TRUST AND INFORMATION PRIVACY CONCERNS IN ELECTRONIC GOVERNMENT

Ardion D. Beldad

Thesis. University of Twente.

ISBN 978-90-365-3168-9

Beldad, A.D. (2011). *Trust and information privacy concerns in electronic government*. Enschede, The Netherlands: University of Twente.

A number of studies presented in this dissertation were subsidized by the Alliantie Vitaal Bestuur and by the IBR Research Institute for Social Sciences and Technology of the University of Twente.

Printed by Gildeprint Drukkerijen

TRUST AND INFORMATION PRIVACY CONCERNS IN ELECTRONIC GOVERNMENT

D I S S E R T A T I O N

to obtain
the degree of doctor at the University of Twente,
on the authority of the rector magnificus,
prof. dr. H. Brinksma,
on account of the decision of the graduation committee,
to be publicly defended
on Thursday the 17th of March 2011 at 14:45

by

Ardion Daroca Beldad

born on the 12th of January 1977

in Manila, Philippines

This dissertation is approved by

Prof. Dr. Michäel Steehouder
Prof. Dr. Menno de Jong

Members of the Graduation Committee

Prof. Dr. Ronald Leenes, University of Tilburg
Prof. Dr. Cees Midden, Eindhoven University of Technology
Prof. Dr. Leo Lentz, University of Utrecht
Prof. Dr. Jan van Dijk, University of Twente
Prof. Dr. Philip Brey, University of Twente

Veritas liberabit vos

Table of Contents

1

General Introduction

This chapter presents an overview of the nature of e-government and the elements that differentiate it from electronic commercial transactions (e.g. online shopping). Factors influencing the acceptance and the adoption of e-government are also discussed. Furthermore, the impact of trust and information privacy concerns on e-government acceptance and adoption is explained. The main research questions of the dissertation are also presented. Chapter 1 ends with a brief introduction of the succeeding chapters of this dissertation.

The Internet opens a world of wonder supposedly surreal only a few decades ago. A world with the Internet has been one where Amazon is not just a tropical rainforest but a site where cravings for things are satiated and Yahoo is not just another expression of exhilaration but a communication medium poised to obscure the existence of the postal service industry. Thanks to the Internet, online shopping, online social networking, and online application for government documents have become performable human acts.

But like most wonderlands, dark entities abound in the Internet. Threats of varied forms and levels of severity lurk and thrive in the ostensibly everything-is-possible digital environment. Online transactions can be fraudulent, just as the facelessness and intangibility of interactions could be maliciously exploited for the benefit of one at the expense of the other. That is where the unpleasant news lies.

The risks that tail most computer-mediated exchanges and interactions are real and copious. An ordered product that has already been paid for online might never be received and personal information supplied for a particular online exchange could be relayed to other parties for dubious purposes. If people can be cheated in their transactions in the physical world, their chances of being defrauded online are not remote. Due to their distant and impersonal nature, computer-mediated transactions and interactions are often deemed risky.

Certainly the risks involved in online commercial transactions are aplenty, but it would be unwise to surmise that those that are non-commercial in nature are risk-free. Online non-commercial transactions, such as those done with government organizations, could hardly be described as entirely safe. Although such transactions rarely propel the shelling out of a euro or two, they can only be completed after the acquisition of complete and correct personal information from citizens. With personal information becoming tradable - and somehow profitable - commodities, the peril of information abuse is not discountable.

In the second chapter of this dissertation, it is advanced that beliefs in the potential of online organizations to abuse their clients' personal data instigate perceptions of risks involved in online information sharing. These perceptions might suffice to dissuade Internet users from engaging in computer-mediated transactions requiring personal data. The reality of risks and risk perceptions in online transactions, therefore, reinforces the indispensability of trust, as a number of authors claimed (e.g. Koller, 1988; Lewis & Weigert, 1985; Mayer, Davis, & Schoorman, 1995).

Empirical studies on trust and information privacy concerns in e-commerce are manifold, while those pursued within the context of e-government are relatively limited. While it is argued that risk perceptions are more prominent in online commercial exchanges than in e-government transactions (Belanger & Carter, 2008), risk perceptions, regardless of magnitude, could already reduce citizens' inclination to use e-government services (Hung, Chang, & Yu, 2006). Though different in several ways, the

success or the failure of e-commerce and e-government banks on a common denominator: the inevitability of risks in both forms of transactions.

The need for trust in the context of e-government and the undeniable reality of privacy risks spurred by the close association of personal information disclosure with e-government services are two themes central to this dissertation. A discussion of these themes would be spineless, however, if the nature of e-government is not scrutinized. This chapter focuses on the nature of electronic government and the impact of trust and information privacy concerns on its acceptance and adoption. The main questions of the research project, which were addressed by the different studies described in the different chapters of this dissertation, are also discussed. The chapter ends with an overview of the different sections of the dissertation.

1.1 The nature of e-government

Perspectives on e-government emphasized the system's dependence on the deployment of technology to support the interaction between organizations and citizens and to enable the former to deliver their services to the latter (Lau et al., 2008; Lenk & Traunmueller, 2007; Sharma & Gupta, 2003; Van Dijk, 2006; Wyld, 2004). Specifically, e-government is described to 'comprise all processes of information processing, communication, and transaction that pertain to the tasks of the government (the political and public administration) and that are realized by a particular application of ICT' (Van Dijk, 2006).

Although it is not surprising that mainstream understanding of e-government would slant toward its reliance on the Internet, other forms of information and communication technologies, such as fax machines and newer mobile technologies are not to be dismissed as important drivers in the performance of different e-government activities (Andersen & Henriksen, 2006; Williams, 2008). However, it is still a widely held view that e-government is intertwined with the Internet. Thus, when one is engaged in an electronic transaction with a government organization, the transaction is mostly done through its website, which, according to Teo, Srivastava, and Jiang (2008), acts as a proxy for a government organization that originally extends it services to the public through traditional offline channels.

The deployment of e-government is expected to improve the quality of service delivery by government organizations to citizens (Germanakos, Christodoulou, & Samaras, 2007; Kumar, Mukerji, Butt, & Persaud, 2007), as it enables citizens to define how and when they will transact with a particular government organization (Kumar et al., 2007). The Internet, upon which e-government is recognizably hinged, broadens people participation in public administration processes, just as the electronic delivery of services spares citizens and government agencies ample time and paperwork (Schwester, 2009).

Two reasons are crucial for the indispensability of e-government for any nation, regardless of its development and economic status. First, the use of technological initiatives by governments will contribute to their efficiency and competitiveness in the current environment. Second, e-government has the potential of enabling democratic governance, promoting democratic practices, and facilitating efficient contact between governments and the citizens (Theunissen, 2007). Aside from the delivery of quality services to customers (citizens and businesses) as a central goal for e-government, it also reduces government costs (Blakemore, 2010).

While 'e-government' would normally be associated with the facilitation of interactions between citizens and their government, also referred to as government-to-citizen (G2C), it also includes transactions between government and businesses (G2B) and between one government agency and another government agency (G2G). G2G initiatives increase efficiency and communication between and among different parts of a government, while G2B primarily involves the sale of government goods and the procurement of goods and services for the government (Jaeger, 2003).

This dissertation focuses on trust and privacy issues in government-to-citizen (G2C) interactions. Therefore, e-government services or online government transactions, as used in the different studies described in the succeeding chapters, should be understood in terms of the transactions between government organizations and citizens.

The development of e-government usually takes longer than the natural transition from winter to spring. The tendency is to look at e-government as undergoing a constant evolution in several phases. For instance, Muir and Oppenheim's (2002) categorization of e-government appears to correspond to the three stages of e-government's development or growth. According to these authors, e-government commences with the development of the use of IT within government. It then proceeds to the provision of information by government organizations, through their electronic channels, to citizens. Finally, it climaxes in the facilitation of a two-way interaction between government organizations and citizens.

1.2 E-government vs. online commercial transactions

The relative 'newness' of research on trust and on information privacy concerns in e-government means that the literature for these research domains is expectedly limited. For instance, while studies on the determinants of trust in the context of e-commerce teem, similar studies within e-government are remarkably few (e.g. Gefen et al., 2002). In fact, in several empirical investigations, trust is just treated as one of the possible factors influencing e-government usage intention (Belanger & Carter, 2008; Carter & Belanger, 2005; Colesca & Dobrica, 2008; Srivastava & Teo, 2009; Teo, Srivastava, & Jiang, 2009). Studies on the determinants of trust in e-

government are considerably scant. Information disclosure behavior and information privacy issues within the context of e-government are also underexplored themes. This would explain for the theoretical dependence of the dissertation on trust and information privacy studies pursued along the tracks of online commercial exchanges, as evidenced by the discussions in Chapters 2 and 3.

It is, however, important to distinguish e-government from online commercial transactions (e.g. e-commerce, e-banking). The reasons for the existence of both e-government and e-commerce (service vs. profit) and their target clients (citizens vs. the general population in the market) delineate the differences between the two (Belanger & Carter, 2008). Jorgensen and Cable (2002) differentiated e-government from e-commerce according to these three criteria: access, structure, and accountability.

With regards to access, while business have the ability to choose their customers, government organizations are expected to deliver their services to an entire segment of a given population. In terms of structure, government organizations, compared to business, have less hierarchies and indirect lines of authority, which make the implementation of e-government challenging. Within the framework of accountability, public constraint in the activities of government agencies differentiates them from private commercial organizations. E-government initiatives take longer to implement, cost more, and deliver less compared to e-business projects (Jorgensen & Cable, 2002).

Nevertheless, despite the differences, e-government shares a lot in common with e-commerce, since both rely on the Internet technology for the exchange of goods, services, and information between two or more parties over great distances (Belanger & Carter, 2008; Carter & Belanger, 2004). Problems that beleaguer e-commerce (*e.g.* lack of well understood rules, trust, and digital divide) also hamper the acceptance and the adoption of e-government initiatives (Mullen & Horner, 2004).

1.3 Acceptance and adoption of e-government

Substantial amounts of financial resources, human efforts, and time invested for the implementation of a new project are fated for the sewage if the project's rate of acceptance and adoption is neighboring *nul*. Acceptance, the expected effect of people's positive attitude toward something, precedes adoption. Naturally, parties and organizations behind projects and initiatives aimed at a widespread acceptance of such projects among their target clients as a logical antecedent of adoption.

