Telematics and Informatics 34 (2017) 569–582

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States

Cory Robinson

Linköping University, Department of Science and Technology, Campus Norrköping, 601 74 Norrköping, Sweden

ARTICLE INFO

Article history:
Received 8 June 2016
Received in revised form 8 September 2016
Accepted 8 September 2016
Available online 9 September 2016

Keywords:
Self-disclosure
Privacy
Online marketing
Cross-cultural
Ecommerce

ABSTRACT

This study examines how demographic variables affect willingness to disclose and perceived risks of disclosing *personally identifying information* (*PII*, also referred to as *personal data* in Europe) in ecommerce in the United States and Estonia. The study utilized a 17-item list of potential disclosure items (name, email address, etc.), categorized reliably into six sub-indices: contact information, payment information, life history information, financial/medical information, work-related information, and online account information. *Online disclosure consciousness* (ODC) is introduced as a framework to conceptualize, explain the study's findings, 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. The results show significant gaps among participants both within and across nations. Despite Estonia's advanced adoption and progressive policies and practices toward the Internet, Americans are more willing to disclose, and less concerned about perceived risks. The findings suggest willingness to disclose and risk aversion can and should be analyzed empirically together. The theoretical model provides an alternative conceptualization to the ideas of the privacy paradox, privacy calculus, and privacy cost-benefit ratios. Implications for theory, consumers, marketing practice, and public policy are discussed. Importantly, the study can inform increased adoption of ecommerce and the digital economy, while also protecting consumer's personal data.

1. Introduction

Ecommerce, defined as the purchasing of goods or services as "digitally enabled commercial transaction[s] between and among organizations and individuals" (Laudon and Traver, 2003, p. 10), is a strong economic force totaling over $1 trillion in sales in 2013 (Leggatt, 2013, para. 1). As with many digital technologies, consumers must divulge personal data in order to utilize services or interact with websites. Ecommerce requires consumers to provide information necessary for fulfilling and completing an online purchase (i.e. address, phone number, credit card information). Further, consumers may disclose information in exchange for a more personalized shopping experience or for product recommendations (Chellappa and Sin, 2005).

As the frequency with which individuals provide private information over the Internet increases, protecting personal information has become critically important. The lack of comprehensive policies in the United States aimed at protecting consumer privacy and controlling access to consumer information has created a sense of urgency around issues of consumer privacy. Global losses of $11 billion in 2012 due to cyber fraud (Quested, 2014) underscore the need to develop better ways

E-mail address: cory.robinson@liu.se

http://dx.doi.org/10.1016/j.tele.2016.09.006
0736-5853/

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 explores how, why, and under what circumstances consumers are willing to disclose personal information in ecommerce transactions.

The article examines willingness to disclose, defined as an individual's openness to the idea of providing specific personal information in the context of ecommerce transactions. It posits 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 data protection processes.

A comparison of the United States and Estonia provides strong contrasts for this study of disclosure in ecommerce. 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.

This article first explores the literature concerning disclosure of personal information. It then states the study's hypotheses. Data collection is described next, proceeded by results and analysis. Importantly, development of a theoretical model building on existing theory is introduced to help explain the study's results. The conclusion outlines several implications for consumers and marketers.

1.1. Theoretical framework

While shopping online, individuals must constantly navigate various "risk-sensitive activities" (Fife and 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 and 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 attempt to conceptualize the idea of balancing or juggling the need to disclose information with perceived risks. 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 and 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 et al., 2007; Yao et al., 2007; Youn and 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 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 and 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 and 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 fail 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, 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.

1.2. Hypothesis

1.2.1. Nationality

The independent variable in this study, nationality is defined here as differences in patterns of behaviors between people residing in one country (nation-state) versus another. More generally, it is defined as "the collective identity that the people of the nation acquire by identifying with the nation" (p. 19), and 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 (Brosdahl and Almousa, 2013; Capece et al., 2013; Choi and Geistfeld, 2004; Gentina et al., 2013).

As a basis for comparison to the US, the country of Estonia was studied due to its 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.

