the personality dimension of "agreeableness" in Estonia (Cronbach α =.56). This issue may be related to faulty translation (as discussed above), or it could have resulted from the use of a shortened set of personality measures. Alternatively, there might be cultural explanation that made the notion of "agreeableness" different in Estonia.

Conducting a cross-national study is a huge undertaking and a challenge for any researcher, and this author learned many things along the road to completion. Working with individuals located nine time zones away presented logistical challenges and being culturally sensitive was extremely important when conducting international research. Researchers seeking to conduct cross-national/cross-cultural research should explore the advantages and disadvantages related to this type of work. Again, as an initial study, this research project has helped the author define a number of new directions for his own research in the areas of

consumer decision-making and privacy disclosure online. This study will guide future research in an important field that remains wide open.

FUTURE RESEARCH

Opportunities for future research exist in several key areas related to this study. The first and most timely extension of this research would be to conduct comparable studies in additional countries in the EU, as well as to countries outside the EU. The question of how citizens in different nations within the EU perceive disclosure of personal information would be a valuable starting point for extending the comparisons of national and individual patterns of belief about privacy and disclosure. Belgium, for example, provides a unique opportunity to study two culturally unique identities side by side (Flemish and Walloon). Continuing to inform public policy about what constitutes sensitive personal data, this proposed research would compare differences in willingness and perception of risk of personal information online between and within various EU states, ultimately noting differences or commonalities upon which legislation and regulation can be successfully adopted. Other researchers might wish to extend this study to Asia, the Middle East, and South America as well. Most importantly, it should be noted that many relevant policy issues will certainly emerge in the next few years, so this program of research will continually evolve along with public debates about online privacy concerns.

Additional research could build on the findings of this study to examine issues around privacy and disclosure. Follow-up studies could be conducted, specifically investigating the impact of additional perceived benefits and their impact on willingness to disclose. Identifying further items of personal data for inclusion in the willingness to disclose and perceived risk of disclosing indices is a priority to be examined in future work as well. If a sufficiently large sample could be obtained, for instance, Structural Equation Modeling (SEM) (Joreskog, 1970)

could be deployed to outline causal relationships within the study's conceptual model. By using SEM, further testing and development of this study's conceptual model might lead to valuable findings.

Beyond extending the current study to additional countries, studies into the use of shopping values or bargains in exchange for personal information are called for. As this research has shown, perceived benefits are powerful motivators, increasing the willingness to disclose and/or lowering perceptions of risk.

Similarly, exchange of information may be either explicit or implicit. Explicit disclosure was examined in this study, where an individual knowingly provides personal information to obtain a benefit. Conversely, implicit disclosure, the focus of future research, is where an individual provides information without his or her knowledge. Differences in these types of disclosures are provided using an everyday scenario faced by individuals looking for travel directions. When an individual accesses Google Maps in the Mac's Safari web browser, the user is asked to use their current GPS location information to pinpoint their exact location on a map. Here again, individuals are exchanging personal information for a benefit. Users routinely authorize access to location information on websites and mobile apps on a daily basis. If a user authorizes disclosure of location information for all future requests, they may easily be disclosing implicitly and unintentionally without their knowledge in the future.

Another new technology involving implicit disclosures with great potential are smart infrastructures, or city infrastructures, that use a feedback loop of data collected by sensors that collect evidence for informed decision making by city and government personnel (Royal Academy of Engineering, 2011). These smart infrastructure systems can monitor, measure, analyze, and communicate and act, based on information captured from sensors. In one scenario,

smart infrastructure may collect, process, and present recommendations to help human operators make decisions, with an example of this system appearing in Tallinn, Estonia and other large cities, where the traffic systems can detect congestion or more efficient routes and notify drivers accordingly. While users may explicitly authorize the use of their location information when they sign up for the service, they become complacent while using the transit system, implicitly disclosing information over the course of time. In this type of exchange, individuals may provide very precise tracking information in exchange for quicker, more efficient travel where the transit authorities can predict usage patterns and increase or decrease transit opportunities in specific parts of the city or during specific times of day. A number of questions arise with new options that provide greater convenience at the expense of privacy, including how these smart infrastructures make us re-evaluate what we perceive as private information? Are users willing to provide tracking information to access simpler, digitally enabled infrastructure such as enhanced bus or postal services or easier access to parking? The commercial exchange of personal information for discounts or coupons is the basis for commercial transactions online, and might become increasingly common among users of smart infrastructure services. These new uses of technology will raise new questions about privacy, making studies like this one increasingly valuable as we move forward.

Ethics provide one framework for understanding the impact and implications of collecting personal information too. When analyzed through Rawls' (2001) notion of the "least advantaged" with regards to privacy and anonymity, clear implications emerge that could serve as guidelines for setting marketing policy and outlining controls. At stake, specifically, is the use of individuals' sensitive personal data similar to the items analyzed in this study. Merchants have a responsibility to conduct data collection ethically, and consumers should be informed of how

their information is used. A critical question evolves around whether privacy policies and other disclosures by organizations actually enhances willingness to disclose or simply raises concerns about risks that might have unintended or detrimental consequences for users. Research, building on findings from this study, may help provide a framework for comparison of US and EU marketing practices. Investigating possible differences in data collection policies through an analysis of Rawls' principle of the least advantaged, could lead to recommendations for government and consumer policy regarding online privacy.

CONCLUSION

This research identified many factors that influence willingness to disclose personal information, as well as what types of information individuals perceive as risky to disclose. This cross-national study of the United States and Estonia informed the creation of a new framework that might be helpful in understanding the complex processes involved in disclosing personal information. Lastly, the findings from this research can help drive increased adoption and usage of ecommerce across the globe by helping marketers understand the linkages between perceived risk and willingness to disclose, as well as increasing consumers' trust and lowering risk involved in purchasing online. This hopefully will lead to multiple studies critically important to building strong research in the field of online disclosure – and which will inform academics, consumers, marketers and public policy in the complex workings of what can be seen as a dynamics defined by Internet technologies, and by the people and nations that use them.

REFERENCES

A.A.K. (2013, July 30). How did Estonia become a leader in technology? *The Economist*. Retrieved from http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21

ABB. (2013). World's first nationwide EV-charging network starts - based on ABB fast charger technology. Retrieved May 12, 2014, from http://www.abb.us/cawp/seitp202/61df2f8f8c7d00a6c1257b18002d5e3c.aspx

Acohido, B. (2014, January 23). Payment card data theft jumps five-fold. *USA Today*. Retrieved from http://www.usatoday.com/story/cybertruth/2014/01/23/payment-card-data-theft-jumps-five-fold/4796685/

Altman, I. (1973). *Social penetration: The development of interpersonal relationships*. New York, NY: Holt, Rinehart and Winston.

Amazon Mechanical Turk. (2014). FAQ - Overview. Retrieved April 25, 2014, from https://http://www.mturk.com/mturk/help?helpPage=overview

American Psychological Association. (2014a). Psychology topics: Anxiety. Retrieved August 5, 2014, from http://www.apa.org/topics/anxiety/

American Psychological Association. (2014b). Psychology topics: Personality. Retrieved August 5, 2014, from http://apa.org/topics/personality/

Amichai-Hamburger, Y., Wainapel, G., & Fox, S. (2002). On the Internet no one knows I'm an introvert: Extraversion, neuroticism, and Internet interaction. *CyberPsychology & Behavior, 5*(2), 125-128. doi:10.1089/109493102753770507

Anderson, J. C. (2013). Identity theft growing, costly to victims. *The Republic.* Retrieved May 8, 2014, from http://www.azcentral.com/business/consumer/articles/20130401identity-theft-growing-costly.html

Arnold, C., Sapir, E., & Zapryanova, G. (2012). Trust in the institutions of the European Union: A cross-country examination. *European Integration online Papers (EIoP), 16*. doi: 10.1695/2012008

Baker, W. B., & Matyjaszewski, A. (2010). The changing meaning of "personal data". Privacy Association.Org. Retrieved from http://www.privacyassociation.org/resource_center/the_changing_meaning_of_personal_data

Barak, A., & Bloch, N. (2006). Factors related to perceived helpfulness in supporting highly distressed individuals through an online support chat. *Cyberpsychology & Behavior, 9*(1), 60-68. doi: 10.1089/cpb.2006.9.60

Bargh, J. A., McKenna, K. Y. A., & Fitzsimons, G. M. (2002). Can you see the real me? Activation and expression of the "true self" on the Internet. *Journal of Social Issues, 58*(1), 33-48. doi: 10.1111/1540-4560.00247

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11 (9), 0-0. http://dx.doi.org/10.5210/fm.v11i9.1394

Bauer, R. (1960, June 15). Consumer behavior as risk-taking. In R. S. Hancock (Ed.). *Dynamic marketing for a changing world: Proceedings of the 43rd National Conference of the American Marketing Association*: Chicago, IL (pp. 389-398). Retrieved from http://www.worldcat.org/title/american-marketing-association-international-member-marketing-services-guide/oclc/34008960&referer=brief_results

Baumgarten, F. (1937). Die charaktereigenschaften [The character traits]. *The Journal of Nervous and Mental Disease, 86*(1), 113-129.