The technology acceptance model of Davis (1989) predicts that people's perceptions of the usefulness and the ease of using a novel technology or system influence their intention to adopt that technology or system. Something is assessed to be useful when it is believed to improve the performance of one's task. When using it would be relatively easy, it may be regarded to have passed the 'ease of use' criterion (Davis, 1989).

One can equate the perceived usefulness of e-government services with the benefits citizens can derive from using the aforementioned system. As Al-Awadhi and Morris (2008) pointed out, a demonstration of the advantages and benefits of e-government services is necessary for their adoption.

Kumar et al. (2007) argued that adoption in the context of e-government can be regarded as a multidimensional construct and involving several phases. Initially, adoption could be a simple decision of using or not using government organizations' online services. Then this proceeds to the question on the frequency of online government service usage. Another dimension that needs to be considered with regards to adoption is the scope of usage. Are government websites used for actual interaction or transaction or just for information search? (Kumar et al., 2007)

Adoption can also be measured in terms of people's preference for a particular medium in an online transaction with a government organization. Are citizens comfortable in transacting with a government agency through its website or would they prefer to carry out that same transaction over the telephone or through the organization's 'physical outlet'? (Kumar et al., 2007). In this dissertation, adoption, expressed in the intention of citizens to engage in an online transaction with a government organization or in their inclination to avail government services online, is viewed in terms of citizens' readiness or willingness to disclose their personal data for e-government services.

This perspective is predicated on the fact that the completion of an electronic form, which presses citizens to supply personal information, precedes the actual online transaction with a government organization. For instance, an online application for a permit can only be processed when the applicant's personal data are supplied to the responsible agency. Those who find online personal information disclosure bothersome and perilous would most likely refuse to share what is being requested, which would eventually result in the failure of the online transaction.

The influence of citizens' perceived usefulness of e-government services on their intention to adopt the aforementioned method of public service delivery has been empirically tested in a number of studies (Al-Awadhi & Morris, 2009; Carter & Belanger, 2004; Colesca & Dobrica, 2008; Horst, Kuttschreuter, & Gutteling, 2007). For instance, respondents in the study of Al-Awadhi and Morris (2009) noted that convenience of access, time, and efficiency of service delivery contributed to their preference for e-government services over those delivered through traditional media, which eventually influenced their adoption of such services. The perceived ease of using e-government systems has also been found to result in users' adoption of online government services (Al-Awadhi & Morris, 2008; Carter & Belanger, 2005; Colesca & Dobrica, 2008).

While e-government provides citizens with a range of benefits, the importance of trust as a catalyst for citizens' willingness to embrace this new mode of service delivery (Warkentin et al., 2002) should not be overlooked. Trust is necessary because of risks, and online transactions with government organizations are far from being risk-free.

1.4 The impact of trust and information privacy concerns on e-government acceptance and adoption

Trust in e-government could be viewed both as trust in the government organization offering its services online and in the technology used for service delivery – the Internet (Teo, Srivastava, & Jiang, 2009). Trust in the technology, as the aforementioned authors defined, is the extent to which website users trust the competence and the security of the Internet.

However, this dissertation subscribes to the notion of trust as citizens' expectation of the behavior (Barber, 1983; Koller, 1988; Luhmann, 1979; Rotter, 1967) of the government organization as the partner in an online exchange. The need for trust in a government organization is anchored on the premise that the risks inherent in e-government transactions requiring online disclosures of personal data are attributable not only to government organizations collecting the data but also to external third parties that could illegally access such data for unknown purposes.

By attributing risks to the two parties just mentioned, trust as an expectation would expectedly focus on trust in the government organizations' willingness to safeguard citizens' personal data and in their ability to protect those data. This notion is based on the definition of trust as a 'belief that a specific other will be able and willing, in a discretionary situation, to act in the trustor's best interest' (McLain & Hackman, 1999). Trust in the organization's willingness (to do something good, for instance protecting citizens' personal data), of course, is a response to the risk of having personal data abused by government organizations; while trust in the organization's ability (to do something good, for instance protecting citizens' personal data) is geared towards the risks of external third parties unlawfully accessing citizens' personal data.

Perceptions of the risks involved in any form of online transactions would expectedly necessitate trust in the Internet technology, which is perceived in terms of the availability of safeguards, structures, or systems to ensure the safety of transactions or exchanges in the virtual environment. However, such safeguards and structures do not spring just out of nowhere. They are implemented, deployed, and maintained. Some hands are responsible for their existence.

Personal data supplied online could be spared from abuse not because the Internet is naturally safe but because parties that collect those data online have done whatever is necessary to safeguard them. Therefore, as Friedman, Kahn, and Howe (2002) advanced, people behind a technology or those using it should be trusted and not the technology itself.

Citizens are almost never asked to supply their data when just looking for information on a government organization's website, although they risk being peeped upon online with those invisible cookies. However,

when the interaction moves from one-way (information search) to two-way (submission of an application for a government document), citizens are left with no choice but to supply information about themselves (McDonagh, 2002).

Disclosure of personal information, on the part of citizens, to access online government services brings information privacy risks to the fore. Citizens' reluctance to adopt e-government services is attributable both to lack of trust in the security of online transactions (Belanger & Carter, 2008) and to concerns regarding the usage and safety of personal information disclosed for a particular online transaction (Belanger & Carter, 2008; Rose & Grant, 2010).

It is imperative, therefore, that citizens believe and trust that their information privacy is protected before they will share their data for an e-government service (Regan, 2008). This dissertation subscribes to the definition of information privacy as 'the potential loss of control over personal data that are used without the knowledge and permission of the person to whom the data pertain' (Featherman & Pavlou, 2003). Chapter 2 contains a thorough discussion of the concept of 'information privacy'.

Previous studies have indicated that trust is crucial in shaping information privacy-related behaviors within the virtual environment, such as disclosing complete and correct personal data for a particular e-government service or consulting online privacy statements to gain insight into organizational usage and processing of citizens' personal data. Personal information disclosure could be expected when Internet users trust an online organization, while information fabrication and non-disclosure could stream from the absence of trust.

The readership of privacy statements, one of the many trustworthiness cues identified in several studies, also depend on users' trust in an online organization. Information-seeking by consulting an online privacy statement would be an irrelevant act when the organization behind the website used for personal data collection is trusted.

1.5 Main research questions

The dissertation attempts at weaving the connection between trust and information privacy concerns in the context of e-government. Concerns regarding the inevitability of information privacy violation, which could primarily be attributed to the probability of having electronically disclosed personal data exploited and misappropriated either by the organization collecting them or by external third parties, fuel perceptions of the risks involved in disclosing such data online. Risks and risks perceptions intensify the need for the cultivation of trust in the other party engaged in an online exchange.

Trust, as shown in several studies, increases people's intention to perform a particular behavior, for instance, engaging in computer-mediated exchanges. The adoption of e-government, as initially noted, depend not

only on its perceived usefulness but also on citizens' trust in the aforementioned mode of service delivery. Since almost all online government transactions are preceded by personal information disclosure, the adoption of the former should be viewed in terms of the citizens' willingness to do the latter. Therefore, it makes sense to focus on online personal information disclosure and the factors that could influence it. The first main research question is predicated on this focus.

1.5.1 What factors influence citizens' willingness to disclose personal data for online government transactions?

The positive impact of trust on Internet users' inclination to engage in electronic transactions is irrefutable, as evidenced by many studies on trust within the context of e-commerce. Studies pursued within this domain have also concentrated on determining the impact of different factors on online trust formation. While studies on the determinants of trust in e-commerce proliferate, those done along the trails of e-government are remarkably scarce. Despite the many differences between e-commerce and e-government, it can still be assumed that the factors that could increase trust in the former would still be applicable for understanding trust in the latter. This precipitates the second main research question.

1.5.2 What are the determinants of trust in government organizations in terms of their processing and usage of citizens' personal data shared for online government transactions?

The relation between trust and risk has never been completely clear. If risks and perceptions of risks necessitate trust, does trust or the lack thereof result in the decline or the increase of risk perceptions, respectively? Does the appraised sensitivity of personal data that will be shared to avail a government service online contribute to risk perceptions? These two inquiries fundamentally shaped the third main research question?

1.5.3 What factors determine perceptions of the risks involved in the disclosure of personal data for online government transactions?

The certainty of information privacy risks in online government transactions fuels the supposition that citizens will look for any guarantee that whatever data they will disclose through a government website will not be abused or misappropriated and will be adequately protected. Different empirical studies identified different trustworthiness cues that are vital in quelling risk perceptions and information privacy concerns. Indications of the usage of security technologies and online privacy statements are regarded as essential trustworthiness cues. Internet users who want to be sufficiently informed how their disclosed personal data will be used and protected only have online privacy statements as primary sources for the needed information.

In the European Union, the importance of information privacy protection is manifested through the implementation of national laws. Privacy statements may say a lot of things, but the question on whether or not the contents of those documents conform to legal requirements merits attention. The fourth main research question finds it shape from this interest.

1.5.4 What are the contents of privacy statements on government websites and do the contents conform to the stipulations of the law on personal data protection?

While trust could heighten online personal information disclosure intention, as implied in the first main research question, it could also be surmised that trust impacts other information privacy-related behaviors such as searching for information on how organizations will use and protect personal data that they collect. Earlier it was mentioned that privacy statements are important trustworthiness cues designed to minimize citizens' perceptions of the risks involved in online personal information disclosure. Studies have shown that they are seldom read or consulted. Nevertheless, there still are a few who bother to read online privacy statements. For the fifth main research question, the focus is on determining the factors that prompt people to read privacy statements on government websites.

1.5.5 What factors contribute to citizens' intention to consult privacy statements on government websites?

1.6 Overview of the dissertation

Chapter 2 explores the different information privacy-related behaviors of Internet users. The discussions presented are founded on the main thesis that behaviors related to information privacy differ because people's attitude toward it varies significantly. Such variations are regarded as closely associated with the disparities in the levels of trust and risk perceptions among individuals. The question on why others would unwarily disclose personal information, while others not, for instance, is addressed using different theoretical perspectives having origins in communication, social psychology, and sociology.