Although Estonia is smaller than the US in terms of geographic size and population, 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 (ABB, 2013; A.A.K., 2013; E-estonia.com, 2014a; Freedom House, 2014; Herlihy, 2014; Horvitz, 2008), advanced government legislation and regulations (Estonian Information System's Authority, 2006; Friedman, 2013; Herlihy, 2014; Keefer, 2012; Privireal, 2005; Woodard, 2003), a culture that is collectivist and long-term oriented (Hofstede, 2011, 2014a,b), high level of citizen proficiency with the Internet (Estonia.eu, 2014; Estonian Information System's Authority, 2006; Freedom House, 2014; Mansel, 2014; Olson, 2014), and a distinct aversion to risk (Davis, 2007; E-estonia.com, 2013; Hofstede, 2014a; Rooney, 2013).

Based on Estonia's unique position as a leader in Internet adoption and use, combined with the country's five unique national attributes, Estonians would be expected to be more favorable toward the disclosure of personally identifiable information (PII) and perceive less risk in disclosing PII.

1.3. Dependent variables

1.3.1. Willingness to disclose

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. 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 and 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 et al., 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 (Gupta et al., 2010).

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. The author hypothesizes:

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

1.3.2. Perception of risk of disclosing specific PII items

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 such 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 and Rich, 1964). Perception of risk generates anxiety that influences the process of consumer decision making (Taylor, 1974). Mayer et al. define 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" (1995, p. 726). Another

common definition is "the buyer's subjective assessment of the consequences of making a purchasing mistake" (Murphy and 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 et al. (2008), this study defines 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 and Fenech, 2003; Shih, 2004), and perceived risks of online shopping ultimately have a negative effect on ecommerce adoption (Van der Heijden et al., 2003).

Importantly, research shows 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 and Almousa, 2013). The authors conclude that differences in perceptions of risk are likely linked by cultural differences, as well as by overall Internet adoption and proficiency. Similarly, Park et al. (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 is critical in the United States, it is not important in South Korea (Park et al., 2012). For online versus offline shoppers in Malaysia, those shopping online are less risk averse then those shopping in physical stores (Lim and Cham, 2015). 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, 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 (2000) reported that 99% of websites collect personal information from individuals browsing their web sites.

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%) at a higher rate than Americans (70%) (E-estonia.com, 2014b; Murphy, 2011). Overall, differences in perceived risk are influenced by overall Internet adoption and proficiency (Brosdahl and 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. Therefore it is hypothesized:

H2. Estonians will have lower perception of risks related to disclosing specific PII items than Americans.

1.3.3. Demographic factors

Previous research suggests that the ways in which Internet users decide to disclose information is partially determined by demographic factors.

1.3.4. Gender

Contradictions abound in the literature regarding gender, specifically on whether males or females disclose more about themselves to others, either in-person or online (Levesque et al., 2002; Sprecher and Hendrick, 2004; Wheeless and Grotz, 1976). In the context of online communication, females are shown to be more aware of their disclosure actions, disclose more than males, and disclose more honest statements compared to males (Punyanunt-Carter, 2006). Comparing gender disclosure in online social networks and the application of privacy settings, Walrave et al. (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 (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 and Heirman, 2012). I therefore hypothesize:

H3. Male individuals will be more willing to disclose PII items online than female users.

1.3.5. Age

Growing evidence on the age factor suggests that young adults disclose more information online compared to older users (Nosko et al., 2010; Walrave et al., 2012). Nosko et al. (2010) show 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 et al., 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. On the basis of these findings, I predict:

H4. Younger individuals will be more willing to disclose PII items online (H4a) and perceive less risk disclosing PII items online than older users (H4b).

1.3.6. Education level

Education has been found to be an indirect influencer of self-disclosure (Bazarova, 2015), however the linkage is not clearly supported in the literature. 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*. 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. 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. Therefore, the present study hypothesizes:

H5. Individuals having completed more education will be less willing to disclose PII information (H5a) and will perceive greater risk disclosing PII online than individuals who have completed less education (H5b).

1.3.7. 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 et al., 2003). Through increased proficiency in using the Internet, individuals are less likely to be concerned with associated risks (Dutton and Shepherd, 2006). Further, it can be assumed the greater the proficiency in using ecommerce the fewer the concerns about perceived risks, 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. Bases on these findings, I hypothesize:

H6. Those who shop online more frequently will be more willing to disclose information (H6a) and will perceive less risk disclosing PII online (H6b).