Berinsky, A. J., Huber, G. A., Lenz, G. S., & Alvarez, E. B. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis, 20*(3): 351-368. doi: 10.1093/pan/mpr057

Boduszek, D. (2013). Multiple regression. [PowerPoint presentation]. University of Ulster. Retrieved from http://www.danielboduszek.com/documents/Multiple%20Regression%20-%20D.%20Boduszek.pdf

Branton, P. (1969). Behaviour, body mechanics and discomfort. *Ergonomics, 12*(2), 316-327. doi:10.1080/00140136908931055

Briggs, F. (2014). Global B2C e-commerce sales to hit $1.5 trillion driven by growth in emerging markets, eMarketer finds. *Retail Times.* Retrieved February 11, 2104, from http://www.retailtimes.co.uk/global-b2c-e-commerce-sales-hit-1-5-trillion-driven-growth-emerging-markets-emarketer-finds/

Brill, J. (2010). Remarks by [FTC] Commissioner Julie Brill - Keynote address. Speech presented at Proskauer on Privacy, New York, NY. Retrieved April 23, 2014, from http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-julie-brill/101019proskauerspeech.pdf

Brosdahl, D. J. C., & Almousa, M. (2013). Risk perception and Internet shopping: Comparing United States and Saudi Arabian consumers. *Journal of Management & Marketing Research, 13,* 1-17. Retrieved from http://www.co.springer.iier.aabri.com/manuscripts/131443.pdf

Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information Security Technical Report, 14*(3), 160-166. Retrieved from http://dx.doi.org/10.1016/j.istr.2009.10.007

Bucur, A., Renold, C., & Henke, M. (1999). How do older netcitizens compare with their younger counterparts? *CyberPsychology & Behavior, 2*(6), 505-513. doi: 10.1089/cpb.1999.2.505

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science, 6*(1), 3-5. doi: 10.1177/1745691610393980

Butt, S., & Phillips, J. G. (2008). Personality and self-reported mobile phone use. *Computers in Human Behavior, 24*(2), 346-360. doi:10.1016/j.chb.2007.01.019

Callahan, M. E. (2012). *Handbook for safeguarding sensitive personally identifiable information*. Washington, DC: Department of Homeland Security. Retrieved February 23, 2014, from https://http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

Capece, G., Calabrese, A., Di Pillo, F., Costa, R., & Crisciotti, V. (2013). The impact of national culture on e-commerce acceptance: The Italian case. *Knowledge & Process Management, 20*(2), 102-112. doi: 10.1002/kpm.1413

Caplan, S. E. (2007). Relations among loneliness, social anxiety, and problematic Internet use. *CyberPsychology & Behavior, 10*(2), 234-242. doi: 10.1089/cpb.2006.9963

Cattell, R. B. (1957). *Personality and motivation structure and measurement*. Oxford, England: World Book Co.

Chen, G. M. (1992). Differences in self-disclosure patterns among Americans versus Chinese: A comparative study. *Journal of Cross-Cultural Psychology*. *26(*1), 84-91. doi: 10.1177/0022022195261006

Cheung, C., & Lee, M. (2002). Trust in Internet shopping: Instrumental development and validation through classical and modern approaches. *Journal of Global Information Management, 9*(3), 23-35. doi: 10.4018/jgim.2001070103

Choi, J., & Geistfeld, L. V. (2004). A cross-cultural investigation of consumer e-shopping adoption. *Journal of Economic Psychology*, *25(*6), 821-838. Retrieved from http://dx.doi.org/10.1016/j.joep.2003.08.006

Cinite, I., Kumar, V., & Kumar, U. (2008, May 24-27). *Trust in e-commerce in Canada and the Baltic states: A comparative study.* Paper presented at the ASAC Conference, Halifax, Nova Scotia.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*(4), 909-927. doi: 10.1037/0021-9010.92.4.909

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications, 2*(3), 203-215. Retrieved from http://dx.doi.org/10.1016/S1567-4223(03)00024-3

Correa, T., Hinsley, A. W., & de Zúñiga, H. G. (2010). Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in Human Behavior, 26*(2), 247-253. Retrieved from http://dx.doi.org/10.1016/j.chb.2009.09.003

Costa, P. T., & McCrae, R. R. (1985). *The NEO Personality Inventory manual.* Odessa, FL: Psychological Assessment Resources.

Countryreports.org. (2014a). Estonia economy. Retrieved January 30, 2014, from http://www.countryreports.org/country/Estonia/economy/overview.htm

Countryreports.org. (2014b). United States of America economy. Retrieved January 30, 2014, from http://www.countryreports.org/country/UnitedStatesofAmerica/economy/overview.htm

Cox, D. F., & Rich, S. U. (1964). Perceived risk and consumer decision-making: The case of telephone shopping. *Journal of Marketing Research, 1*(4), 32-39. Retrieved from http://www.jstor.org/stable/3150375

Cozby, P. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*, 73-91. doi: 10.1037/h0033950

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,16*(3), 297-334. doi: 10.1007/BF02310555

Davis, J. (2007). Hackers take down the most wired country in Europe. *Wired*. Retrieved January 28, 2014, from http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102-115. doi: 10.1111/j.1540-4560.1977.tb01885.x

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. *Annual Review of Psychology, 41*(1), 417. doi: 10.1146/annurev.ps.41.020190.002221

Dillard, J. P. (1993). Persuasion past and present: Attitudes aren't what they used to be. *Communication Monographs, 60*(1), 90-97. doi:10.1080/03637759309376299

Dillman, D. A. (2009). *Internet, mail, and mixed-mode surveys: The tailored design method* (3rd ed.). Hoboken, NJ: Wiley & Sons.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/isre.1060.0080?journalCode=isre

DMAaction.org. (2011). Safeguarding ethical use of consumer data for marketing purposes. New York, NY: Direct Marketing Association. Retrieved November 26, 2011, from http://www.dmaaction.org/issues/consumer-data

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing, 61*(2), 35-51. Retrieved from http://www.jstor.org/discover/10.2307/1251829

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October 4-5). Behavioral response to phishing risk. Paper presented at the 2nd Annual Anti-Phishing and eCrime Researchers Summit, Pittsburgh, PA.

Durand, C. (2010). A comparative study of self-disclosure in face-to-face and email communication between Americans and Chinese. Unpublished undergraduates's thesis, University of Rhode Island, Kingston, RI. Retrieved from http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1199&context=srhonorsprog

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society, 9*(4), 433-451. doi: 10.1080/13691180600858606

E-estonia.com. (2013). Turning around the 2007 cyber attack: Lessons from Estonia. Retrieved January 28, 2014, from http://e-estonia.com/news/13-09-16/turning-around-2007-cyber-attack-lessons-estonia

E-estonia.com. (2014a). Electronic ID Card | e-Estonia. Retrieved January 13, 2014, from http://e-estonia.com/components/electronic-id-card

E-estonia.com. (2014b). e-Tax | e-Estonia. Retrieved January 13, 2014, from http://e-estonia.com/components/e-tax

Eagly, A. H. & Chaiken, S. (1993). *The psychology of attitudes*. Fort Worth, TX: Harcourt Brace Jovanovich College Publishers.

The Economist. (2014). The rise of e-commerce has set off a boom in the market for warehouses. Retrieved September 5, 2014, from http://www.economist.com/news/business/21610288-rise-e-commerce-has-set-boom-market-warehouses-stores-value

eMarketer. (2013). B2C ecommerce climbs worldwide, as emerging markets drive sales higher. Retrieved from http://www.emarketer.com/Article/B2C-Ecommerce-Climbs-Worldwide-Emerging-Markets-Drive-Sales-Higher/1010004

Endline, S. (2013). Think global, act local: Four ways your company can be socially responsible and prosperous. *Forbes*. Retrieved from http://www.forbes.com/sites/entrepreneursorganization/2013/09/09/think-global-act-local-four-ways-your-company-can-be-socially-responsible-and-prosperous/

Erlanger, S. (2013). Conflicting goals complicated an effort to forge a Trans-Atlantic trade deal. *New York Times*. Retrieved from http://www.nytimes.com/2013/06/13/business/global/to-create-jobs-europe-pushes-for-trade-deal-with-us.html?pagewanted=all&_r=0

Estonia.eu. (2014). Estonia at a Glance - estonia.eu. Retrieved January 13, 2014, from http://estonia.eu/about-estonia/country/estonia-at-a-glance.html

Estonian Information System's Authority. (2006). Facts about e-Estonia. Retrieved January 23, 2014, from http://www.ria.ee/facts-about-e-estonia/

Estonian Information System's Authority. (2013). Data exchange layer X-Road. Retrieved May 9, 2014, from https://http://www.ria.ee/x-road/

Estonian Ministry of Foreign Affairs. (2010). Glance in the mirror 2010: Estonia as reflected by foreign media. Retrieved January 23, 2014, from http://www.vm.ee/?q=en/node/10957

Estonian Review. (2012). Use of online banking in Estonia exceeds EU average by one-third. Retrieved May 7, 2014, from http://www.vm.ee/?q=en/node/14912

European Commission. (2011). *Special Eurobarometer: Attitudes on data protection and electronic identity in the European Union*. Brussels, Belgium: Publications Office of the European Union. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

European Commission. (2014). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union. Retrieved from http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

European Consumer Centre of Estonia. (2014). Trustmarks in Estonia. Retrieved October 9, 2014 from http://www.consumer.ee/trustmarks/

European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities.* (L 281, 23/11/1995 P. 0031 – 0050). Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

Federal Trade Commission. (2000a). Online profiling: A Federal Trade Commission report to Congress, Part 2. Retrieved from http://www.ftc.gov/reports/online-profiling-federal-trade-commission-report-congress-part-2

Federal Trade Commission. (2000b). Privacy online: Fair information practices in the electronic marketplace: A report to Congress. Retrieved from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Ferguson, M. A., Valenti, J. M., & Melwani, G. (1991). Communicating with risk takers: A public relations perspective. *Public Relations Research Annual, 3,* 195-224. doi: 10.1207/s1532754xjprr0301-4_10

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management, 5*(6), 1-10. doi: 10.5772/51645

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fiske, D. W. (1949). Consistency of the factorial structures of personality ratings from different sources. *The Journal of Abnormal and Social Psychology, 44*(3), 329-344. doi: 10.1037/h0057198

Fiske, S. T., & Taylor, S. E. (2013). *Social cognition: From brains to culture* (2nd Ed.). London, England: Sage.