The concept of trust is thoroughly discussed in **Chapter 3**. Information privacy concerns, as emphasized in Chapter 2, stem from perceptions of the risks involved in online personal information disclosure. Risks (or risk perceptions), as a number of authors suggest, necessitate trust. The third chapter, hence, does not only dwell on trust as a stand-alone complex socio-psychological phenomenon but also defines it in relation to risks and risk perceptions. Diverging theoretical perspectives on trust are also articulated, while the differences and the similarities between trust in offline and online contexts are discussed. The second section of

Chapter 3 expounds on the different factors influencing online trust formation, based mostly on the results of empirical studies pursued within the framework of online commercial exchanges. It is, nevertheless, argued that some of the factors that could contribute to the formation of trust in online commercial exchanges could also be used to gain insight into the possible determinants of trust in e-government.

Three focus group discussions (FGDs) were conducted to explore Dutch citizens' experiences with and concerns in availing government services online. Results of the FGDs, discussed in **Chapter 4**, did not only provide the foundation for the construction of the instruments used for a number of succeeding empirical investigations but also contributed to an understanding of the issues related to the adoption or usage of e-government in the Netherlands. The FGDs revealed that although participants recognized the advantages of transacting with government organization online, they also perceived risks in those transactions.

Chapter 5 discusses the results of the Internet-based survey that aimed at ascertaining the impact of a number of factors on Internet users' behavioral intention to disclose personal data for e-government services. Trust in government organizations in terms of how they will deal with citizens' personal information has been found to be a very significant factor positively influencing the information disclosure intentions of Internet users - with and without e-government experience. However, low risk perceptions, high expectations of the benefits that can be derived from e-government services requiring personal data, and strong beliefs in the adequacy of legal protection mechanisms also play crucial roles in augmenting information disclosure intentions.

Since trust positively influences citizens' willingness to share personal information for e-government services, as pointed out in Chapter 5, another online survey was implemented to estimate the impact of several trustworthiness cues, those discussed in the third chapter, on Internet users' trust in government organizations in terms of their processing and usage of citizens' personal information. Results of the third survey are discussed in **Chapter 6**. Citizens' confidence in online privacy statements, their positive evaluation of a government organization's reputation, and their satisfaction with an online government transaction have the potency to increase their trust in a government organization in terms of how it processes and uses citizens' personal data.

In Chapter 5 it is also accentuated that high levels of trust propel the reduction of risk perceptions concerning online information disclosure. **Chapter 7** focuses on the determinants of the perceptions of risks involved in online information disclosure. Trust in an organization, as one of the hypothesized determinants, is categorized into two – trust in the organization's willingness and in the organization's ability to protect citizens' personal information. Results of the online survey indicated that Internet users' lack of trust in a government organization's ability to protect citizens' personal information and users' assessment of the sensitivity of

some types of personal information contribute to perceptions of the risks involved in online personal information disclosure.

Citizens' confidence in privacy statements on government websites is somehow pivotal in increasing trust in a government organization in an online context, as noted in Chapter 6. **Chapter 8** focuses on online privacy statements. A content analysis was performed to dissect the contents of the those documents and to evaluate their conformity to the provisions of the Personal Data Protection Law of the Netherlands. The study also looked into the availability and the ease of finding privacy statements on Dutch municipal websites. Two important findings resulted from this study. First, privacy statements on municipal websites varied in their structures and contents, with some privacy statements being too detailed with their guarantees, while others only offered general, and sometimes vague, assurances. Second, while most municipal websites posted privacy statements, a significant number of those statements were relatively difficult to find.

While it is known that privacy statements are almost never read, reading privacy statements is also regarded as one of the strategies in managing information privacy risks. Results of another Internet-based survey, as discussed in **Chapter 9**, show that risk perceptions indeed prompt Internet users to peruse or consult privacy statements before deciding to share personal information for online government transactions.

The important results of the different studies are discussed in **Chapter 10**. The theoretical and practical implications of the results of the different studies are also presented. Furthermore, recommendations for future research are elaborated in the last chapter. Shown below is a tabular representation of the interrelatedness among the different chapters for this dissertation.

Research Questions	Type of Data	Chapters in the Dissertation
1. What factors influence citizens' willingness to disclose personal data for online government transactions?	Data obtained through a literature review, focus group discussions, and a large-scale Internet-based survey	Chapter 2 Chapter 4 Chapter 5
2. What are the determinants of trust in government organizations (in terms of their processing and usage of citizens' personal data shared for online government transactions)?	Data obtained through a literature review, focus group discussions, and a large-scale Internet-based survey	Chapter 3 Chapter 4 Chapter 6
3. What factors determine citizens' perceptions of the risks involved in the disclosure of personal data for online government transactions?	Data obtained through a small-scale Internet-based survey	Chapter 7
4. What are the contents of privacy statements on government websites and do the contents conform to the stipulations of the law on personal data protection?	Data from a content analysis of privacy statements on municipal websites	Chapter 8
5. What factors contribute to citizens' intention to consult privacy statements on government websites?	Data obtained through a literature review and a small-scale Internet-based survey	Chapter 2 Chapter 9

2

What's behind sharing, faking, and keeping? Online personal information-related behaviors from the lenses of various theoretical perspectives

Almost all forms of online transactions, like purchasing a gadget through an electronic shop or signing in for a social networking site, are hinged on the need to collect Internet users' personal data. With the economic value attached to most personal data, it does not astound to know that any data disclosed for an online transaction could be abused either by the collecting organization or by external third parties.

The perceived risks of information abuse suffice to instigate Internet users to employ varied information privacy-protection strategies that are either technically- or behaviorally-based. People, however, differ in terms of how they value their different personal information, in particular, and their information privacy, in general. While some people might be overly protective of their personal data, others might relentlessly trade them for rewards and benefits of any kind. This chapter discusses the different information privacy-related behaviors of Internet users from the perspectives of different theories in communication, social psychology, and sociology.

This chapter is based on a manuscript by Beldad, A., De Jong, M., & Steehouder, M., which will be published in The Information Society.

2.1 Introduction

Almost everything and everybody is getting webbed every time, everywhere. While people surely do different things on the Internet - from applying for an email account to opening an online bank account, and from joining a social networking site to purchasing the latest gadget from a commercial website – the need for people to disclose personal data to complete an online transaction binds these diverging activities together. It is, therefore, reasonable, that privacy as a moral right of individuals is frequently and increasingly becoming an issue whenever people use information systems, such as the Internet (Brey, 2007).

In a world where privacy is a right, sharing personal data, offline or online, could somehow be discomforting. Divulging one's personal data, for one, would have never been a problem if such data are devoid of any value and if they can just be 'left alone' – a phrase so central in the conceptualization of 'privacy' by Warren and Brandeis (1890). However, personal data have become commodities and this commoditization process increases the susceptibility of data to different forms of exploitation. Due to the risks involved in online personal data disclosure, Internet users would be expected to long for an assurance that whatever personal data shared online will not be abused or misappropriated.

In an age when information can be effortlessly transferred, shared, and even accessed, one can be certain that users would be very protective of their personal information. This is obvious since the potential threats to information privacy are not only human beings who work for organizations that collect personal data and those with the expertise to intrude them, but also the technologies employed not only to gain unauthorized access to Internet users' information but also to monitor users' online behaviors. Just think of those inconspicuous tracking devices that sound too edible to be malignant.

Nevertheless, people's attitude toward their personal data and their information privacy is rather complex. Consider Westin's (1991) categorization of people according to their information privacy concerns: privacy fundamentalist, pragmatist, and privacy unconcerned. While people in the first category would hardly reveal any information about themselves, those in the last category would readily share any personal data under any circumstance. Or even consider the fact that although people may claim that they value their information privacy, they would have no qualms over trading their personal data for tangible or intangible benefits, even if it would mean compromising the aforementioned privacy, (Culnan & Bies, 2003; Olivero & Lunt, 2004). All these support the assertion that people indubitably differ in terms of the value they attach to their information privacy (Volkmann, 2003)

This chapter primarily aims at understanding people's personal information-related behaviors in the virtual environment according to different theoretical perspectives. The paper begins with a discussion of the

concept of privacy and its different types. Online privacy is also differentiated from offline privacy by highlighting the risks associated with the former. The next section of this chapter discusses the different behaviors of Internet users in relation to their personal data. Theories in communication, social psychology, and sociology are used to explain the different behaviors. Empirical findings from studies on online transactions and exchanges substantiate discussions of the different personal information-related behaviors. The last section of this chapter is apportioned for a synthesis of all the important postulations from various theoretical perspectives.

2.2 Privacy: a singular term with a plurality of faces

Privacy as an individual's right to 'be left alone' (Warren & Brandeis, 1890) is one of the conventional views on privacy. However, the notion of privacy as one's freedom from intrusion has been regarded as both 'too broad and too narrow' to be considered as a successful definition of privacy (Moor, 1991). Hence, privacy as a concept should be seen as multifaceted or having different states, which, according to Newell (1995), would result in a profusion of both complementary and contradictory definitions. This somehow coincides with the view of privacy as an umbrella term referring to a wide and diverging group of related things (Solove, 2006).

Westin (1967) identified four states of privacy: solitude, intimacy, anonymity, and reserve. A person acquires solitude when he is spared from being observed by others. Intimacy refers to seclusion for individuals to foster close relationships with others. When one is free from identification and monitoring in public spaces and for public activities anonymity is achieved, while reserve is anchored on the person's desire to restrict information disclosure to others (Westin, 1967).

The multidimensionality of privacy is also evident in Clark's (1997) typology. First, there is what he called as 'privacy of the person', which is concerned with the integrity of the person's body. Issues under this dimension include blood transfusion without consent and compulsory immunization. The second dimension is labeled as privacy of personal behavior, which relates to all aspects of behavior, but more specifically to sensitive matters like sexual preferences and religious practices. DeCew (1997) referred to this dimension of privacy as 'accessibility privacy', which allows an individual to have seclusion for a particular behavior that is socially defined as private – for instance, sexual and bathroom activities.

The third dimension, according to Clark, is privacy of personal communications or 'interception privacy', which enables people to communicate among themselves, through different forms of media, free from surveillance or monitoring by others. This corresponds to DeCew's

(1997) 'expressive privacy' that protects a realm for expressing one's self-identity or personhood through speech and activity.

Aspects of the first three forms of privacy identified by Clark (1997) somehow correspond to Van Dijk's (2006) conceptualization of privacy as either physical (the right to selective intimacy) or relational (the right to make contacts selectively). Physical privacy pertains to the inviolability of the human body and the fulfillment of human needs, while relational privacy refers to the individual's ability to determine one's personal relationships without the observation and interference of other people (Van Dijk, 2006).