2. Materials and methods

2.1. Procedure and participants

During July 2014 in both the United States and Estonia, individuals over age 18 were recruited using quota sampling to complete the online survey administered through Qualtrics, a major online survey research service. Two filter questions were utilized in the survey: one to ensure participants had ecommerce experience, and a second question to ensure participants lived in the US or Estonia. Participants with no ecommerce experience, or not residing in the US or Estonia, were redirected to the end of the survey.

The total sample consisted of 554 participants – 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.

2.2. Translation

A translation service provider was utilized to translate the survey into Estonian. 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, 2014).

2.3. Measures

2.3.1. Willingness to disclose specific PII items

Participants were provided the prompt "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." and were asked 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. 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 $\alpha = 0.87$).

2.3.2. Perceived risk of disclosing specific PII items

Participants were asked 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. Similar to willingness to disclose, a perceived risk of disclosing index of all 17 items was created and found to be reliable (Cronbach $\alpha = 0.90$).

2.3.3. Demographic questions

Participants answered questions relating to 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.

2.3.4. Ecommerce experience

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 one item on 7-point Likert scale with 1 = Beginner and 7 = Expert.

3. Results and discussion

3.1. Nationality predicting willingness to disclose

To compare Estonians versus Americans willingness to disclose specific items, and test H1, student *t*-tests were conducted to compare the two groups. Americans ($M = 3.70$, $SD = 0.905$) are more willing to disclose the 17 items of PII than Estonians ($M = 3.37$, $SD = 1.11$; $t(402) = 3.40$, $p \leqslant 0.001$). Thus, H1 is rejected.

To investigate how well the demographic variables predict willingness to disclose, a hierarchical multiple regression was conducted using the 17-item willingness to disclose index as the dependent measure. To facilitate regression analysis, age and education were collapsed into two groups. For age, those age 34 and younger (dummy variable value = 0) and those age 35 and older (dummy variable value = 1). For education, 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). Table 1 shows the results. Nationality significantly predicted willingness to disclose ($\beta = -0.161$, $p \leqslant 0.001$, $R^2 = 0.024$).

Table 1
Predictors for willingness to disclose.

Step and predictor variable	*B*	*SE B*	*β*	R^2	ΔR^2
Step 1:				0.024***	0.026***
Nationality	−0.327	0.095	−0.161***		
Step 2:				0.035**	0.009
Nationality	−0.370	0.098	−0.182***		
Education	−0.189	0.097	−0.093		
Gender	0.012	0.097	0.006		
Age	0.035	0.095	0.017		
Step 3:				0.06***	0.031***
Nationality	−0.158	0.111	−0.078		
Education	−0.192	0.096	−0.094***		
Gender	−0.003	0.096	−0.001		
Age	0.114	0.096	0.056		
Ecommerce Experience	0.151	0.039	0.211***		

* $p \leqslant 0.05$.
** $p \leqslant 0.01$.
*** $p \leqslant 0.001$.

3.2. Nationality predicting perceived risk of disclosing

To compare Estonians versus Americans levels of perceived risk to disclose specific items and answer H2, student *t*-tests were conducted to compare the two groups.

When measuring perceived risk of disclosing specific PII items, lower scores equate higher perceived risk (*1 = very risky*) and higher scores equate lower perceived risk (*7 = not risky*). Americans ($M = 3.71$, $SD = 1.01$) perceived significantly less risk in disclosing all the 17 PII items than Estonians ($M = 3.31$, $SD = 1.12$, $t(426) = 3.99$, $p = 0.000$). Thus, H2 is rejected.

Hierarchical regression analysis was completed to investigate how the variables of the study effected perceived risk of disclosing specific PII items (see Table 2). Nationality significantly predicted perceived risk of disclosing ($\beta = -0.187$, $p \leqslant 0.001$, $R^2 = 0.035$).

3.3. Gender

Gender is not significantly related to willingness to disclose (H3).

3.4. Effect of age on willingness to disclose and perceived risk of disclosing

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, $p \leqslant 0.006$). 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

Table 2
Predictors for perceived risk of disclosing.