Flaherty, G. G., & Fitzpatrick, J. J. (1978). Relaxation technique to increase comfort level of postoperative patients: A preliminary study. *Nursing Research, 27*(6), 352-355. doi: 10.1097/00006199-197811000-00006

Fox, S. (2013). 51% of US adults bank online. Washington, DC: Pew Internet and American Life Project. Retrieved May 7. 2014, from http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/

Freedom House. (2014). Estonia. Retrieved January 13, 2014, from http://www.freedomhouse.org/report/freedom-net/2012/estonia

Friedlander, W. J. (1982). The basis of privacy and autonomy in medical practice. A model. *Social Science & Medicine, 16*(19), 1709-1718. doi: 10.1016/0277-9536(82)90097-1

Friedman, U. (2013). Behold: The world's first digitally signed international agreement. *The Atlantic*. Retrieved January 23, 2014 from http://www.theatlantic.com/international/archive/2013/12/behold-the-worlds-first-digitally-signed-international-agreement/282582/

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal, 89*(3), 421-471. Retrieved from http://www.jstor.org/stable/795891

Gefen, D., & Heart, T. (2006). On the need to include national culture as a central issue in e-commerce trust beliefs. *Journal of Global Information Management, 14*(4), 1-30. doi: 10.4018/jgim.2006100101

Gentina, E., Butori, R., Rose, G. M., & Bakir, A. (2013). How national culture impacts teenage shopping behavior: Comparing French and American consumers. *Journal of Business Research, 67*(4), 464–470. doi: 10.1016/j.jbusres.2013.03.033

Gliner, J. A., Morgan, G. A., & Leech, N. L. (2009). *Research methods in applied settings: An integrated approach to design and analysis* (2nd ed.). New York, NY: Routledge.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy and Marketing, 10*(1), 149-166. Retrieved from http://www.jstor.org/stable/30000257

Gosling, S. D., Rentfrow, P. J., & Swann Jr, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality, 37*(6), 504-528. doi: 10.1016/S0092-6566(03)00046-1

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/07363760210433627

Griffin, J. J. (1991). The monitoring of electronic mail in the private sector workplace: An electronic assault on employee privacy rights. *Software Law Journal, 4*(3), 493-527.

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the US and in India. *Journal of Electronic Commerce Research, 11*(1), 41-52. Retrieved from http://www.questia.com/library/journal/1P3-1981541041/facilitating-global-e-commerce-a-comparison-of-consumers

Hallahan, K. (1999). Content class as a contextual cue in the cognitive processing of publicity versus advertising. *Journal of Public Relations Research, 11*(4), 293-320. doi: 10.1207/s1532754xjprr1104_02

Hamilton, J. (1989). Comfort and the hospitalized chronically ill. *Journal of Gerontological Nursing, 15*(4), 28-33. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/2708793

Harkness, J. (2003). Questionnaire translation. In J. Harkness, F. J. R. Van de Vijver & P. P. Mohler (Eds.), *Cross-cultural survey methods* (pp. 35-56). Hoboken, NJ: Wiley.

Harkness, J., Van de Vijver, F. J. R., & Johnson, T. P. (2003). Questionnaire design in comparative research. In J. Harkness, F. J. R. Van de Vijver & P. P. Mohler (Eds.), *Cross-cultural survey methods* (pp. 19-34). Hoboken, NJ: Wiley.

Henderson, S., & Gilding, M. (2004). 'I've never clicked this much with anyone in my life': Trust and hyperpersonal communication in online friendships. *New Media & Society, 6*(4), 487-506. doi: 10.1177/146144804044331

Herlihy, P. (2014). Government as a data model: What I learned in Estonia. Retrieved January 13, 2014, from http://digital.cabinetoffice.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

Hofstede, G. (2011). Dimensionalizing cultures: the Hofstede model in context. *Online Readings in Psychology and Culture, 2*(1), 8. Retrieved January 24, 2014, from http://dx.doi.org/10.9707/2307-0919.1014

Hofstede, G. (2014a). Estonia. Retrieved from http://geert-hofstede.com/estonia.html

Hofstede, G. (2014b). Dimensions [website]. Retrieved January 24, 2014, from http://geert-hofstede.com/dimensions.html

Horvitz, R. (2008, February 14). Where Wi-Fi is everywhere: Service-provision learnings from Estonia. *W2i Wireless Government Report.* Retrieved January 23, 2014, from http://w2i.com/resource_center/the_w2i_report__weekly_newsletter/news/p/id_199

IAPP—International Association of Privacy Professionals (2014). Glossary of privacy terms. Retrieved from https://privacyassociation.org/resources/privacy-glossary/personal-data/

Inselberg, K. (2013). Consumers wary of e-commerce. *Postimees*. Retrieved from http://news.postimees.ee/1322338/consumers-wary-of-e-commerce

International Telecommunication Union. (2013). The World in 2013: ICT facts and figures. Retrieved January 15, 2014, from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *Advances in Consumer Research, 3,* 382-383.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 0-0. doi: 10.1111/j.1083-6101.1999.tb00337.x

John, O. P., Donahue, E. M., & Kentle, R. L. (1991). *The Big Five Inventory-Versions 4a and 54.* Berkeley, CA: Institute of Personality and Social Research.

Johnson, C. (2007). Safeguarding against and responding to the breach of personally identifiable information. (M-07-16). Washington, DC: US Office of Management and Budget. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*(2), 177-192. doi: 10.1002/ejsp.36

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In A. N. Joinson, K. Mckenna, T. Postmes & U. D. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 237-252). New York, NY: Oxford University Press.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. doi: 10.1080/07370020903586662

Jones, J. M. (2014, August 12). Congressional job approval stays near historical lows. Gallup Poll. Retrieved August 27, 2014, from http://www.gallup.com/poll/174806/congressional-job-approval-stays-near-historical-low.aspx

Joreskog, K. G. (1970). *A general method for estimating a linear structural equation system*. Princeton, NJ: Educational Testing Service.

Kaasik, T., Andersson, R., & Horte, L. G. (1998). The effects of political and economic transitions on health and safety in Estonia: An Estonian-Swedish comparative study. *Social Science & Medicine, 47*(10), 1589-1599. doi: 10.1016/S0277-9536(98)00221-4

Kahn, J. H., & Hessling, R. M. (2001). Measuring the tendency to conceal versus disclose psychological distress. *Journal of Social and Clinical Psychology, 20*(1), 41-65. doi: 10.1521/jscp.20.1.41.22254

Kazdin, A. E. (2000). Anxiety. In *Encyclopedia of psychology*. (pp. 209-212). Washington, DC: Oxford University Press.

Keefer, P. T. (2012). How Estonia became a world leader in digital governance. Washington, DC: Aspen Institute. Retrieved January 23, 2014, from http://www.aspeninstitute.org/about/blog/how-estonia-became-world-leader-digital-governance

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564. Retrieved from http://dx.doi.org/10.1016/j.dss.2007.07.001

Klages, L. (1932). *The science of character*. Oxford, England: Sci-Art.

Kolcaba, K. Y. (1991). A taxonomic structure for the concept comfort. *Journal of Nursing Scholarship, 23*(4), 237-240. doi: 10.1111/j.1547-5069.1991.tb00678.x

Kolcaba, K. Y. (1992). Holistic comfort: Operationalizing the construct as a nurse-sensitive outcome. *Advances in Nursing Science, 15*(1), 1-10. Retrieved from http://journals.lww.com/advancesinnursingscience/abstract/1992/09000/holistic_comfort__operationalizing_the_construct.3.aspx

Kotler, P. (1988). *Marketing management: Analysis, planning, implementation, and control* (9th ed.). Englewood Cliffs, NJ: Prentice-Hall.

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009, August). *'It won't happen to me!': Self-disclosure in online social networks*. Paper presented at the Americas Conference on Information Systems, San Francisco, CA. Retrieved from http://www.icsi.berkeley.edu/pubs/other/itwont09.pdf

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109-125. doi:10.1057/JIT.2010.6

Krasnova, H., & Veltri, N. (2010, January 4-7). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. Paper presented at the Hawaii International Conference on System Sciences. Manoa, HI: University of Hawaii at Manoa. Retrieved from http://doi.ieeecomputersociety.org/10.1109/HICSS.2010.307

Laudon, K. C., & Traver, C. G. (2003). *E-commerce: Business,technology, society.* Upper Saddle River, NJ: Prentice Hall.

Ledbetter, A. M. (2009). Measuring online communication attitude: Instrument development and validation. *Communication Monographs, 76*(4), 463-486. doi: 10.1080/03637750903300262

Ledbetter, A. M., Broeckelman-Post, M. A., & Krawsczyn, A. M. (2011). Modeling everyday talk: Differences across communication media and sex composition of friendship dyads. *Journal of Social and Personal Relationships, 28*(2), 223-241. doi: 10.1177/0265407510377904

Ledbetter, A. M., Mazer, J. P., DeGroot, J. M., Meyer, K. R., Yuping Mao, & Swafford, B. (2011). Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness. *Communication Research, 38*(1), 27-53. doi: 10.1177/0093650210365537

Lee, M., & Turban, E. (2001). Trust in B-to-C electronic commerce: A proposed research model and its application. *International Journal of Electronic Commerce, 6*(1), 75-91.

Leggatt, H. (2013). Global ecommerce sales top US $1 trillion. *BizReport*. Retrieved January 22, 2014, from http://www.bizreport.com/2013/08/global-ecommerce-sales-top-us1-trillion.html

Levesque, M. J., Steciuk, M., & Ledley, C. (2002). Self-disclosure patterns among well-acquainted individuals: Disclosers, confidants and unique relationships. *Social Behavior and Personality, 30*(6), 579-592. doi: 10.2224/sbp.2002.30.6.579

Lewin, K. (1935). *A dynamic theory of personality*. New York, NY: McGraw-Hill.