Privacy of personal data or information, the fourth dimension in Clark's typology, affords individuals with the opportunity to prevent the automatic transmission of their data to other individuals or groups. This type of privacy is also referred to as information privacy (DeCew, 1997; Van Dijk, 2006) or the 'right to selective disclosure (Van Dijk, 2006). DeCew (1997) claimed that information privacy safeguards individuals from intrusions or fear of threats of intrusions and affords them with control over decisions on who will have access to their personal information and for what purposes.

In the online environment, the fourth dimension is very much applicable since the issue there is the protection of information, which includes not only personal data but also online behaviors and computer-mediated communications (Rezgui, Bouguettaya, & Eltoweissy, 2003). Throughout this chapter, personal information and personal data are used interchangeably.

What makes online information privacy different from offline information privacy is the formidability of threats the former is bound to face. The sophistication of technologies that enable external parties to gain unauthorized access to Internet users' personal data and aid organizations to efficiently relay their clients' information to third parties within the digital environment is a major nemesis to the vulnerability of online information privacy.

The threats to online information privacy include unauthorized data transfer, weak security, data magnets, and indirect data collection (Rezgui et al, 2003). Since personal data have also become economic commodities (Franzak, Pitta & Fritsche, 2001; Olivero & Lunt, 2004; Turner & Dasgupta, 2003), those who collect them can easily succumb to the temptation of sharing them for commercial purposes, even without the consent of those to whom the data pertain. There are also real concerns that collected personal data might not be adequately protected resulting in unauthorized third party access (Wang, Lee, & Wang, 1999).

2.3 Information privacy as control of the flow of one's personal data

Clark's (1997) perspective on information privacy clearly emphasizes the importance of the ability of people to whom the data pertain to filter the flow of their personal data regardless of the environment where the flow is expected to occur. When personal information privacy is equated with control in terms of the quantity and the quality of data to be shared, Westin's notion of privacy as reserve comes back to mind. Westin (1967) defined information privacy as the 'claim of individuals or groups to determine for themselves when, how, and to what extent information about them is communicated to others'. Though practically formulated for privacy in an offline setting, the definition is also irrefutably applicable in an online context.

A number of definitions have also accentuated control as a crucial ingredient for attaining information privacy (Altman, 1975; Diffie & Landau, 1998; Fried, 1984; Nissembaum, 1998; Stone et al., 1983). When control is referred to in this context, it is expected that it is not only information flow that is controlled but also the access others have to a person's information (Diffie & Landau, 1998; Nissembaum, 1998). It can, therefore, be argued that when individuals have control over information dissemination and information access they have acquired a certain level of information privacy, since information control is a part and an aspect of this type of privacy (Moore, 1991; Newell, 1995).

2.4 Information privacy as control of and restricted access to personal data in an online environment

Despite the seemingly plausible points forwarded by the notion of privacy as a matter of control, it is not spared from criticisms for its ambiguity in terms of (a) the kinds of personal information people can expect to have control over and (b) the amount of control that people can expect to have over their personal information (Tavani, 2007). The difficulty in controlling information manifests itself in a highly computerized environment where information greases and slides instantly through computer systems worldwide (Moor, 1991). Hence, as Moor also adduced, to ensure the protection of their information privacy, people should limit the availability of their personal information for the right recipients at the right time.

Flaws in the conceptualization of privacy as control spurred the modification of the notion of privacy as control and restricted access, which advocates for the provision of varying levels of access to different people for different types of information at different times (Moor, 1997). From this perspective emerged a privacy model known as Restricted Access and Limited Control (RALC) (Tavani, 2007), which highlights the need for the

creation of 'privacy zones' that would enable people to limit or restrict others from accessing their personal information (Tavani, 2008).

Absolute control over information about oneself is not necessary in managing one's privacy (Tavani, 2007; Tavani & Moor, 2001). Some degree of control can already be achieved through choice, consent, and correction. Managing one's privacy through choice, as an aspect of limited control, involves prudency in defining the flow of one's personal information and in determining the level of access other parties have to that same information.

Consent, as an element of limited control, implies that people waive their right to privacy and provide others with access to their information. The management of one's privacy is incomplete if the individuals concerned are not provided with access to their data and the opportunity to correct those data if necessary (Tavani, 2007; Tavani & Moor, 2001). Providing online users with the opportunity to update and modify any information collected from them is an indication that they are respected and is an attempt at affording them control over their information (Ashworth & Free, 2006).

Control over personal information, therefore, can be exercised in two-phases: before information will be disclosed and after information disclosure. However, control of information after disclosure depends on the organizations gathering the data. Internet users are not always in the position to have access to their information. Instead, organizations must be ethical enough to provide users with the needed access. In this chapter, the focus is on control before information disclosure.

2.5 Online information privacy as a response to risks

In flesh-and-blood encounters and relationships, it would be disappointing, and even devastating, to find out that personal information we shared to a trusted associate had been relayed to others. The level of dismay, of course, depends on the sensitivity of the information relayed without our consent and the negative consequences that we expect from such disclosure. Most likely it would be the same in the online environment. We expect that whatever data we share to an online organization would not be shared to external parties without our knowledge and consent.

The extension of human interactions from the physical world to the digital environment indicates an expansion of the claim to information privacy rights in the cyberspace. People who are very concerned about their privacy in an offline environment are also prone to bring their privacy concerns in the online world (Lwin & Williams, 2003; Yao, Rice, & Wallis, 2007). People in the digital environment are concerned about their information privacy not only because they do not know the information practices of online organizations (Reagle & Cranor, 1997), but also because

they do not have the ability to control the access others have to their information (Hoffman, Novak, & Peralta, 1999).

The risks related to the disclosure of personal data are copious and depend on the amount and type of data disclosed. For instance, sharing one's contact details online could result in the inundation of one's mailbox with unsolicited marketing materials, as the said data could be sold to marketing organizations. Sharing one's income and health-related information could have more serious consequences for the data owners. Regardless of the type and amount of personal data shared, what is certain is that, in one way or another, such data could be abused in two ways. First, organizations collecting those data might share them with other organizations for commercial or for other unknown purposes. Second, third parties could gain unauthorized access to data stored in organizational electronic databases using the most advanced technology available.

In reality, people in the digital environment have limited control over how their information will be used once shared, just as they have limited control over who will have access to their personal data. So what do Internet users do to ensure the protection of their information privacy in an online environment? Since privacy risks are indubitably inescapable, thereby precipitating information privacy concerns, Internet users would be expected to engage in varied courses of protection strategies, ranging from behavioral techniques to technology-based protection acts.

However, it is important to note that people also differ in their privacy concerns (Ackerman, Carnor, & Reagle, 1999; Sheehan, 2002), which means that personal information-related behaviors can be structured in a pole, as shown in Figure 2.1, with information privacy protection behaviors such as information withholding and incomplete and incorrect information sharing on one side and complete and correct information disclosure on the other side. Positioned in the middle of the pole is information-seeking behavior. Internet users who are concerned about the 'fate' of their personal data once shared online would be expected to consult privacy statements to be adequately informed of organizational usage, processing, and protection of collected personal data.

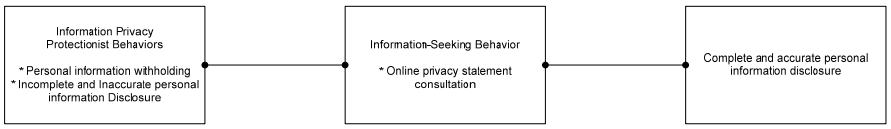

Figure 2.1. Personal information-related behaviors

2.6 When uncertainty triggers a search: Uncertainty reduction and information seeking

It is assumed that Internet users who are concerned about their online information privacy would first search for information on how organizations will deal with their clients' personal data. Often the necessary information can be found in online privacy statements (Vail, Earp, & Anton, 2008). Chapters 8 and 9 will discuss the results of studies on privacy statements on government websites. Decisions on whether or not to share personal data for a particular online transaction could be based on the evaluation of the information in the privacy statements.

The need for information in the decision-making process could be prompted by an awareness of the risks involved in online personal data disclosure and by the fear of disclosing personal data in an environment thriving in uncertainties. In reality, Internet users are often confronted with the uncertainty of what will happen to their personal data once disclosed online.

From a broader perspective, uncertainties stem from situations that are ambiguous, complex, unpredictable, or probabilistic; from the absence or inconsistency of information; from feelings of insecurity about one's own state of knowledge or the state of knowledge, in general (Brashers, 2001). Because uncertainties breed discomfort, anybody plagued with them should be galvanized to eliminate them by acquiring pertinent information (Heath & Bryant, 2000). When people are unsure about the other party in the encounter, disturbance in the flow of the interaction is bound to occur and interaction would require a lot of effort (Berger, 1986).

Berger and Calabrese's (1975) Uncertainty Reduction Theory postulates that high levels of uncertainty accelerate information-seeking behavior and a decline in uncertainty levels decreases information-seeking behavior. Information seeking, Marchionni (1995) pointed out, is a process driven by people's needs for information so that they can interact with the environment, which can only be possible if uncertainties are minimized or even eliminated, as URT accentuates (Berger & Calabrese, 1975).

Within the framework of rational behavior, uncertainties related to one's information privacy during and after online information disclosure should motivate Internet users to perform information-seeking behavior for the acquisition of relevant information about how their personal data will be handled to reduce uncertainties related to their online information privacy. Uncertainty spurs the need for information and the link between the two is captured in Atkin's (1973) definition of the need for information as a 'function of extrinsic uncertainty produced by a perceived discrepancy between the individual's current level of certainty about important environmental objects and a criterion state he seeks to achieve'.

Figure 2.2 shows that people's uncertainties regarding the usage and the processing of their personal data once disclosed trigger concerns

related to information privacy violations, which would push them to perform information-seeking behaviors.

Figure 2.2. Hypothesized three-stage act of information seeking to reduce uncertainty regarding online information privacy

Users who are serious about protecting their online information privacy would be expected to check the privacy statement of every site they visit (Jensen & Potts, 2004). Results of a survey by Milne and Culnan (2004) indicated that reading privacy policies or notices is used as one part of an overall strategy in dealing with the risks of online personal information disclosure and that Internet users are inclined to read privacy notices to manage information privacy-related risks.

The study also shows that users consult privacy policies to acquire information on how their personal data will be used by organizations that collect them (Milne & Culnan, 2004), considering that privacy policies are often the only means for users to know how organizations will use and process their data (Vail, Earp, & Anton, 2008). Privacy statements could also serve as a basis for decision-making (Jansen & Potts, 2004). Internet users who perceive high levels of information privacy risks are more likely to read online privacy statements (Pan & Zinkhan, 2006).