Step and predictor variable	*B*	*SE B*	*β*	R^2	ΔR^2
Step 1:				0.035***	0.035***
Nationality	−0.403	0.100	−0.187***		
Step 2:				0.037**	0.002
Nationality	−0.416	0.104	−0.193***		
Education	−0.095	0.103	−0.044		
Gender	−0.043	0.103	−0.020		
Age	0.002	0.101	0.001		
Step 3:				0.052***	0.015**
Nationality	−0.262	0.119	−0.121*		
Education	−0.097	0.102	−0.045		
Gender	−0.053	0.103	−0.025		
Age	0.059	0.103	0.028		
Ecommerce Experience	0.110	0.042	0.144**		

* $p \leqslant 0.05$.
** $p \leqslant 0.01$.
*** $p \leqslant 0.001$.

34 or younger, and 45% were 35 or older. In Estonia, 44% were 34 or younger, and 56% were 35 or older. Age is not significantly related to either willingness to disclose (H4a) or perceived risk (H4b).

3.5. Effect of education level and willingness to disclose and perceived risk of disclosing

The two groups revealed important differences in education patterns, with the American sample having higher completed education levels overall. 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%). Those less educated were more willing to disclose information online, therefore H5a is supported. Education level is not significantly related to perceived risk of disclosing (H5b).

3.6. Ecommerce experience and willingness to disclose and perceived risk of disclosing

At a statistically significant level, Americans were more experienced with ecommerce ($M = 5.75$, $SD = 0.933$) than their Estonian ($M = 4.30$, $SD = 1.48$) counterparts ($t(372) = 12.91$, $p = 0.000$).

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 (H6a), and perceived less risk in disclosing (H6b). Thus, hypotheses H6a and H6b were supported.

4. Discussion

The study found some interesting results regarding the effect of nationality, education, and ecommerce experience toward individuals willingness to disclose and perceived risk of disclosing while shopping online.

First, Estonians were less willing to disclose versus Americans. This could be explained by cultural reasons: the lower levels of willingness to disclose online 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. 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.

Secondly, those less educated were more willing to disclose information online. Education has been found to influence disclosure (Bazarova, 2015). The findings of this manuscript support the notions posited by the author that more sophisticated users might have a better understanding of why certain types of personally identifying information might be requested to facilitate transactions and collect marketing intelligence, and are thus likely to be more deliberative and discriminating concerning both the amount and the nature of the personal data they disclose to others.

Lastly, 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 and

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.

4.1. Online disclosure consciousness model

As an alternative model, the gap between willingness and perceived risk suggested in this study might be conceptualized as *online disclosure consciousness*. 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 and 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 and 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. If the individual's willingness-to-disclose score exactly equals risk concern, they might 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.

4.2. 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 (see Fig. 1) 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 3.

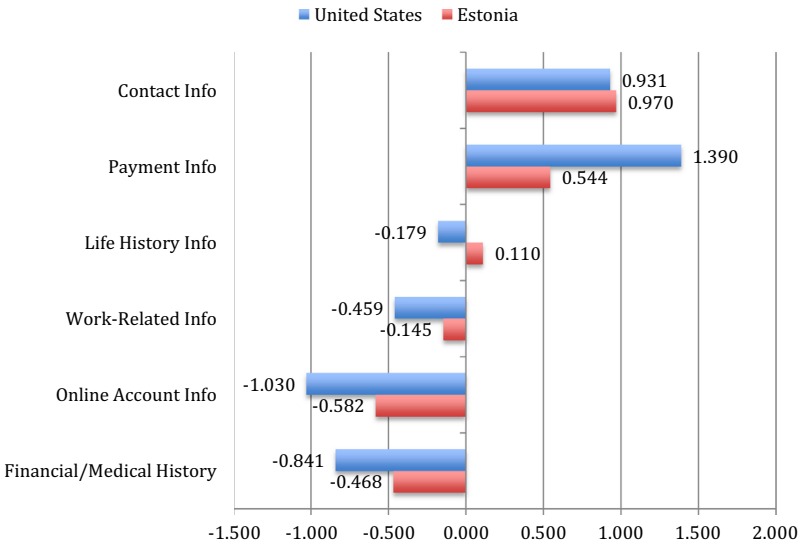

Fig. 1. Gap differences between willingness to disclose and perceived risk. (Note: Scores to the right of the 0.00 line indicate willingness to disclose exceeds perceived risk. Scores to the left of the 0.00 line indicate perceived risk is greater than willingness to disclose. US = blue bar; Estonia = red bar). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 3
Comparison between US & EE gaps between willingness to disclose and perceived riskiness of disclosure.