Lewin, K. (1936). Some social-psychological differences between the United States and Germany. *Character and Personality, 4*(4), 265-293. doi: 10.1111/j.1467-6494.1936.tb02034.x

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. *Qualitative Market Research: An International Journal, 5*(4), 291-300. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/13522750210443245

Loiacono, E., Carey, D., Misch, A., Spencer, A., & Speranza, R. (2012, April). Personality impacts on self-disclosure behavior on social networking sites. Paper presented at the AMCIS 2012, Seattle, WA. Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/HCIStudies/6/

Mansel, T. (2014). How Estonia became E-stonia. BBC News. Retrieved March 15, 2014, from http://www.bbc.co.uk/news/business-22317297

Markel, M. (2005). The rhetoric of misdirection in corporate privacy-policy statements. *Technical Communication Quarterly, 14*(2), 197-214. doi: 10.1207/s15427625tcq1402_5

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods, 44*(1), 1-23. doi: 10.3758/s13428-011-0124-6

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734. doi: 10.5465/AMR.1995.9508080335

Mazer, J. P., & Ledbetter, A. M. (2012). Online communication attitudes as predictors of problematic Internet use and well-being outcomes. *Southern Communication Journal, 77*(5), 403-419. doi: 10.1080/1041794X.2012.686558

McAfee, Inc.(2014). International privacy and data protection laws [web page]. Retrieved February 4, 2014, from http://www.mcafee.com/us/regulations/international.aspx

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII): Recommendations of the National Institute of Standards and Technology*. Washington, DC: US Department of Commerce. [Special Publication 800-122]. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

McCoyd, J. L. M., & Kerson, T. S. (2006). Conducting intensive interviews using email: A serendipitous comparative opportunity. *Qualitative Social Work: Research and Practice, 5*(3), 389-406. doi: 10.1177/1473325006067367

McCrae, R. R., & John, O. P. (1992). An introduction to the five-factor model and its applications. *Journal of Personality, 60*(2), 175-215. doi: 10.1111/j.1467-6494.1992.tb00970.x

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

Merriam-Webster Dictionary. (2014a). Willing. Retrieved May 8, 2014, from http://www.merriam-webster.com/dictionary/willing

Merriam-Webster Dictionary. (2014b). Trust. Retrieved April 23, 2014, from http://www.merriam-webster.com/dictionary/trust

Merriam-Webster Dictionary. (2014c). Consciousness. Retrieved September 5, 2014, from http://www.merriam-webster.com/dictionary/consciousness

Mesch, G. S., & Beker, G. (2010). Are norms of disclosure of online and offline personal information associated with the disclosure of personal information online? *Human Communication Research, 36*(4), 570-592. doi: 10.1111/j.1468-2958.2010.01389.x

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 1-27. doi: 10.1111/j.1083-6101.2007.00328.x

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29. doi: 10.1002/dir.20009

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 12*(2), 206-215. Retrieved from http://www.jstor.org/stable/30000091

Moorman, C., Deshpandé, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of Marketing, 57*(1), 81-101. doi: 10.2307/1252059

Morse, J. (1983). An ethnoscientific analysis of comfort: A preliminary investigation. *Nursing Papers: Perspectives in Nursing, 15*(1), 6-19. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/6552516

Murphy, P. E., & Enis, B. M. (1986). Classifying products strategically. *Journal of Marketing, 50*(3), 24-42. doi: 10.2307/1251583

Murphy, S. (2011). Tax season: E-filing becomes the new normal. NBC News. Retrieved May 7, 2014, from http://www.nbcnews.com/id/42275764/ns/technology_and_science-tech_and_gadgets/t/tax-season-e-filing-becomes-new-normal/ - .U2pot17YjRg

Neal, E. (2009). Electronic transmission of PII policy. Washington, DC. U.S. Department of Commerce Office of the Chief Information Officer. Retrieved February 4, 2014, from http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240 - P38_752

Nelson, S. (2013). Tallinn: The former Soviet city that gave birth to Skype. National Public Radio. Retrieved January 24, 2014, from http://www.npr.org/blogs/parallels/2013/06/12/190693661/tallinn-the-former-soviet-city-that-gave-birth-to-skype

Nguyen, M., Bin, Y. S., & Campbell, A. (2012). Comparing online and offline self-disclosure: A systematic review. *CyberPsychology, Behavior & Social Networking, 15*(2), 103-111. doi: 10.1089/cyber.2011.0277

Nicol, A., & Pexman, P. (2010). *Presenting your findings: A practical guide for creating tables* (6th ed.). Washington, DC: American Psychological Association.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. doi: 10.1111/j.1745-6606.2006.00070.x

Norman, W. T. (1963). Toward an adequate taxonomy of personality attributes: Replicated factor structure in peer nomination personality ratings. *The Journal of Abnormal and Social Psychology, 66*(6), 574-583. doi: 10.1037/h0040291

Nosko, A., Wood, E., & Molema, S. (2010). 'All about me,' Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior, 26*(3), 406-418. doi: 10.1016/j.chb.2009.11.012

O'Cass, A., & Fenech, T. (2003). Web retailing adoption: Exploring the nature of Internet users web retailing behaviour. *Journal of Retailing and Consumer Services, 10*(2), 81-94. doi: 10.1016/S0969-6989(02)00004-8

Ohm, P. (2010). Broken promises of privacy: Responding to the suprising failure of anonymization. *UCLA Law Review, 57*(6), 1701-1777. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262. doi: 10.1016/S0167-4870(02)00172-1

Olson, P. (2014). Why Estonia has started teaching its first-graders to code. *Forbes.* Retrieved January 13, 2014, from http://www.forbes.com/sites/parmyolson/2012/09/06/why-estonia-has-started-teaching-its-first-graders-to-code/

Oommen, T. K. (1997). *Citizenship, nationality, and ethnicity: Reconciling competing identities*. Cambridge, UK: Blackwell.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon's Mechanical Turk. *Judgment and Decision Making, 5*(5), 411-419. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1626226

Park, J., Gunn, F., & Han, S.L. (2012). Multidimensional trust building in e-retailing: Cross-cultural differences in trust formation and implications for perceived risk. *Journal of Retailing and Consumer Services, 19*(3), 304-312. Retrieved from http://dx.doi.org/10.1016/j.jretconser.2012.03.003

Parloff, M. B., Kelman, H. C., & Frank, J. D. (1954). Comfort, effectiveness, and self-awareness as criteria of improvement in psychotherapy. *American Journal of Psychiatry, 111*(5), 343-352. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/13197596

Pavlou, P. A. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 69-103. doi: 10.1.1.86.7139

Pavlou, P., & Chellappa, R. (2001). The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. *Information System Research, 11*, 18-36.

Petronio, S. (2002). *Boundaries of privacy dialectics of disclosure*. Albany, NY: SUNY Press.

Petronio, S., & Durham, W. (2008). Communication privacy management theory. In L. Baxter & D. Braithewaite (Eds.), *Engaging theories in interpersonal communication: Multiple perspectives.* (pp. 309-322). Thousand Oaks, CA: Sage Publications.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41. doi: 10.2307/30000485

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

Plaisance, P. L. (2009). *Media ethics: Key principles for responsible practice*. Los Angeles, CA: Sage.

Poritz, J. A. (2007). Who searches the searchers? Community privacy in the age of monolithic search engines. *Information Society, 23*(5), 383-389. doi: 10.1080/01972240701572921

Prensky, M. (2001). Digital natives, digital immigrants: Part 1. *On the horizon, 9*(5), 1-6. http://dx.doi.org/10.1108/10748120110424843

Privireal—Privacy in Research Ethics & Law. (2005). Estonia - Data protection. Sheffield, UK: University of Sheffield Department of Law. Retrieved January 24, 2014, from http://www.privireal.org/content/dp/estonia.php

Punyanunt-Carter, N. (2006). An analysis of college students' self-disclosure behaviors on the Internet. *College Student Journal, 40*(2), 329-331. Retrieved from http://eric.ed.gov/?id=EJ765329

Quested, T. (2014). Cambridge technology fights massive password theft. *Business Weekly* [UK]. Retrieved February 11, 2013, from http://www.businessweekly.co.uk/hi-tech/16483-cambridge-technology-fights-mass-password-theft

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. Washington, DC: Pew Internet and American Life Project. Retrieved May 7, 2014, from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of Research in Personality, 41*(1), 203-212. Retrieved from http://dx.doi.org/10.1016/j.jrp.2006.02.001

Rawls, J. (2001). *Justice as fairness: A restatement*. Cambridge, MA: Harvard University Press. Retrieved from http://www.usatoday.com/story/cybertruth/2014/01/23/payment-card-data-theft-jumps-five-fold/4796685/

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM, 40*(8), 92-100. doi: 10.1145/257874.257896

Rokeach, M. (1968). *Beliefs, attitudes and values: A theory of organization and change*. San Francisco, CA: Jossey-Bass.

Rooney, B. (2013). Estonia: The role model for tech-enabled states. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887323477604578653792712743194#livefyre-comment

Rose, R. (2003, September). *The dynamics of digital choice.* Paper presented at the Information, Communication, Society Symposium, University of Oxford, Oxford: UK.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with facebook use. *Computers in Human Behavior, 25*(2), 578-586. doi: 10.1016/j.chb.2008.12.024

Royal Academy of Engineering. (2011). *Smart infrastructure: The future*. London, England.

Ryckman, R. (2012). *Theories of personality*. Belmont, CA: Wadsworth, Cengage Learning.

Salam, A. F., Rao, H. R., & Pegels, C. C. (2003). Consumer-perceived risk in e-commerce transactions. *Communications of the ACM, 46*(12), 325-331. doi: 10.1145/953460.953517

Schaar, A. K., Valdez, A. C., & Ziefle, M. (2013). The impact of user diversity on the willingness to disclose personal information in social network services. In A. Holzinger, M. Ziefle, M. Hitz & M. Debevc (Eds.), *Human factors in computing and informatics* (Vol. 7946, pp. 174-193). Berlin, Germany: Springer.