Assuming that users have religiously perused an online privacy statement, can we automatically expect them to opt for information disclosure to transact with organizations online? Probably yes, if users would be convinced that online organizations would do whatever they have indicated on their online privacy statements; probably not, if users would only regard privacy statements as an intricate mishmash of hollow promises. Information search results in a two-fold enlightenment – users may be enlightened that information disclosure is safe resulting in the sharing of complete and correct information or users may be enlightened that information disclosure is still risky prompting information withholding or information fabrication.

2.7 Information withholding and incomplete information disclosure as information privacy protectionist behaviors

Moor (1997) advanced that the creation of a 'privacy zone' enables people to decide how much information should stay private and how much information should be divulged. Akin to this assertion is Pedersen's (1997) notion of boundary control, which refers to the process of restricting and

seeking interaction to achieve a desired degree of access to the self (or one's group) by others at a defined moment and in a particular circumstance. Boundaries are opened when information is voluntarily shared and closed when information is withheld (Stanton, 2002). The concept of boundary distinguishes the self and the non-self – the others (Altman, 1975).

Founded on the premises of privacy regulation, Communication Privacy Management (CPM) suggests that people formulate rules to guide them in deciding whether or not to disclose personal information and in determining the most effective strategies to protect their privacy (Petronio, 2002). The theory also emphasizes that people create rules as an attempt both to maximize the benefits and to minimize the risks of information disclosure.

CPM is anchored on five principles stipulating the ways people regulate the withholding or the sharing of their private information. First, people believe that they own their information. Second, such a belief in information ownership influences people's view that they are entitled to control the flow of their information to others. Third, the decision to open or close privacy boundaries is guided by a set of rules that people create individually. Fourth, when people disclose information, they consider recipients as stakeholders of the information and presuppose that recipients will observe existing privacy rules or negotiate to make some revisions on the rules. Fifth, privacy management in an imperfect world can be turbulent, which occurs when managing one's privacy rules is disrupted or one's privacy boundary is trespassed (Petronio, 2002; 2007).

Although a number of studies have already investigated the various behavioral strategies users employ to define the boundaries surrounding their personal information in online transactions (Earp & Baumer, 2003; Milne, Rohm, & Bahl, 2004; Sheehan & Hoy, 1999), only Metzger's (2007) study uses CPM in understanding the information privacy regulation practices of Internet users. Metzger argued that Internet users erect boundaries around their personal information and formulate rules to decide when to disclose information.

She further claims that withholding information in the context of online exchanges is a common information privacy protection strategy and depends on the sensitivity of the information requested, which can be considered as an important guiding rule in privacy management. Information privacy concerns have been found to primarily contribute to Internet users' reluctance to share their personal information (Son & Kim, 2008). Information concealment or refusal to share personal information is seen both as an important aspect of privacy (Posner, 1984) and an exercise of control over one's personal information (Milne, Rohm, & Bahl, 2004).

People do not only withhold data but also falsify them as another information privacy protection strategy. People are most likely to falsify sensitive personal data, but not those deemed relevant for the completion of a specific online transaction (Metzger, 2007). The type of information that is requested is also an important indicator of whether or not people will decide to disclose their information - the more sensitive they are to the

requested information, the weaker are their intentions to disclose them online (Castaneda & Montoro, 2007).

Internet users are conscious about the amount and type of personal information they divulge online by limiting the amount of information that they will provide (Paine et al., 2007), which enables users to control the outflow of their information without the risks of forfeiting possible online benefits (Sheehan & Hoy, 1999). Metzger (2007) pointed out that people are wary about supplying their personal information whenever requested because they know that they have limited opportunities to negotiate mutually-accepted privacy rules. Such a limitation prompts them to erect privacy boundaries through information withholding and information falsification. People would probably have a lower inclination to withhold or fabricate their personal data if they will be adequately notified how data they will disclose will be used (Kobsa, 2007).

2.8 Risks perceptions and their influence on information withholding and incomplete information disclosure: the views of Protection Motivation Theory and Bounded Rationality

As already cited, the risks inherent in disclosing personal data online are bountiful. Sophisticated technologies enabling external parties to gain unauthorized access to Internet users' personal data are formidable threats to the vulnerability of online information privacy. One should not also forget that the ability of collecting organizations to exploit users' personal data for varied purposes is also intensified by the effortlessness on their part to transfer and share such data, with the use of available advanced technologies, to other parties in the digital environment - without the knowledge and consent of those to whom the data pertain.

From the perspective of protection motivation, the fear of compromising one's information privacy in the digital environment is a strong motivation for an individual to adopt some forms of privacy-protection strategies such as refusing to share personal data or opting to disclose incorrect or incomplete personal information. Protection Motivation Theory (PMT) postulates that protection motivation arises from the cognitive appraisal of a depicted event as noxious (threat severity) and likely to occur (probability of threat occurrence), along with the belief that a recommended coping response can effectively prevent the threatening event from happening (Rogers, 1975, 1983).

However, if the privacy threats are not appraised to be severe or as likely to occur, protection motivation would not be triggered (Rogers, 1983). We can only assume that when Internet users do not magnify the severity of the privacy threats and the likelihood that they will occur, their inclination to perform privacy protection behaviors would be low, which would probably result in their decision to supply correct and complete personal data for the completion of an online transaction.

Users' decision to share personal information completely and accurately might not always be shaped by their lowered assessment of the risks. There is also the possibility that they are not aware of the risks involved in the decision to share something about themselves. As Simon (1955) claimed, human beings, by nature, possess limited computational and predictive abilities, which make decision-making within a rational framework relatively crude.

The fact that people do not always have complete information primarily contributes to the 'boundedness' of human rationality (Simon, 1972). Individual decision processes with respect to information privacy are restrained not only by bounded rationality but also by incomplete information (Acquisti & Grossklags, 2005) and systematic deviations from rationality (Acquisti & Grossklags, 2005; Kobsa, 2007). Incomplete information becomes a problem for Internet users if they will just share personal information without being aware of the risks involved in the disclosure and without any knowledge of the ways to protect their personal information (Acquisti & Grossklags, 2004).

2.9 Trust and the lack thereof: their impact on information withholding and complete information disclosure

Threats to information privacy can be attributed either to the organization collecting the personal data or to external parties possessing the expertise and technology to acquire unauthorized access to users' personal data. These threats offer enough force to shove Internet users from sharing any information about themselves. Although users' awareness of the risks involved in online personal information disclosure could reduce their trust in an online organization soliciting for their information (Olivero & Lunt, 2004), there is substantial empirical support for the positive impact of trust in organizations and in their websites on users' intention and willingness to share personal data (Schoenbachler & Gordon, 2002; Zimmer et al., 2010).

Users' trust in this case is not one-dimensional, but is expected to target two organizational characteristics – the organization's ability to protect users' data from unwarranted external intrusion and its motivation and willingness to protect and to respect those data, considering its freedom to abuse them under any circumstance. When trust in either both or one of these two categories is missing, one can just expect users to refuse disclosing their personal information or they may even share fabricated information. This is in consonance with Zand's (1972) assertion that lack of trust in another party is deleterious to the disclosure of accurate, relevant, and complete information.

In deciding whether or not to trust organizations in terms of their ability and willingness to protect personal data, users may look for a number of cues. First, there is the privacy statement, which is expected to

inform users how their personal data will be used, processed, and protected. A couple of studies show that Internet users read online privacy statements either as a strategy to manage one's online information privacy (Milne & Culnan, 2004) or as a way to address information privacy concerns (Pan & Zinkhan, 2006).

Although it is also known that most Internet users do not bother to read privacy statements (Arcand et al., 2007; Jensen, Potts, & Jensen, 2005; Meinert, et al., 2004; Vu et al., 2007), they are most likely to trust organizations that post privacy statements on their websites (Pan & Zinkhan, 2006) and would feel greater control over their personal data when shared to organizations with websites that post privacy statements (Arcand et la., 2007). Aside from online privacy statements, Internet seals of approval from third-party certifying organizations, which help in endorsing organizational policies on privacy and security, have also been found to improve users' positive evaluation of the privacy practices of online organizations behind websites with those seals (Miyazaki & Krishnamurthy, 2002) and to encourage online information disclosure (LaRose & Rifon, 2007).

Concerns regarding unauthorized access to users' personal in organizational databases could also spur users to look for an indication of the deployment of security technologies to ensure the protection of their personal data, in particular, and their transactions, in general. Koufaris and Hampton-Sosa (2004) revealed that the presence of security mechanisms significantly increases users' trust in initial online exchanges. In fact, the presence of security measures on websites is regarded as more important than privacy statements and seals of approval in building Internet users' trust (Belanger, Hiller, & Smith, 2002).

Internet users also consider a positive organizational reputation when deciding to supply personal information for online transactions (Olivero & Lunt, 2004; Xie, Teo, & Wan, 2006). Users without any prior experience with an online organization consider its reputation as an indicator of its trustworthiness (Chen, 2006; Kim, Ferrin, & Rao, 2003; Koufaris and Hampton-Sosa, 2004; McKnight, Choudhoury, & Kacmar, 2002).

Organizations with a reputation to protect are not expected to engage in opportunistic behaviors that will result in the depreciation of their reputation (Herbig, Milewicz, & Golden, 1994), such as selling their clients' personal information to third parties. Indeed, Internet users will not hesitate to disclose their personal information to well-known online organizations with an image to maintain (Olivero & Lunt, 2004).

2.10 Only when the price is right: information withholding and complete information disclosure according to the social exchange perspective

People may claim that they value their information privacy (Ackerman, Carnor, & Reagle, 1999; Acquisti & Grossklags, 2005; Nehf, 2007; Strandburg, 2006), but with the estimated benefits of information disclosure, personal information can be traded (Nehf, 2007; Olivero & Lunt, 2004), which could eventually compromise information privacy. From a calculus-based perspective (Laufer & Wolfe, 1977), people will not hesitate to reveal, or even trade, their personal information, even it would mean jeopardizing their information privacy, if benefits can be expected (Berendt, Gunther, & Spiekermann, 2005; Norberg & Dholakia, 2003) and the calculated value of the benefits outweighs the estimated costs of information disclosure (Culnan & Bies, 2003; Olivero & Lunt, 2004).