Measure	US Gap	EE Gap	Difference	*t*	p
Index (17 items)	1.64	1.61	|0.030|	0.28	0.777
Contact Information	0.931	0.970	|0.038|	0.32	0.749
Payment Information	1.39	0.544	|0.844|	5.54	0.000
Life History Information	−0.179	0.110	|0.288|	−2.23	0.026
Work-Related Information	−0.459	−0.145	|0.314|	−2.13	0.034
Online Account Information	−1.03	−0.582	|0.449|	−3.09	0.002
Financial/Medical History Info	−0.841	−0.468	|0.372|	−3.00	0.003

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*).

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.

4.3. 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. 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*).

In the first of five possible situations, 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 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 continuum fall between absolute willingness to disclose and MDC, and absolute perceived risk and MDC. In the fourth situation, 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), 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, 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.

4.4. Limitations

As found in any study, this study had some limitations. First, the research used non-probability sampling to recruit enough participants from both the United States and Estonia. Because the study utilized self-reported measures, the influence of common method bias may be present. Future studies should measure ecommerce experience 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 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).

4.5. Implications for consumers and marketers

The 17 items of personal data measure used 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 this study created a reliable scheme for classifying different types of personal information.

The ODC 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 are evident as well. 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 obtaining benefits while 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.

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.

For marketers, the findings suggest 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.

For public policy, this study provides the following insights and recommendations. 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. 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.

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 disclosure willingness and perceived risk 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.

5. Conclusion

For many around the globe, shopping online has become an almost daily occurrence; however, there is great need to understand the ensuing risk(s) of disclosing information necessary when shopping online. This study examined many factors that influence willingness to disclose personal information, and what types of information individuals perceive as risky to disclose. This cross-national study of the U.S. and Estonia informed the creation of a new framework, online disclosure consciousness, useful for understanding the complex processes involved in disclosing personal data. Lastly, the findings from this study can help encourage increased adoption and usage of ecommerce across the globe by helping marketers understand the linkages between perceived risk and willingness to disclose. Driving increased adoption of ecommerce and the digital economy is important, but protecting the personal information of consumers is just as vital.

References

A.A.K., 2013. How did Estonia become a leader in technology? 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. 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. Holt, Rinehart and Winston, New York, NY.

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

Bauer, R., 1960. Consumer behavior as risk-taking. In: Hancock, R.S. (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>.

Bazarova, N.N., 2015. Online disclosure. In: Berger, C.R., Roloff, M.E. (Eds.), The International Encyclopedia of Interpersonal Communication. Wiley-Blackwell, Hoboken, NJ.

Brosdahl, D.J.C., Almousa, M., 2013. Risk perception and internet shopping: comparing United States and Saudi Arabian consumers. J. Manage. Market. Res. 13, 1–17. Retrieved from <http://www.co.springer.iier.aabri.com/manuscripts/131443.pdf>.