Schmitt, D. P., Allik, J., McCrae, R. R., & Benet-Martínez, V. (2007). The geographic distribution of Big Five personality traits: Patterns and profiles of human self-description across 56 nations. *Journal of Cross-Cultural Psychology, 38*(2), 173-212. doi: 10.1177/0022022106297299

Scott, C. R. (2004). Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations. *Free Speech Yearbook, 41*, 127-141. doi:10.1080/08997225.2004.10556309

SDL plc. (2014). Marketing data and consumer privacy: What your customers really think. Maidenhead, England: SDL Globe House. Retrieved May 7, 2014, from http://www.sdl.com/campaign/2014_Data_and_Privacy_Survey.html

Seminerio, M. (1998). E-commerce: Progress or pitfalls? Depends on government, experts say. ZDnet. Retrieved January 23, 2014, from http://www.zdnet.com/news/e-commerce-progress-or-pitfalls-depends-on-government-experts-say/100323

Sessler, J. B. (1997). Computer cookie control: Transaction generated information and privacy regulation on the Internet. *Journal of Law and Policy, 5*, 627-677. Retrieved from https://litigation-

essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=5+J.L.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73. doi: 10.2307/30000488

Shih, H.-P. (2004). An empirical study on predicting user acceptance of e-shopping on the Web. *Information & Management, 41*(3), 351-368. Retrieved from http://dx.doi.org/10.1016/S0378-7206(03)00079-X

Siefert, M. L. (2002). Concept analysis of comfort. *Nursing Forum, 37*(4), 16-23. doi: 10.1111/j.1744-6198.2002.tb01288.x

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce, 10*(1), 1-16. doi: 10.1080/15332861.2011.558454

Sprecher, S., & Hendrick, S. S. (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social and Clinical Psychology, 23*(6), 857-877. doi: 10.1521/jscp.23.6.857.54803

Steinhauser, P. (2014, August 8). CNN Poll: Trust in government at all time low. CNN Poll. Retrieved October 7, 2014, from http://politicalticker.blogs.cnn.com/2014/08/08/cnn-poll-trust-in-government-at-all-time-low-2/

Suler, J. (2002). Identity management in cyberspace. *Journal of Applied Psychoanalytic Studies, 4*(4), 455-459. doi: 10.1023/a:1020392231924

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321-326. doi: 10.1089/1094931041291295

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. doi: 10.1111/jcc4.12052

Tarbijakaitseamet. (2014). E-poed kes ei täida seadusest tulenevaid nõudeid [E-shops who do not comply with the statutory requirements]. Retrieved October 9, 2014 from http://www.tarbijakaitseamet.ee/et/ametist/e-poed-kes-ei-taida-seadusest-tulenevaid-noudeid

Taylor, J. W. (1974). The role of risk in consumer behavior. *Journal of Marketing, 38*(2), 54-60. Retrieved from http://www.jstor.org/stable/1250198

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication efects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*(3), 317-348. doi: 10.1111/j.1468-2958.2002.tb00811.x

Torney-Purta, J., Barber, C. H., & Richardson, W. K. (2004). Trust in government-related institutions and political engagement among adolescents in six countries. *Acta Politica, 39*(4), 380-406. doi:10.1057/palgrave.ap.5500080

Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure: Results from three countries. *Journal of Global Information Management, 19*(4), 76-94. doi: 10.4018/jgim.2011100104

Trimpop, R. (1994). *The psychology of risk-taking behavior*. Amsterdam, Nethlands: North-Holland.

Trumbo, C. (2012). Communicating the significance of risk. In J. K. Gilbert & S. M. Stocklmayer (Eds.), *Communication and engagement with science and technology: Issues and dilemmas: A reader in science communication* (pp. 93-109). New York, NY: Routledge.

Tupes, E. C., & Christal, R. E. (1992). Recurrent personality factors based on trait ratings. *Journal of Personality, 60*(2), 225-251. doi: 10.1111/j.1467-6494.1992.tb00973.x

United States Department of Health and Human Services. (2014). The Department of Health and Human Services privacy awareness training. Retrieved February 4, 2014, from http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/privacyawarenesstraining.pdf

United States General Services Administration. (2013). *Personally identifiable information (PII).* Retrieved February 6, 2014, from http://www.gsa.gov/portal/content/104256

United States Government Accountability Office. (2008). *Privacy: Alternatives exist for enhancing protection of personally identifiable information*. (GAO-08-536). Retrieved from http://www.gao.gov/new.items/d08536.pdf.

Uslaner, E. M. (2004). Trust, civic engagement, and the Internet. *Political Communication, 21*(2), 223-242. doi: 10.1080/10584600490443895

Van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems, 12*(1), 41-48. doi: 10.1057/palgrave.ejis.3000445

Varadarajan, P. R., & Yadav, M. S. (2002). Marketing strategy and the internet: An organizing framework. *Journal of the Academy of Marketing Science, 30*(4), 296-312. doi: 10.1177

VisitEstonia.com. (2014a*).* Facts about Estonia [web page]. Retrieved January 13, 2014, from http://www.visitestonia.com/en/articles/195DO

VisitEstonia.com. (2014b). World beating Estonia. Retrieved January 13, 2014, from http://www.visitestonia.com/en/news/319

Wallace, P. (2001). *The psychology of the Internet*. New York, NY: Cambridge University Press.

Walrave, M., & Heirman, W. (2012). Adolescents, online marketing and privacy: Predicting adolescents' willingness to disclose personal information for marketing purposes. *Children & Society, 27*(6), 1-14. doi: 10.1111/j.1099-0860.2011.00423.x

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1), article 1. doi: 10.5817/CP2012-1-3

Walther, J. B. (2011). Theories of computer-mediated communication and interpersonal relations. In M. L. Knapp & J. A. Daly (Eds.), *The Sage handbook of interpersonal communication* (pp. 443-479). Thousand Oaks, CA: SAGE Publications.

Walther, J. B., Pingree, S., Hawkins, R. P., & Buller, D. B. (2005). Attributes of interactive online health information systems. *Journal of Medical Internet Research, 7*(3), e33. doi:10.2196/jmir.7.3.e33

Wang, H. (2011). *Protecting privacy in China*. Berlin, Germany: Springer.

Warren, S. V., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220. Retrieved from http://www.jstor.org/stable/1321160

Warshaw, P. R., & Davis, F. D. (1985). Disentangling behavioral intention and behavioral expectation. *Journal of Experimental Social Psychology, 21*, 213-228. doi: 10.1016/0022-1031(85)90017-4

Wei, M., Russell, D. W., & Zakalik, R. A. (2005). Adult attachment, social self-efficacy, self-disclosure, loneliness, and subsequent depression for freshman college students: A longitudinal study. *Journal of Counseling Psychology, 52*(4), 602-614. doi: 10.1037/0022-0167.52.4.602

Westin, A. (1967). *Privacy and freedom.* New York, NY: Atheneum.

Westin, A. (1984). The origins of modern claims to privacy. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy* (pp. 56-74). Cambridge, England: Cambridge University Press.

Wheeless, L. (1976). Self-disclosure and interpersonal solidarity: Measurement, validation, and relationships. *Human Communication Research, 3*(1), 47-67. doi: 10.1111/j.1468-2958.1976.tb00503.x

Wheeless, L., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 339-346.

Wheeless, L. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research, 4*, 143-157. doi: 10.1111/j.1468-2958.1978.tb00604.x

Wiedemanni Translation Company. (2014a). 15038:2006 Certification [web page]. Retrieved April 24, 2014, from http://www.wiedemanni.ee/en/about-the-company/150382006-certification/

Wiedemanni Translation Company. (2014b). Our quality [web page]. Retrieved April 24, 2014, from http://www.wiedemanni.ee/en/our-quality/

Windham, C. (2005). Father Google and mother IM: Confessions of a Net Gen learner. *Educause Review, 40*(5), 43-58.

Wolfradt, U., & Doll, J. (2001). Motives of adolescents to use the Internet as a function of personality traits, personal and social factors. *Journal of Educational Computing Research, 24*(1), 13-27. doi: 10.2190/anpm-ln97-aut2-d2ej

Woodard, C. (2003). Estonia, where being wired is a human right. *Christian Science Monitor.* Retrieved January 23, 2014, from http://www.csmonitor.com/

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science & Technology, 58*(5), 710-722. doi: 10.1002/asi.20530

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior, 11*(6), 763-765. doi: 10.1089/cpb.2007.0240

Zuckerman, M. (1988). Behavior and biology: Research on sensation seeking and reactions to the media. In L. Donohew, H. E. Sypher & E. T. Higgins (Eds.), *Communication, social cognition, and affect* (pp. 173-194). Hillsdale, NJ: Erlbaum.

APPENDIX A: Mturk HIT assignment directions and Informed Consent statement

Thank you for participating in this 15-minute survey about sharing personal information during e-commerce transactions. Your answers are important to us, and we need truthful ones. Compensation will be based on quality of survey completion, including careful reading of all questions, and taking your time as you work through the survey.

INFORMED CONSENT

Title: Sharing Online Information in Ecommerce

About the Research: This study seeks to gain insights into individual's attitudes toward providing personal information during online ecommerce purchases. This study is being conducted by the Department of Journalism and Technical Communication at Colorado State University USA. The Principal Investigator is Dr. Kirk Hallahan and the Co-Principal Investigator is Cory Robinson.