The attachment of economic value to personal information is a crucial impetus for the recognition of information disclosure-benefits accumulation in online contexts as a form of economic exchange. Organizations are seeing the value of information from their clients (Henderson & Snyder, 1999), thereby prompting them to acquire such information in exchange for something. Internet users are most willing to sacrifice their 'priced' information if disclosure would result in the acquisition of something in return - either tangible or intangible.

From a social exchange perspective, human behavior and social interaction is an exchange of both tangible and intangible goods (Homans, 1958, 1961). People engaged in exchanges consider what they are giving up as a cost and what they are about to receive as a reward and their behavior changes less as profits (rewards minus costs) are maximized (Homans, 1958). Blau (1964) defined social exchange as the voluntary action of individuals who are motivated by the returns they are expected to bring and typically do in fact bring from others. Although social exchange can be seen as resembling economic exchange, with the principles of elementary economics perfectly reconcilable with those of elementary social behavior (Homans, 1961), the two perspectives on exchange differ in their conceptual cores (Emerson, 1987).

The entailment of unspecified obligations primarily differentiates social exchanges from economic exchanges (Blau, 1964). Blau underscored that while economic exchanges are moored on a formal contract that specifies the exact amount to be exchanged, the benefits involved in social exchange are not definitively priced in terms of a single quantitative medium of exchange, which is the reason why obligations in social exchanges are not specific. Emerson (1987) claimed that goods involved in social exchanges have subjective values.

In computer-mediated interactions, exchanges are common, not just involving material goods but also intangible ones. Setting aside online

shopping involving tangible commodities with defined prices, a pure economic exchange, non-material goods are also exchanged for non-material rewards and benefits. People sign in to become members of social networking sites, disclosing personal information in exchange for online membership to connect with other online members. People register with webmail services at the expense of sharing specific personal data just to have an email address. People request for documents and information from online organizations but requests can only be completed upon 'payment' of personal information.

Indeed, personal information, with its subjective value, can be traded for another commodity also with a subjective value (e.g. membership to a networking site) or another item with a defined price (e.g. gift check). One study indicated that while most respondents were relatively sensitive to online privacy concerns, some respondents showed a degree of willingness to disclose personal information in exchange for money or convenience (Hann, et al., 2007). In this case, people do consider the information collected from them as their input into an exchange with an online agent, and this spurs them to expect to receive something of value (Ashworth & Free, 2006).

As already mentioned, benefits can be tangible or intangible. Tangible benefits for the disclosure of personal information online could be vouchers, cash, or gift items. Rewards in the form of monetary vouchers have a positive impact on Internet users' decision to provide accurate personal information for personally identifiable data but not for demographic data (Xie et al., 2006). An important implication of this finding is that online users may be calculating the impact of disclosing a certain amount of information against the value of rewards to be received.

Could it be that the higher the reward is the greater also is the probability for the Internet user to disclose more sensitive information? According to Olivero and Lunt (2004), Internet users were willing to give away some degree of information privacy against rewards only for those personal data whose loss of control was deemed to be not too risky. This implies that users are calculating and balancing the information they will give with what they will receive in the exchange (Sheehan & Hoy, 2000). Figure 2.3 shows the calculative process involved in a decision to disclose or withhold information based on estimations of the value of the expected benefits that could be derived from the disclosure act.

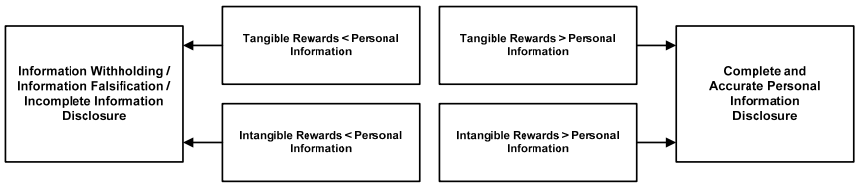

Figure 2.3. Diagram of cost-benefit calculations of information disclosure and information protection

Intangible benefits include the convenience of doing things online such as electronic shopping, gaining access to a range of Internet services such an emailing and joining online social networks, and experiencing the comforts of personalization and personalized services – all requiring the disclosure of personal information. According to a survey by Chellapa and Sin (2005), Internet users' value for personalization is almost two times more influential than their concern for privacy in determining usage of personalization services.

As Figure 2.3 indicates, people weigh the incalculable costs of their decisions to disclose personal data against the expected value of the benefits that they can derive from information sharing. It can be assumed that when the expected benefits from information disclosure do not outweigh the value attached to the personal data to be disclosed, information withholding or incomplete information disclosure could be forthcoming.

2.11 Other factors influencing information withholding and complete information disclosure

While the roles of risk perceptions, trust, and expected benefits are crucial in influencing people's decision to either withhold their personal data or disclose them accurately and completely, other factors certainly merit discussion. Users' 'degree of relationship' with organizations requesting for their personal data should not be discounted as an important influence, since users would not hesitate to share their data to online organizations with which they have established relationships (Olivero & Lunt, 2004).

Regardless of relational depth, people can still disclose personal information despite a preference for keeping such information private (Strandburg, 2006). Strandburg further argued that people share information not just for the benefits that can be derived from the sharing but also for the 'taste' of disclosure itself. In a study on information disclosure in social networking sites (Strater & Richter, 2007), it is known that some respondents admitted that they were not sure why they shared information, with others claiming that they had been so used to filling out forms that they did not even think twice before supplying any information.

Another recent investigation into the phenomenon of information sharing in networking sites reveals a relatively similar result – that despite concerns over online information privacy as substantiated by the use of available privacy settings, Internet users still displayed a general tendency to disclose information (Christofides, Muise, & Desmarais, 2009). Perhaps, this is true to people belonging to Westin's privacy unconcerned category – that online disclosure of personal information gives them a kick. Probably, those privacy fundamentalists will not view information disclosure as some kind of a stimulating drug but a toxic substance to be evaded.

Although it is apparent that some Internet users are used to the habit of information sharing when doing things online, even with a slight awareness of the possible risks involved in disclosure, such habitual disclosure might be influenced by users' trust propensity in a variety of situations, as well as by their prior experience with online disclosures. Trust propensity is regarded as a trait that leads to a generalized expectation about the trustworthiness of others (Mayer, Davis, & Schoorman, 1998). People with high levels of trust propensity might be willing to do something even without a consideration of the possible risks involved in the information disclosure act.

Internet users with more experience in online transactions requiring information disclosure are less concerned about online information privacy (Bellman et al., 2004; Cho et al., 2009; Metzger, 2004), in general, and are less concerned about privacy risks such as improper access to and unauthorized secondary use of data (Bellman et al., 2004), in particular. High levels of Internet experience would result in low information privacy concerns and risk perception, which would expectedly prompt a heightened intention to disclose personal information (Metzger, 2004).

2.12 Discussion

Pieces of personal information are like priced resources – expendable whenever necessary but may require utmost protection. The need to protect personal data in the online environment is rooted on the need to uphold information privacy. However, the relativity of information privacy has a strong bearing on how people deal with their personal information, especially in the online environment.

People's personal information-related behaviors can be a fixed on a pole – with information privacy protection behaviors such as information withholding and incomplete and inaccurate disclosure on one side, and information privacy-risking behaviors such as complete and accurate information disclosure on the other. Situated right at the middle of the pole is information-seeking behavior, which aims at accumulating the necessary information for users to be adequately informed of the ways organizations will use, process, and protect collected personal data from their clients. This behavior in manifested in users' intention to consult privacy statements on organizational websites.

Although the said behavior is not a prerequisite for information withholding or complete information disclosure, it is plausible to assume that users who are too engulfed by the risks involved in the sharing of their personal information would first resort to information-seeking behavior before deciding to withhold or completely share information about themselves. As mentioned previously, the accumulation of the necessary information on organizational usage and processing of Internet users'

personal information might not automatically result in complete information disclosure.

Users have to be convinced that collecting organizations will do that whatever they have indicated on their online privacy statements. Those who do not trust the claims of organizations might shy away from information disclosure and resort to information privacy protection behaviors. While perceptions of risks could easily thrust people to seek information, their levels of trust in organizations in terms of how they will use, process, and protect their clients' personal data (Vu et al., 2007) and their positive prior experience with those organizations (Milne & Culnan, 2004) could significantly reduce their intention to consult online privacy statements.

Information privacy protection behaviors in an online environment are often precipitated by privacy concerns, which are shaped by the belief that information disclosure is too risky due to the high probability of abuse either by the collecting organization or by external third parties. People who are highly concerned about their information privacy might magnify the risks involved in information disclosure, while those with minimal privacy concerns would be more inclined to underestimate the magnitude of risks. The impact of risks perceptions on privacy concerns should not also be discounted. People's estimation of the risks in information disclosure might even increase or decrease their levels of privacy concerns.

The degree of risk perception in an online sharing of personal information could be shaped by the appraised sensitivity of personal information to be divulged. One may not worry so much about disclosing one's preference in film or music, but the concern would surely be different when that same person is asked to indicate his or her income or disclose information regarding his or her health. Users' appraisal of the sensitivity of information requested by organizations would also be instrumental in driving users either to perform information privacy protection behaviors or prompt them to disclose information completely.

Complete personal information disclosure could be expected if users do not estimate high risks or when they are not aware of the risks in divulging their information or when they trust organizations' ability and willingness to protect their information. Users' level of trust could influence their risks perceptions, or their perceptions of the risks could have a bearing on their willingness to trust.

Users' lack of trust in organizations' ability and willingness to protect their clients' personal data have been found to strongly prompt them to withhold their personal data or disclose them incompletely and inaccurately. However, complete information disclosure is imminent when users trust that online organizations are competent in ensuring the protection of their clients' personal data and when those organizations are believed to have a close-to-nil propensity to abuse those data. Several empirical studies have indicated that trustworthiness cues such as privacy protection assurances, seals of approval, security features, and a positive

organizational reputation have a considerable impact on users' degree of trust in online organizations.

While some researchers argue that Internet users would be very willing to compromise their information privacy by disclosing their personal information in exchange for something in the digital environment, there is no denying that users can also be rational in dealing with information sharing. Rationality dictates that users weigh the benefits that can be gained from supplying their personal information for an online transaction against the costs (specifically the risks) of their intention to share their information. The premise is that when the benefits outweigh the costs, complete information disclosure could be expected. However, when the risks of information disclosure exceed the estimated value of the benefits expected from the disclosure, users might resort to privacy protection behaviors.