Bucur, A., Renold, C., Henke, M., 1999. How do older netcitizens compare with their younger counterparts? CyberPsychol. Behav. 2 (6), 505–513. http://dx.doi.org/10.1089/cpb.1999.2.505.
Capece, G., Calabrese, A., Di Pillo, F., Costa, R., Crisciotti, V., 2013. The impact of national culture on e-commerce acceptance: the Italian case. Knowled. Process Manage. 20 (2), 102–112. http://dx.doi.org/10.1002/kpm.1413.
Chellappa, R.K., Sin, R.G., 2005. Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf. Technol. Manage. 6 (2–3), 181–202.
Choi, J., Geistfeld, L.V., 2004. A cross-cultural investigation of consumer e-shopping adoption. J. Econ. Psychol. 25 (6), 821–838. http://dx.doi.org/10.1016/j.joep.2003.08.006.
Corbitt, B.J., Thanasankit, T., Yi, H., 2003. Trust and e-commerce: a study of consumer perceptions. Electron. Commer. Res. Appl. 2 (3), 203–215. http://dx.doi.org/10.1016/S1567-4223(03)00024-3.
Cox, D.F., Rich, S.U., 1964. Perceived risk and consumer decision-making: the case of telephone shopping. J. Mark. Res. 1 (4), 32–39. Retrieved from <http://www.jstor.org/stable/3150375>.
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>.
Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Inform. Syst. Res. 17 (1), 61–80. Retrieved from <http://pubsonline.informs.org/doi/abs/10.1287/isre.1060.0080?journalCode=isre>.
Dutton, W.H., Shepherd, A., 2006. Trust in the Internet as an experience technology. Inform. Commun. Soc. 9 (4), 433–451. http://dx.doi.org/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, 2014. Electronic ID Card|e-Estonia. Retrieved January 13, 2014, from <http://e-estonia.com/components/electronic-id-card>.
E-estonia.com, 2014. e-Tax|e-Estonia. Retrieved January 13, 2014, from <http://e-estonia.com/components/e-tax>.
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 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. Publications Office of the European Union, Brussels, Belgium. Retrieved from <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>.
Federal Trade Commission, 2000. Privacy online: fair information practices in the electronic marketplace: a report to Congress. Retrieved from <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.
Fife, E., Orjuela, J., 2012. The privacy calculus: mobile apps and user perceptions of privacy and security. Int. J. Eng. Bus. Manage. 4 (11), 1–9. http://dx.doi.org/10.5772/51645.
Fiske, S.T., Taylor, S.E., 2013. Social Cognition: From Brains to Culture. Sage, London, England.
Fox, S., 2013. 51% of US Adults Bank Online. Pew Internet and American Life Project, Washington, DC. 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>.
Friedman, U., 2013. Behold: the world's first digitally signed international agreement. Atlantic. Retrieved January 23, 2014 from <http://www.theatlantic.com/international/archive/2013/12/behold-the-worlds-first-digitally-signed-international-agreement/282582/>.
Gentina, E., Butori, R., Rose, G.M., Bakir, A., 2013. How national culture impacts teenage shopping behavior: comparing French and American consumers. J. Bus. Res. 67 (4), 464–470. http://dx.doi.org/10.1016/j.jbusres.2013.03.033.
Goodwin, C., 1991. Privacy: recognition of a consumer right. J. Public Pol. Market. 10 (1), 149–166. Retrieved from <http://www.jstor.org/stable/30000257>.
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. J. Electr. Comm. Res. 11 (1), 41–52. Retrieved from <http://www.questia.com/library/journal/1P3-1981541041/facilitating-global-e-commerce-a-comparison-of-consumers>.
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 Read. Psychol. Cult. 2 (1), 8. http://dx.doi.org/10.9707/2307-0919.1014. Retrieved January 24, 2014.
Hofstede, G., 2014. 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. 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>.
Keefer, P.T., 2012. How Estonia Became a World Leader in Digital Governance. Aspen Institute, Washington, DC. 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. Decis. Support Syst. 44 (2), 544–564. http://dx.doi.org/10.1016/j.dss.2007.07.001.
Laudon, K.C., Traver, C.G., 2003. E-Commerce: Business, Technology, Society. Prentice Hall, Upper Saddle River, NJ.
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 Behav. Personal. 30 (6), 579–592. http://dx.doi.org/10.2224/sbp.2002.30.6.579.
Lewin, K., 1935. A Dynamic Theory of Personality. McGraw-Hill, New York, NY.
Lewin, K., 1936. Some social-psychological differences between the United States and Germany. Charact. Personal. 4 (4), 265–293. http://dx.doi.org/10.1111/j.1467-6494.1936.tb02034.x.
Lim, Y.M., Cham, T.H., 2015. A profile of the Internet shoppers: evidence from nine countries. Telematics Inform. 32 (2), 344–354. http://dx.doi.org/10.1016/j.tele.2014.10.002.
Mansel, T., 2014. How Estonia became E-stonia. BBC News. Retrieved March 15, 2014, from <http://www.bbc.co.uk/news/business-22317297>.
Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of organizational trust. Acad. Manage. Rev. 20 (3), 709–734. http://dx.doi.org/10.5465/AMR.1995.9508080335.
Metzger, M.J., 2007. Communication privacy management in electronic commerce. J. Comput.-Mediated Commun. 12 (2), 1–27. http://dx.doi.org/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. J. Interact. Market. 18 (3), 15–29. http://dx.doi.org/10.1002/dir.20009.
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>.
Murphy, P.E., Enis, B.M., 1986. Classifying products strategically. J. Market. 50 (3), 24–42. http://dx.doi.org/10.2307/1251583.

Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Affairs 41 (1), 100–126. http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x.
Nosko, A., Wood, E., Molema, S., 2010. 'All about me', Disclosure in online social networking profiles: the case of Facebook. Comput. Hum. Behav. 26 (3), 406–418. http://dx.doi.org/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. J. Retailing Consum. Services 10 (2), 81–94. http://dx.doi.org/10.1016/S0969-6989(02)00004-8.
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. J. Econ. Psychol. 25 (2), 243–262. http://dx.doi.org/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. Blackwell, Cambridge, UK.
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. J. Retail. Consum. Services 19 (3), 304–312. http://dx.doi.org/10.1016/j.jretconser.2012.03.003.
Petronio, S., 2002. Boundaries of Privacy Dialectics of Disclosure. SUNY Press, Albany, NY.
Petronio, S., Durham, W., 2008. Communication privacy management theory. In: Baxter, L., Braithewaite, D. (Eds.), Engaging Theories in Interpersonal Communication: Multiple Perspectives. Sage Publications, Thousand Oaks, CA, pp. 309–322.
Prensky, M., 2001. Digital natives, digital immigrants: Part 1. Horizon 9 (5), 1–6. http://dx.doi.org/10.1108/10748120110424843.
Privireal—Privacy in Research Ethics & Law, 2005. Estonia – Data Protection. University of Sheffield Department of Law, Sheffield, UK. 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. Coll. Stud. J. 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>.
Rooney, B., 2013. Estonia: the role model for tech-enabled states. Wall Street J. Retrieved January 7, 2014 from <http://online.wsj.com/news/articles/SB10001424127887323477604578653792712743194#livefyre-comment>.
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: Holzinger, A., Ziefle, M., Hitz, M., Debevc, M. (Eds.), Human Factors in Computing and Informatics, vol. 7946. Springer, Berlin, Germany, pp. 174–193.
Shih, H.-P., 2004. An empirical study on predicting user acceptance of e-shopping on the Web. Inform. Manage. 41 (3), 351–368. http://dx.doi.org/10.1016/S0378-7206(03)00079-X.
Sprecher, S., Hendrick, S.S., 2004. Self-disclosure in intimate relationships: associations with individual and relationship characteristics over time. J. Soc. Clin. Psychol. 23 (6), 857–877. http://dx.doi.org/10.1521/jscp.23.6.857.54803.
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. J. Comput.-Mediated Commun. 19 (2), 248–273. http://dx.doi.org/10.1111/jcc4.12052.
Taylor, J.W., 1974. The role of risk in consumer behavior. J. Market. 38 (2), 54–60. Retrieved from <http://www.jstor.org/stable/1250198>.
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>.
Van der Heijden, H., Verhagen, T., Creemers, M., 2003. Understanding online purchase intentions: contributions from technology and trust perspectives. Eur. J. Inform. Syst. 12 (1), 41–48. http://dx.doi.org/10.1057/palgrave.ejis.3000445.
Walrave, M., Heirman, W., 2012. Adolescents, online marketing and privacy: predicting adolescents' willingness to disclose personal information for marketing purposes. Child. Soc. 27 (6), 1–14. http://dx.doi.org/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. Cyberpsychol.: J. Psychosoc. Res. Cybersp. 6 (1). http://dx.doi.org/10.5817/CP2012-1-3. article 1.
Wheeless, L., Grotz, J., 1976. Conceptualization and measurement of reported self-disclosure. Hum. Commun. Res. 2 (4), 339–346.
Wiedemanni Translation Company, 2014. 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. Educ. Rev. 40 (5), 43–58.
Woodard, C., 2003. Estonia, where being wired is a human right. Christ. Sci. Monit. Retrieved January 23, 2014, from <http://www.csmonitor.com/>.
Yao, M.Z., Rice, R.E., Wallis, K., 2007. Predicting user concerns about online privacy. J. Am. Soc. Inform. Sci. Technol. 58 (5), 710–722. http://dx.doi.org/10.1002/asi.20530.
Youn, S., Hall, K., 2008. Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. CyberPsychol. Behav. 11 (6), 763–765. http://dx.doi.org/10.1089/cpb.2007.0240.