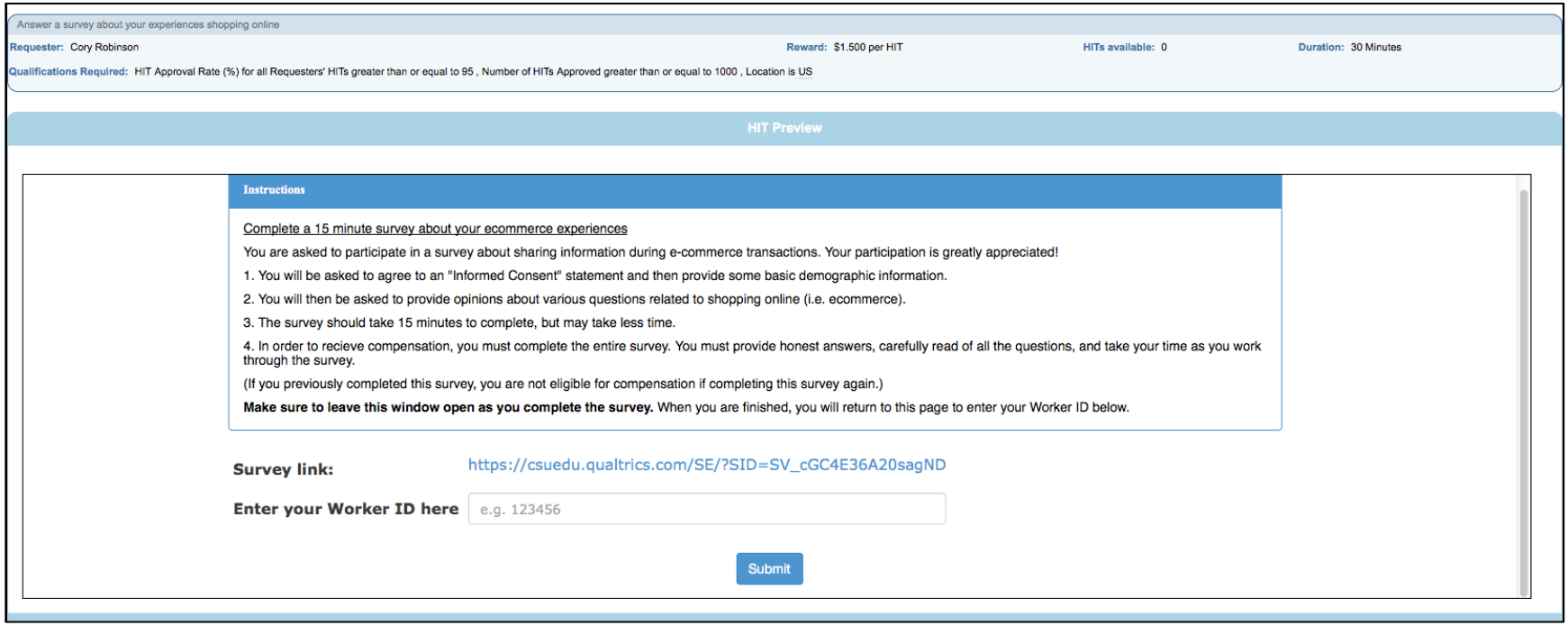
It will take only about 15 minutes to complete. The survey is anonymous and voluntary, and you may withdraw at any point.

All data will be reported in aggregate; we will not share any personal information about you. Although there are no direct benefits to you, we hope to gain more knowledge on individual's attitude toward sharing personal information during ecommerce transactions. There are no known risks involved in completing this survey. You will be compensated $1.50 for completion of the survey.

For questions about the study, contact Cory Robinson at cory.robinson@colostate.edu. For questions about your rights as a volunteer in this research, contact Colorado State's Institutional Review Board at ricro_irb@mail.colostate.edu; or +1 970-491-1553.

Consent: By clicking "I agree" below, you are confirming that you a) have read the above information, b) you voluntarily agree to participate, and c) are at least 18 years of age.

APPENDIX B: Overview of Mturk HIT assignment details



APPENDIX C: English Survey Instrument

All information you provide will be kept strictly confidential. First, please tell us about yourself.

Have you purchased at least one product or service online?
- ❍ Yes
- ❍ No

Which country do you reside:
- ❍ USA
- ❍ Other

Your gender?
- ❍ Male
- ❍ Female
- ❍ Other

Your age in years?

Highest level of education you have completed:
- ❍ Some High School
- ❍ High School
- ❍ Some College
- ❍ College Degree
- ❍ Some Graduate School
- ❍ Graduate School

Ecommerce is the buying and selling of goods and services on the Internet. Choose the number that best reflects your proficiency or experience with purchasing goods or services online.
- ❍ Beginner 1
- ❍ 2
- ❍ 3
- ❍ Neutral 4
- ❍ 5
- ❍ 6
- ❍ Expert 7

This set of statements is about your opinions using the Internet.

For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.

	Strongly disagree 1	2	3	Neutral 4	5	6	Strongly agree 7
The Internet is a safe environment in which to exchange information with others.	❍	❍	❍	❍	❍	❍	❍
The Internet is a reliable environment in which to conduct business transactions or personal purchases.	❍	❍	❍	❍	❍	❍	❍
Internet merchants are dependable.	❍	❍	❍	❍	❍	❍	❍
The Internet can be trusted.	❍	❍	❍	❍	❍	❍	❍

This set of statements is about purchasing goods or services from online merchants. Think in general about your previous experiences purchasing goods or services online.

For each of the following pairs of adjectives, select the number that best describes your feelings:

How would you characterize a decision of whether to buy a product from an online retailer?

	1	2	3	4	5	6	7	
Significant opportunity	❍	❍	❍	❍	❍	❍	❍	Significant risk
High potential for loss	❍	❍	❍	❍	❍	❍	❍	High potential for gain
Very positive situation	❍	❍	❍	❍	❍	❍	❍	Very negative situation

This set of statements is about purchasing goods or services from online merchants. Think in general about your previous experiences purchasing goods or services online.

For each of the following pairs of adjectives, select the number that best describes your feelings:

What is the likelihood of finding a bargain by purchasing a good or service online?

	1	2	3	4	5	6	7	
Very unlikely	❍	❍	❍	❍	❍	❍	❍	Very likely
Probable	❍	❍	❍	❍	❍	❍	❍	Not probable
Happens all the time	❍	❍	❍	❍	❍	❍	❍	Never happens

This set of statements is about you and your personality.

For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.

How well do the following statements describe your personality?

	Strongly disagree 1	2	3	Neutral 4	5	6	Strongly agree 7
... is talkative	❍	❍	❍	❍	❍	❍	❍
... is generally trusting	❍	❍	❍	❍	❍	❍	❍
... does a thorough job	❍	❍	❍	❍	❍	❍	❍
... is relaxed, handles stress well	❍	❍	❍	❍	❍	❍	❍
... is inventive	❍	❍	❍	❍	❍	❍	❍
... is outgoing, sociable	❍	❍	❍	❍	❍	❍	❍
... is considerate and kind to almost everyone	❍	❍	❍	❍	❍	❍	❍
... does things efficiently	❍	❍	❍	❍	❍	❍	❍
... gets nervous easily	❍	❍	❍	❍	❍	❍	❍
... has an active imagination	❍	❍	❍	❍	❍	❍	❍
... is reserved	❍	❍	❍	❍	❍	❍	❍
... tends to	❍	❍	❍	❍	❍	❍	❍

find fault with others							
... tends to be disorganized	❍	❍	❍	❍	❍	❍	❍
... worries a lot	❍	❍	❍	❍	❍	❍	❍
... is curious about many different things	❍	❍	❍	❍	❍	❍	❍
... is shy, inhibited	❍	❍	❍	❍	❍	❍	❍
... likes to cooperate with others	❍	❍	❍	❍	❍	❍	❍
... tends to be lazy	❍	❍	❍	❍	❍	❍	❍
... can be tense	❍	❍	❍	❍	❍	❍	❍
... is original, has new ideas	❍	❍	❍	❍	❍	❍	❍

This set of statements is about your opinions of various public institutions.

For each of the following statements, please indicate the extent to which you disagree or agree where 1 = never and 7 = always.

How much of the time can you trust each of the following institutions?

	Never 1	2	3	Sometimes 4	5	6	Always 7
National government	❍	❍	❍	❍	❍	❍	❍
Local government	❍	❍	❍	❍	❍	❍	❍
Local businesses	❍	❍	❍	❍	❍	❍	❍
International businesses	❍	❍	❍	❍	❍	❍	❍

This set of statements is about you.

For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.

	Strongly disagree 1	2	3	Neutral 4	5	6	Strongly agree 7
I often act on the spur of the moment.	❍	❍	❍	❍	❍	❍	❍
I quite enjoy taking risks.	❍	❍	❍	❍	❍	❍	❍
I’m willing to take some risks.	❍	❍	❍	❍	❍	❍	❍
I’m an adventurous person.	❍	❍	❍	❍	❍	❍	❍
I welcome new and exciting experiences.	❍	❍	❍	❍	❍	❍	❍

When purchasing goods or services online, people are asked to provide personal information in order to complete the purchase.

Please indicate your level of willingness to share each of the following types of personal information online when purchasing goods or services where 1 = not willing and 7 = very willing.

	Not willing 1	2	3	Neutral 4	5	6	Very willing 7
Name	❍	❍	❍	❍	❍	❍	❍
Home address	❍	❍	❍	❍	❍	❍	❍
Phone number	❍	❍	❍	❍	❍	❍	❍
Work address (if applicable)	❍	❍	❍	❍	❍	❍	❍
Work phone number	❍	❍	❍	❍	❍	❍	❍
Email address	❍	❍	❍	❍	❍	❍	❍
Date of birth	❍	❍	❍	❍	❍	❍	❍
Credit card number	❍	❍	❍	❍	❍	❍	❍
Annual income	❍	❍	❍	❍	❍	❍	❍
PayPal account	❍	❍	❍	❍	❍	❍	❍
Credit history	❍	❍	❍	❍	❍	❍	❍
Medical history	❍	❍	❍	❍	❍	❍	❍
Marital status	❍	❍	❍	❍	❍	❍	❍
Age	❍	❍	❍	❍	❍	❍	❍
Twitter username	❍	❍	❍	❍	❍	❍	❍

Facebook profile	❍	❍	❍	❍	❍	❍	❍
Skype username	❍	❍	❍	❍	❍	❍	❍

Websites sometimes offer coupons or discounts in exchange for providing personal information, such as your email address or phone number. Below are some benefits that might be received in exchange for your personal information.

For each of the following statements, please indicate your level of willingness to provide information to companies where 1 = not willing and 7 = very willing.

	Not willing 1	2	3	Neutral 4	5	6	Very willing 7
The company tailors their product offerings to my tastes.	❍	❍	❍	❍	❍	❍	❍
The company sends me special discounts on merchandise.	❍	❍	❍	❍	❍	❍	❍
It will help me save time when I make my next purchase from the same site.	❍	❍	❍	❍	❍	❍	❍
I can get better customer service from the company.	❍	❍	❍	❍	❍	❍	❍
It will provide a greater merchandise selection.	❍	❍	❍	❍	❍	❍	❍
The company website clearly states	❍	❍	❍	❍	❍	❍	❍

how my personal information will be used.							
The company website lets me know that they respect my privacy rights.	❍	❍	❍	❍	❍	❍	❍
I always know the purpose of the information being collected.	❍	❍	❍	❍	❍	❍	❍
I have a choice in whether my personal information should be disclosed to a third party.	❍	❍	❍	❍	❍	❍	❍
At any time, I can delete or edit my personal information.	❍	❍	❍	❍	❍	❍	❍

When purchasing goods or services online, people are asked to provide personal information in order to complete the purchase.

