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.