Nevertheless, other factors, which could be described as either rational or non-rational, should also be considered as important determinants of Internet users' intention to withhold their personal data, share them incompletely, or disclose them accurately. While trust, risk appraisal, and benefits calculation could be regarded as rational factors influencing personal information-related behaviors, non-rational elements have also been found to be important determinants of information withholding and information disclosure. Users with sufficient experience with online transactions are found to have low privacy concerns (Bellman, et al., 2004; Cho et al., 2009), which would most likely result in a heightened intention to share requested personal information. Habits also play a part. While some people, especially those privacy fundamentalists, may have the habit of refusing information disclosure under any circumstance; others, probably those 'privacy unconcerned', habitually share information regardless of the risks and the expected benefits.

An important rational factor that could also influence users' decision to withhold or disclose personal data is their appraisal of the relevance of the data for a transaction. The lesser is the relevance of the data for an exchange the lower will be the tendency of users to disclose them whenever requested. Figure 2.4 shows the different factors influencing different information privacy-related behaviors according to the postulations of the different theories discussed in this chapter.

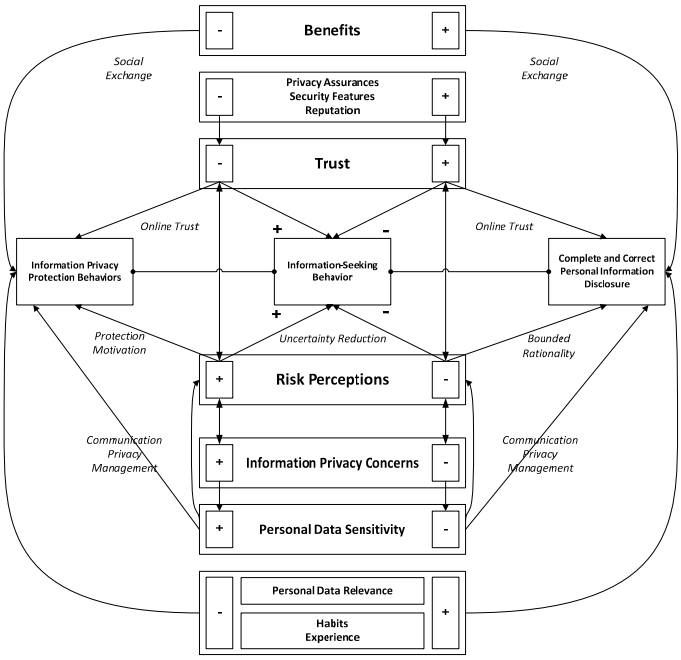

Figure 2.4. Different factors influencing different information-related behaviors according to the postulations of different theories

2.13 Conclusion

The complexity of personal information-related behaviors signifies the need to further investigations in this area using a comprehensive framework, which can benefit from different theoretical perspectives offering diverging insights into the determinants of users' decision to either withhold or share information. Users' information privacy concerns, which could be based on their estimation of the risks involved in online information sharing, are serious matters that every organization collecting personal information online should consider.

An organizational objective, therefore, is to reduce users' level of risk perceptions. This is only possible when online organizations can win users' Internet trust in the organization's ability and willingness to protect whatever personal data are collected from users. Several empirical studies, particularly in online commercial exchanges, have shown that users look for a number of cues to assess whether or not an organization can be trusted with their personal data. Because of privacy issues and the concerns regarding the security of personal data, users would expect that privacy statements and security features are available on websites used for the collection of data.

From a theoretical point-of-view, the impact of such cues on trust formation and risk perception reduction would depend on users' level of privacy concerns. For instance, privacy statements may not really mean so

much for people who have totally submitted to the belief that information disclosure is extremely risky (the privacy fundamentalists, in particular), but these documents may be forceful enough to sway those non-fundamentalist to share their information whenever asked online. We can postulate the same thing for the impact of perceived benefits on information disclosure intentions. However, these are just postulations that should merit the attention of future research agenda.

In order to predict the factors that motivate Internet users to withhold or share personal information during online transactions, it would be expedient to consider the premises of a number of theoretical perspectives, which would eventually result in a more exhaustive framework that would capture information disclosure behavior in different online transaction contexts.

It can also be noted that most of the empirical studies cited in this paper were conducted within the context of online commercial exchanges. This can be justified by the fact that studies on privacy concerns within the context of online non-commercial transactions are rather limited, or even non-existent. Findings from published studies on privacy in e-commerce, although may not be applicable in understanding privacy behavioral patterns within the context of online non-commercial transactions, are useful in providing a framework for understanding personal information disclosure and protection in non-commercial transactions, such as those in electronic government.

3

How shall I trust the faceless and the intangible? A literature review on the determinants of online trust

As underscored in the previous chapter, Internet users resort to various behavioral-based strategies to safeguard their information privacy. Decisions to share or withhold complete personal data for online transactions are often predicated on several considerations, just as different factors influence Internet users' reluctance to supply personal information whenever requested. For instance, from an exchange perspective, Internet users will not hesitate to share personal data when the estimated value of the expected benefit that can be derived from the disclosure act outweighs the 'cost' (or the risk) of information disclosure. Trust is also regarded as a crucial determinant of information disclosure intentions. While Chapter 2 initially discusses cues that would improve Internet users' trust in organizations within the virtual environment, this chapter takes a closer look at the many factors influencing online trust, as revealed in numerous empirical studies.

This chapter is based on a manuscript by Beldad, A., De Jong, M., & Steehouder, M. (2010), which has been published in Computers in Human Behavior, 26(5), 857-869.

3.1 Introduction

Perhaps the most important innovation of the last few years is the Internet technology, as it allows people to interact and transact with others without the constraints of time and space. Organizations can considerably thank the aforementioned technology for providing them with the possibility of extending their services outside their walled offices and shops. Probably people also have more reasons to be grateful about being able to buy things or avail of different services anytime, anywhere.

Nevertheless, the apparent blessings computer-mediated transactions bring may be countered by fear and anxiety. Transactions characterized as faceless and intangible are plagued with a host of concerns, which could result in people's reluctance to engage in any form of online transaction. The wider acceptance of online transactions, despite the perceived risks involved, depend not only on the estimated benefits they offer but also on people's trust in online transactions, in the technology used for the transactions, and in organizations as the other parties in the transactions.

Lack of trust in the organization as the other party in a transaction is often blamed for people's disinclination to engage in an online transaction (Hoffman, Novak, & Peralta, 1999), in general, and in online economic exchanges (Grabner-Kraeuter, 2002; Lee & Turban, 2001), in particular. In recent years, both the academe and the business sector have shown a heightened interest in trust within the digital environment. Knowing the nature of online trust and its determinants has become an important goal. This is obvious since online trust is regarded as a crucial factor for the success of an online enterprise or initiative.

In this chapter, the different determinants of online trust and the process involved in its formation, as identified in different empirical studies, will be discussed. Studies cited in this paper, however, were done mostly in the context of e-commerce, considering the profusion of investigations pursued in that domain. Since trust is also an important factor in the adoption of e-government (Belanger & Carter, 2008; Horst, Kuttschreuter, & Gutteling, 2007; Welch & Hinnant, 2002) and e-health (Sillence, Briggs, Fishwick, & Harris, 2004) services, results of a few studies on the determinants of online trust in those two contexts will also be included in the discussions.

In the first section of this chapter, the nature of trust, in general, will be explained according to the perspectives of psychology, social psychology, and sociology. The second section deals with the concept of online trust and how it differs from trust in an offline setting. The third section presents a comprehensive discussion of the different determinants or antecedents of online trust based on the results of different empirical studies. Determinants of trust are categorized into three, as introduced by Chen and Dhilon (2003): customer-/client-based, web-based, and company-/organization-based.

3.2 Trust – under a multidisciplinary microscope

3.2.1 The definition predicament

The problem with trust as a concept is that it does not have a universally accepted definition yet (Barber, 1983; Das & Teng, 2004; Kee & Knox, 1970; McKnight & Chervany, 2002; Rosseau, Sitkin, Burt, & Camerer, 1998). From the profusion of trust definitions emerges a two-way stream of trust conceptualization. The first centers on trust as an expectation regarding the behavior of an interaction partner (Barber, 1983; Koller, 1988; Luhmann, 1979; Rotter, 1967), whereas the second couples trust with the acceptance of and an exposure to vulnerability (Doney, Cannon, & Mullen, 1998; Mayer, Davis, & Schoorman, 1995; Rosseau et al., 1998; Zand, 1972).

Different disciplines treat trust as a research interest in significantly different ways. Lewicki and Bunker (1996) categorized trust research into three, as defined by a particular disciplinary perspective. First, trust is regarded as an individual feature from the viewpoint of personality theorists. Second, trust is considered as an expectation of another party in any interaction or transaction proposed by social psychologists. Third, trust is an institutional phenomenon according to sociologists and economists. This categorization will be the basis for the elaboration of the different conceptualizations of trust.

3.2.2 Trust as an individual feature

Viewed from the individual level, trust is best understood by looking at the psychology of the person. Such a perspective can explain why a person trusts and why trust declines or increases (Tyler & Kramer, 1996). Jones and George (1998) proposed the notion of trust as a psychological construct. As such, the interaction of an individual's values, attitudes, moods, and emotion is expected to result in an experience of trust (Jones & George, 1998).

Trust is also regarded as an attitude, which is neither subjective nor objective, and does not simply involve mechanical influences from the environment since it has to be learned (Luhmann, 1979). Viewing trust as a psychological state implies that people vary in terms of when and how much they are willing to trust. Such willingness to trust, according to Tyler and Kramer (1996), is based on people's estimation of the probability that those trusted will reciprocate the trust.

Some people are just more trusting than others, indicating substantial variations in their propensity or disposition to trust (Mayer et al., 1995), defined as the tendency for human beings to believe in the trustworthiness of others (Das & Teng, 2004). Claiming that individuals vary considerably in their trust propensity aptly corresponds to Rotter's (1980) proposition that in terms of trusting people can be positioned in a

spectrum from high to low. People's readiness to trust depends on the systemic nature of their personalities (Luhmann, 1979).

This readiness also varies from one person to another and from situation to situation (Worchel, 1979). Variations in propensity to trust among people can be attributed to their developmental experiences, personality types, and cultural backgrounds (Mayer et al., 1995). Trusting propensity or trusting impulse could be specific or general – it could refer to a specific category of people or it could encompass all people (Sztompka, 1999).