Please indicate the level of risk you perceive exists when you might share each of the following types of personal information online when purchasing goods or services where 1 = very risky and 7 = not risky.

	Very risky 1	2	3	Neutral 4	5	6	Not risky 7
Name	❍	❍	❍	❍	❍	❍	❍
Home address	❍	❍	❍	❍	❍	❍	❍
Phone number	❍	❍	❍	❍	❍	❍	❍
Work address (if applicable)	❍	❍	❍	❍	❍	❍	❍
Work phone number	❍	❍	❍	❍	❍	❍	❍
Email address	❍	❍	❍	❍	❍	❍	❍
Date of birth	❍	❍	❍	❍	❍	❍	❍
Credit card number	❍	❍	❍	❍	❍	❍	❍
Annual income	❍	❍	❍	❍	❍	❍	❍
PayPal account	❍	❍	❍	❍	❍	❍	❍
Credit history	❍	❍	❍	❍	❍	❍	❍
Medical history	❍	❍	❍	❍	❍	❍	❍
Marital status	❍	❍	❍	❍	❍	❍	❍
Age	❍	❍	❍	❍	❍	❍	❍
Twitter username	❍	❍	❍	❍	❍	❍	❍

Facebook profile	❍	❍	❍	❍	❍	❍	❍
Skype username	❍	❍	❍	❍	❍	❍	❍

Think back to a time when you were completing an information request form online, such as when you were purchasing a product or making a reservation for a hotel or restaurant.

For each of the following statements, please indicate the extent to which you disagree or agree where 1 = strongly disagree and 7 = strongly agree.

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

This set of statements is about how you would feel when providing personal information online.

For each of the following pairs of adjectives, select the number that best describes your feelings.

I would describe providing information online as:

	1	2	3	4	5	6	7	
Risky	❍	❍	❍	❍	❍	❍	❍	Safe
Trustworthy	❍	❍	❍	❍	❍	❍	❍	Untrustworthy
Unreliable	❍	❍	❍	❍	❍	❍	❍	Reliable
Bad	❍	❍	❍	❍	❍	❍	❍	Good
Unimportant	❍	❍	❍	❍	❍	❍	❍	Necessary
Not valuable	❍	❍	❍	❍	❍	❍	❍	Valuable
Always willing	❍	❍	❍	❍	❍	❍	❍	Never willing

APPENDIX D: Estonian participant survey directions and Informed Consent statement

Thank you for participating in this 10-minute survey about sharing personal information during ecommerce transactions. Your answers are important to us, and we need truthful ones.

INFORMED CONSENT

Title: Sharing Online Information in Ecommerce

About the Research: This study seeks to gain insights into individual's attitudes toward providing personal information during online ecommerce purchases. This study is being conducted by the Department of Journalism and Technical Communication at Colorado State University USA. The Principal Investigator is Dr. Kirk Hallahan and the Co-Principal Investigator is Cory Robinson.

It will take only about 10 minutes to complete. The survey is anonymous and voluntary, and you may withdraw at any point.

All data will be reported in aggregate; we will not share any personal information about you. Although there are no direct benefits to you, we hope to gain more knowledge on individual's attitudes toward sharing personal information during ecommerce transactions. There are no known risks involved in completing this survey.

For questions about the study, contact Cory Robinson at cory.robinson@colostate.edu. For questions about your rights as a volunteer in this research, contact Colorado State's Institutional Review Board at ricro_irb@mail.colostate.edu; or +1 970-491-1553.

Consent: By clicking "I Agree", you are confirming that you a) have read the above information, b) voluntarily agree to participate, and c) are at least 18 years of age.

APPENDIX E: Estonian Survey Instrument

Aitäh, et osalete selles 10 minutit võtvas uuringus isiklike andmete jagamise kohta e-kaubanduse tehingute sooritamisel. Teie vastused on meie jaoks olulised ja me palume teil vastata ausalt.

INFORMEERITUD NÕUSOLEK
Pealkiri: Andmete jagamine Internetis e-kaubanduse keskkondades (Sharing Online Information in Ecommerce)

Uuringust: Uuringu eesmärk on selgitada välja inimeste suhtumine isiklike andmete edastamisse e-kaubanduse keskkondades ostude sooritamise käigus. Uuringu korraldaja on USA Colorado osariigi ülikooli (USA Colorado State University) ajakirjanduse ja tehnilise kommunikatsiooni osakond. Uuringu juht on doktor Kirk Hallahan ja tema abiline on Cory Robinson.

Küsimustikule vastamine võtab aega umbes 10 minutit. Küsitlus on anonüümne ja vabatahtlik, võite küsimustele vastamise igal hetkel katkestada.

Kõiki andmeid käsitletakse koondandmete vormis, teie isiku kohta ei jagata mingit teavet. Kuigi uuringuga ei kaasne teie jaoks mingit otsest kasu, loodame selle abiga saada parema ülevaate inimeste suhtumisest oma andmete jagamisse e-kaubanduse tehingute käigus. Küsimustikule vastamisega ei kaasne teadaolevalt mingeid riske.

Küsimustele uuringu kohta vastab Cory Robinson, meiliaadress cory.robinson@colostate.edu. Kui teil on küsimusi oma õiguste kohta selles küsitluses vabatahtliku osalejana, vastab neile Colorado osariigi ülikooli eetikakomitee (Colorado State's Institutional Review Board), meiliaadress ricro_irb@mail.colostate.edu; or +1 970-491-1553.

Nõusolek: Klõpsates „Nõustun“, kinnitate, et a) te olete ülaltoodud informatsiooni läbi lugenud, b) te olete nõus vabatahtlikult osalema ja c) te olete vähemalt 18-aastane.

- ❍ Nõustun
- ❍ Ei nõustu

Kogu teie poolt edastatud teabe konfidentsiaalsus tagatakse. Rääkige palun kõigepealt endast.

Kas olete Internetist ostnud vähemalt ühe kauba või teenuse?
- ❍ Jah
- ❍ Ei

Millises riigis te elate:
- ❍ Eesti
- ❍ Muu

Teie sugu?
- ❍ Mees
- ❍ Naine
- ❍ Muu

Teie vanus aastates?

Teie kõrgeim lõpetatud haridustase:
- ❍ Käinud keskkoolis
- ❍ Lõpetanud keskkooli
- ❍ Käinud kõrgkoolis
- ❍ Kraad kõrgkoolist
- ❍ Käinud magistriõppes
- ❍ Läbinud magistriõppe

E-kaubandus on kaupade ja teenuste ostmine ja müük Internetis. Valige number mis kirjeldab kõige paremini teie vilumust või kogemust Intenetist kaupade või teenuste ostmisel.
- ❍ Algaja 1
- ❍ 2
- ❍ 3
- ❍ Keskmine 4
- ❍ 5
- ❍ 6
- ❍ Asjatundja 7

Need väited puudutavad teie arvamust Interneti kasutamise kohta.

Märkige palun iga väite juures ära, millisel määral te sellega nõustute või ei nõustu, kusjuures 1 = olen kindlasti vastu ja 7 = nõustun kindlasti.

	Olen kindlasti vastu 1	2	3	Neutraalne 4	5	6	Olen kindlasti nõus 7
Internet on teiste inimestega informatsiooni vahetamiseks turvaline keskkond.	❍	❍	❍	❍	❍	❍	❍
Internet on usaldusväärne keskkond äritehingute või isiklike ostude sooritamiseks.	❍	❍	❍	❍	❍	❍	❍
Interneti-kaupmehed on usaldusväärsed.	❍	❍	❍	❍	❍	❍	❍
Internetti võib usaldada.	❍	❍	❍	❍	❍	❍	❍

Need väited puudutavad kaupade või teenuste ostmist Interneti-kaupmeestelt. Mõelge üldiselt oma seniste kogemuste peale kaupade või teenuste Internetist ostmisel.

Valige iga järgneva omadussõnade paari kohta välja number, mis teie tundeid kõige paremini väljendab:

Kuidas kirjeldaksite otsust, kas osta mingi toode Interneti-müüja käest?

	1	2	3	4	5	6	7	
Märkimisväärne võimalus	❍	❍	❍	❍	❍	❍	❍	Märkimisväärne risk
Suur võimalus saada kahju	❍	❍	❍	❍	❍	❍	❍	Suur võimalus saada kasu
Väga positiivne olukord	❍	❍	❍	❍	❍	❍	❍	Väga negatiivne olukord

Need väited puudutavad kaupade või teenuste ostmist Interneti-kaupmeestelt. Mõelge üldiselt oma seniste kogemuste peale kaupade või teenuste Intenetist ostmisel.

Valige iga järgneva omadussõnade paari kohta välja number, mis teie tundeid kõige paremini väljendab:

Kui suur on tõenäosus, et Internetist kaupa või teenust ostes leiate hea pakkumise?

	1	2	3	4	5	6	7	
Väga ebatõenäoline	❍	❍	❍	❍	❍	❍	❍	Väga tõenäoline
Tõenäoline	❍	❍	❍	❍	❍	❍	❍	Ebatõenäoline
Seda juhtub pidevalt	❍	❍	❍	❍	❍	❍	❍	Seda ei juhtu kunagi

Need väited puudutavad teid ja teie isiksust.

Märkige palun iga väite juures ära, millisel määral te sellega nõustute või ei nõustu, kusjuures 1 = olen kindlasti vastu ja 7 = nõustun kindlasti.

Kui hästi kirjeldavad järgmised väited teie isiksust?

	Olen kindlasti vastu 1	2	3	Neutraalne 4	5	6	Olen kindlasti nõus 7
... on jutukas	❍	❍	❍	❍	❍	❍	❍
... on üldiselt usaldav	❍	❍	❍	❍	❍	❍	❍
... teeb kõike põhjalikult	❍	❍	❍	❍	❍	❍	❍
... on muretu, saab stressiga hästi hakkama	❍	❍	❍	❍	❍	❍	❍
... on leidlik	❍	❍	❍	❍	❍	❍	❍
... on sotsiaalne, hea suhtleja	❍	❍	❍	❍	❍	❍	❍
... on tähelepanelik ja lahke peaaegu kõigi vastu	❍	❍	❍	❍	❍	❍	❍
... teeb kõike tõhusalt	❍	❍	❍	❍	❍	❍	❍
... muutub kergesti närviliseks	❍	❍	❍	❍	❍	❍	❍
... on hea fantaasiaga	❍	❍	❍	❍	❍	❍	❍
... on vaoshoitud	❍	❍	❍	❍	❍	❍	❍
... kipub süüdistama teisi	❍	❍	❍	❍	❍	❍	❍
... kaldub	❍	❍	❍	❍	❍	❍	❍

lohakusele							
... muretseb palju	❍	❍	❍	❍	❍	❍	❍
... tunneb huvi paljude erinevate asjade vastu	❍	❍	❍	❍	❍	❍	❍
... on uje, tagasihoidlik	❍	❍	❍	❍	❍	❍	❍
... armastab teistega koostööd teha	❍	❍	❍	❍	❍	❍	❍
... kipub olema laisk	❍	❍	❍	❍	❍	❍	❍
... võib olla pinges	❍	❍	❍	❍	❍	❍	❍
... on originaalne, tulvil uusi ideid	❍	❍	❍	❍	❍	❍	❍

Need väited puudutavad teie arvamust mitmesuguste avalike institutsioonide kohta.

Märkige palun iga väite juures ära, millisel määral te sellega nõustute või ei nõustu, kusjuures 1 = mitte kunagi ja 7 = alati.

Millisel määral saab järgnevaid institutsioone usaldada?

	Mitte kunagi 1	2	3	Mõnikord 4	5	6	Alati 7
Keskvalitsus	❍	❍	❍	❍	❍	❍	❍
Kohalik omavalitsus	❍	❍	❍	❍	❍	❍	❍
Kohalik ettevõte	❍	❍	❍	❍	❍	❍	❍
Rahvusvaheline ettevõte	❍	❍	❍	❍	❍	❍	❍
Euroopa Liit	❍	❍	❍	❍	❍	❍	❍

Need väited puudutavad teid.

Märkige palun iga väite juures ära, millisel määral te sellega nõustute või ei nõustu, kusjuures 1 = olen kindlasti vastu ja 7 = nõustun kindlasti.

	Olen kindlasti vastu 1	2	3	Neutraalne 4	5	6	Olen kindlasti nõus 7
Tegutsen tihti hetke ajel.	❍	❍	❍	❍	❍	❍	❍
Mulle üpriski meeldib riskida.	❍	❍	❍	❍	❍	❍	❍
Ma olen vahel nõus riskima.	❍	❍	❍	❍	❍	❍	❍
Olen seiklushimuline inimene.	❍	❍	❍	❍	❍	❍	❍
Mulle meeldivad uued ja põnevad kogemused.	❍	❍	❍	❍	❍	❍	❍

Internetis kaupade või teenuste ostmisel küsitakse inimestelt tellimuse vormistamiseks isikuandmeid.

Palun näidake ära oma valmisolek iga järgneva andmetüübi jagamiseks Internetis kaupade või teenuste ostmisel, kusjuures 1 = ei ole valmis ja 7 = olen täielikult valmis.

	Ei ole valmis 1	2	3	Neutraalne 4	5	6	Olen täielikult valmis 7
Nimi	❍	❍	❍	❍	❍	❍	❍
Kodune aadress	❍	❍	❍	❍	❍	❍	❍
Telefoninumber	❍	❍	❍	❍	❍	❍	❍
Töökoha aadress (kui on)	❍	❍	❍	❍	❍	❍	❍
Telefoninumber tööl	❍	❍	❍	❍	❍	❍	❍
Meiliaadress	❍	❍	❍	❍	❍	❍	❍
Sünniaeg	❍	❍	❍	❍	❍	❍	❍
Krediitkaardi number	❍	❍	❍	❍	❍	❍	❍
Aastane sissetulek	❍	❍	❍	❍	❍	❍	❍
PayPali konto	❍	❍	❍	❍	❍	❍	❍
Laenuajalugu	❍	❍	❍	❍	❍	❍	❍
Haigused	❍	❍	❍	❍	❍	❍	❍
Perekonnaseis	❍	❍	❍	❍	❍	❍	❍
Vanus	❍	❍	❍	❍	❍	❍	❍
Twitteri kasutajanimi	❍	❍	❍	❍	❍	❍	❍
Facebooki profiil	❍	❍	❍	❍	❍	❍	❍
Skype'i kasutajanimi	❍	❍	❍	❍	❍	❍	❍

Vahel pakuvad veebisaidid isikuandmete, nt meiliaadressi või telefoninumbri nendega jagamise eest soodustusi või kuponge. Järgnevalt on nimetatud mõned soodustused, mida võidakse teile isikuandmete jagamise eest pakkuda.

Märkige palun iga järgneva väite puhul, kui valmis te olete ettevõtetele oma andmeid jagama, kusjuures 1 = ei ole valmis ja 7 = olen täelikult valmis.

	Ei ole valmis 1	2	3	Neutraalne 4	5	6	Olen täielikult valmis 7
Ettevõte kohandab oma tootepakkumisi vastavalt minu maitsele.	❍	❍	❍	❍	❍	❍	❍
Ettevõte saadab mulle eripakkumisi toodete kohta.	❍	❍	❍	❍	❍	❍	❍
See aitab mul järgmisel korral samalt saidilt ostes aega kokku hoida.	❍	❍	❍	❍	❍	❍	❍
Saan ettevõttelt paremat klienditeenindust.	❍	❍	❍	❍	❍	❍	❍
See suurendab kaubavalikut.	❍	❍	❍	❍	❍	❍	❍
Ettevõtte veebisaidil on täpselt selgitatud	❍	❍	❍	❍	❍	❍	❍
Ettevõtte veebisait teatab mulle	❍	❍	❍	❍	❍	❍	❍
Ma tean alati	❍	❍	❍	❍	❍	❍	❍
Mul on võimalik valida	❍	❍	❍	❍	❍	❍	❍
Saan oma isikuandmeid igal ajal muuta või kustutada.	❍	❍	❍	❍	❍	❍	❍

Internetis kaupade või teenuste ostmisel küsitakse inimestelt tellimuse vormistamiseks isikuandmeid.

Palun näidake ära, milline tundub teile olevat riskiaste iga järgneva andmetüübi jagamisel Internetis kaupade või teenuste ostmisel, kusjuures 1 = väga kõrge risk ja 7 = riski ei ole.

	Väga kõrge risk 1	2	3	Neutraalne 4	5	6	Riski ei ole 7
Nimi	❍	❍	❍	❍	❍	❍	❍
Kodune aadress	❍	❍	❍	❍	❍	❍	❍
Telefoninumber	❍	❍	❍	❍	❍	❍	❍
Töökoha aadress (kui on)	❍	❍	❍	❍	❍	❍	❍
Telefoninumber tööl	❍	❍	❍	❍	❍	❍	❍
Meiliaadress	❍	❍	❍	❍	❍	❍	❍
Sünniaeg	❍	❍	❍	❍	❍	❍	❍
Krediitkaardi number	❍	❍	❍	❍	❍	❍	❍
Aastane sissetulek	❍	❍	❍	❍	❍	❍	❍
PayPali konto	❍	❍	❍	❍	❍	❍	❍
Laenuajalugu	❍	❍	❍	❍	❍	❍	❍
Haigused	❍	❍	❍	❍	❍	❍	❍
Perekonnaseis	❍	❍	❍	❍	❍	❍	❍
Vanus	❍	❍	❍	❍	❍	❍	❍
Twitteri kasutajanimi	❍	❍	❍	❍	❍	❍	❍
Facebooki profiil	❍	❍	❍	❍	❍	❍	❍
Skype'i kasutajanimi	❍	❍	❍	❍	❍	❍	❍

Meenutage aega, mil täitsite Internetis andmete edastamise vormi, näiteks mõnda toodet ostes või hotellis või restoranis broneeringut tehes.

Märkige palun iga väite juures ära, millisel määral te sellega nõustute või ei nõustu, kusjuures 1 = olen kindlasti vastu ja 7 = nõustun kindlasti.

	Olen kindlasti vastu 1	2	3	Neutraalne 4	5	6	Olen kindlasti nõus 7
Andmete esitamine tundus mulle ebamugav.	❍	❍	❍	❍	❍	❍	❍
See ei tekitanud mingit stressi.	❍	❍	❍	❍	❍	❍	❍
See ei hirmutanud mind.	❍	❍	❍	❍	❍	❍	❍
Andmete sisestamine tekitas minus ebakindlust.	❍	❍	❍	❍	❍	❍	❍
Mind häiris see.	❍	❍	❍	❍	❍	❍	❍
Parem meelega ei oleks ma kõiki neid andmeid andnud.	❍	❍	❍	❍	❍	❍	❍
Olin muretu.	❍	❍	❍	❍	❍	❍	❍

Need väited puudutavad seda, kuidas te end Internetis isikuandmeid jagades tunnete.

Valige iga järgneva omadussõnade paari kohta number, mis teie tundeid kõige paremini väljendab.

Kirjeldaksin Internetis andmete jagamist järgmiselt:

	1	2	3	4	5	6	7	
Ohtlik	❍	❍	❍	❍	❍	❍	❍	Turvaline
Usaldatav	❍	❍	❍	❍	❍	❍	❍	Ebausaldatav
Ebakindel	❍	❍	❍	❍	❍	❍	❍	Kindel
Halb	❍	❍	❍	❍	❍	❍	❍	Hea
Üleliigne	❍	❍	❍	❍	❍	❍	❍	Vajalik
Väärtusetu	❍	❍	❍	❍	❍	❍	❍	Väärtuslik
Olen alati valmis	❍	❍	❍	❍	❍	❍	❍	Ei ole kunagi valmis