As a stable factor, trust determines the likelihood that people will trust, just as it influences how much they trust others prior to the availability of any data about them (Mayer et al., 1995). Rotter (1971) advanced that people's propensity to trust influences their levels of trust in their interactional partners, especially in cases when the former has limited knowledge about the latter.

In the model of initial trust formation by McKnight, Cummings, and Chervany (1998), propensity or disposition to trust is proposed to be one of the determinants of trusting intention. They identify two types of disposition to trust: faith in humanity and trusting stance. Faith in humanity refers to the belief that others are well-meaning and reliable; whereas trusting stance means that people believe that they will obtain better interpersonal outcomes by dealing with others as if they are well-meaning and reliable, regardless of whether those others are really reliable or not (McKnight et al., 1998).

McKnight, Choudhoury, and Kacmar (2002) defined trusting intention as people's willingness or intention to depend on their interactional partners. Willingness to depend (volitional preparedness to make oneself vulnerable to the trustee) and subjective probability of depending (perceived likelihood that one will depend on the other) form two distinct subconstructs of trusting intention (McKnight et al., 2002).

3.2.3 Trust as an expectation

Individuals would have no occasion or need to trust apart from their relationships with others (Lewis & Weigert, 1985). This assertion emphasizes the sociological function of trust instead of its supposed psychological function. Luhmann (1979) regarded trust as 'a generalized expectation that others will handle their freedom, their disturbing potential for diverse action, in keeping with their personalities – or, rather, in keeping with the personalities they have presented and made socially visible'.

Koller (1988) accentuated the association between trust and expectation by referring to trust as people's expectation that others are able and willing to behave promotively towards them, despite the freedom of the ones trusted to choose among alternative behaviors that could have negative consequences for those who trust.

To view trust as an expectation regarding the behavior of other people is to affirm that social relations and exchanges are not devoid of ambiguities. This implies that the necessity to engage in human transactions obliges individuals to resort to trusting behaviors despite the uncertainties that trail social contacts just for the sake of active participation in various social interactions. Luhmann (1979) asserted that trust reduces social complexity, as it simplifies life by the taking of a risk. In the later part of this chapter, the nature of trust as the acceptance of risk will be explained.

Barber (1983) identified three kinds of expectations in relation to trust: (1) an expectation of the persistence and fulfillment of the natural and social order, (2) an expectation of the technically competent role performance from those involved with an individual in social relationships, and (3) an expectation that partners in interactions will carry out their fiduciary obligations and responsibilities. The three presented perspectives on trust as an expectation highlight trustors' beliefs that the trustees are good and honest in dealing with the goods, material or non-material, entrusted to them despite their ability to cheat or betray the trustors.

Trust is partially a product of people's capacity to assess the trustworthiness of their potential partners (Sheppard & Sherman, 1998). Trust, therefore, can be considered as the reflected trustworthiness of the trustees and their trustworthiness that is subjectively entertained in the judgment of the trustors (Sztompka, 1999). The potential partners then have the burden of not only creating trust but also maintaining it and this process involves the duty of presenting themselves as trustworthy persons (Haas & Deseran, 1981). This corresponds to Goffman's (1959) presentation of the self theory, which proposes that people are constantly engaged in managing and controlling the impressions they make on others to attain their goals.

In assessing the trustworthiness of interaction partners, people can use a set of criteria to come up with a reliable assessment. These criteria or factors of trustworthiness (Mayer et al., 1995) include ability or competence (Barber, 1983; Luhmann, 1979; Mayer et al., 1995; McKnight et al., 1998), benevolence (Luhmann, 1979; Mayer et al., 1995; McKnight et al., 1998), integrity or honesty (Mayer et al., 1995; McKnight et al., 1998).

Based on the characterization of Mayer et al. (1995), parties in transactions are assessed to be trustworthy when they (1) have the required skills, competencies, and characteristics that enable them to exert influence within a specific domain – a description for the ability or competence criterion, (2) are believed to do good to trustors, setting aside an egocentric motive – thereby meeting the benevolence criterion, and (3) are perceived to adhere to a set of principles that trustors consider acceptable – a definition of integrity.

Sztompka (1999) also claimed that people employ three criteria in estimating the trustworthiness of their transactional partners: reputation, performance, and appearance. Reputation refers to a record of past deeds; whereas, performance includes actual deeds, present conduct, and

currently obtained results. Appearance also matters as one's look and self-presentation can exude trustworthiness or stimulate suspicion on the part of the looker (Sztompka, 1999).

3.2.4 Trust as acceptance of and exposure to vulnerability

When people trust they are increasing their vulnerability to others whose behavior they cannot control (Zand, 1972). Mayer et al. (1995) conceptualized trust as a willingness of people to be vulnerable to the actions of others based on the expectation that the latter will perform a particular action important to the former, irrespective of the ability to monitor and control the latter.

The idea of being vulnerable when trusting skews towards the realization that while uncertainties and ambiguities are abounding in all forms of exchanges and transactions, risks creep underneath. Doney et al. (1998) claimed that sources of risks are related to vulnerability and/or uncertainty about an outcome. Trust can be regarded as people's behavioral reliance on others on a condition of risk (Currall & Judge, 1995).

And so we can ask: do we trust because there are risks or do we take risks because we trust? The first question emphasizes that risks determine trust (Koller, 1988; Lewis & Weigert, 1985), while the second question supposes that trust is an antecedent of risk-taking behavior in any relationship, in which the form of risk-taking, according to Mayer et al. (1995), is dependent on the situation. People's level of trust in their interaction partners is positively related to the perceived risks present in the situation. This means that an increase in risk perceptions could result in the augmentation of people's degree of trust (Koller, 1988; Mayer et al., 1995).

Even when risk is negligible in an exchange situation, trust is still necessary as long as the possibility for trust to be betrayed exists (Kee & Knox, 1970). Risk is indispensable in the cultivation of trust because trust would not be necessary if actions could be pursued with absolute certainty (Lewis & Weigert, 1985).

We can either have complete or incomplete information, or even, without any information at all, regarding the chances of our trust being reciprocated. In Bachmann's (1998) view, trust is necessary in situations in which trustors have partial information about the factors that will possibly influence trustees' future behavior. Luhmann (1979) stated that in reality there is less information than required to be assured of success when trusting. This assertion cements the exigency of trust in an environment abounding in uncertainties and ambiguities.

3.2.5 Trust as an institutional phenomenon

From a sociological perspective, trust should be viewed as a property of collective units (dyads, groups, and collectivities), and not of isolated individuals. As a collective attribute, trust is applicable to the relations among individuals rather than to their psychological states taken

individually (Lewis & Weigert, 1985). From the perspective of social exchange, human interactions are grounded on exchanges involving material and non-material goods (Blau, 1964; Homans, 1958, 1961).

As mentioned in the previous chapter, social exchange centers on the voluntary action of individuals who are motivated by the returns they are expected to bring and typically do in fact bring from others (Blau, 1964). Blau added that the benefits involved in social exchange are not definitively priced in terms of a single quantitative medium of exchange. This is the reason why obligations in social exchanges are not specific, while economic exchanges are moored on a formal contract that specifies the exact amount to be exchanged. Though both exchanges conceptually differ (Emerson, 1987), both also depend on trust for their continuation and completion (Buskens, 1998; Doney et al., 1998; James, 2002), just as both exchanges involved varying amounts of uncertainty and risks (Molm, Takahashi, & Peterson, 2000).

Groups, organizations, and institutions must also work together. Pronounced division of labor results in strong ties of dependence, and trust is a requirement for effective operation (Sztompka, 1999). Within the framework of social relations, trust is a product of people's dependency on others, since people have needs that require the services of others and trust must be dealt with (Kipnis, 1996). Viewing trust as an institutional phenomenon indicates the need to acknowledge that trust is not only confined within interpersonal relations but also extends to relations between a person and an organization and between organizations or institutions (Lewicki & Bunker, 1996).

Trust is essential in economic exchanges. Viewed from an economic standpoint, trust is an expectation that people will not be exploited by others, which exists when there are no strong incentives for people to behave opportunistically (James, 2002). Hosmer (1995) referred to trust as the reliance by one person, group, or firm upon a voluntarily accepted duty on the part of another person, group, or firm to recognize and protect the rights and interests of all parties engaged in a cooperative endeavor or economic exchange.

In most economic exchanges, not everything can be verified before the occurrence of a transaction, thereby making the elimination of risks impossible and thereby necessitating trust (Tullber, 2008). For instance, within marketing, customers need to determine the extent to which they trust the company and its personnel to make purchases and long-term relational commitments (Doney & Cannon, 1997).

3.2.6 The rationality and irrationality of trust

People as *homo economicus* often calculate the costs and projected outcomes of their decisions to trust. From a rational perspective, trusting involves expectations about interaction partners based on calculations which weigh the cost and benefits of certain courses of action to either the trustors or the trustees (Lane, 1998). Sztompka (1999) echoed a similar view

by emphasizing that from a rational-choice perspective, both trustors and the trustees are rational actors attempting to maximize their utilities (the goals realized, benefits achieved, profits obtained minus costs incurred) by rational calculations using whatever information is available.

Uncertainties in social relationships prompt calculativeness and a preference for shorter term returns (Anderson, 1971, as cited by Chadwick-Jones, 1976). The degree of calculativeness in trusting relationships changes both with the contexts and the objects of the trust, just as it varies according to the stages of trusting relationships (Lane, 1998).

The claim for the rationality of trust is grounded on the justification that it is based on empirically grounded expectations of other people's or institutions' behavior (Hardin, 1991). Rational trust, therefore, implies that people fastidiously define how much trust they grant to whom – that their trust varies according to situations and to the level of relationships they have with their interaction partners. Furthermore, trusting behavior from a rational perspective involves people trusting those proven not to betray their trust.

However, the rational-choice perspective on trusting behaviour is criticized for its failure to accommodate large, highly risky trusting acts that occur early in a relationship (Weber, Malhotra, & Murnighan, 2005). Citing the experimental study on investment game by Berg, Dickhaut, and McCabe (1995), Weber et al. (2005) noted that in some cases people display a willingness to trust people they do not know and will never meet or see.

Another flaw in the rational choice approach, according to Weber et al. (2005), is the tendency to view trustors and trustees symmetrically under the premise that each party interprets each other's actions similarly. They add that although many trusting relationships develop between parties with congruous perspectives on relevant matters, the likelihood that trusting parties will be asymmetrically dependent on their relationships is incontrovertible. Hardin (1991) himself admitted that although trust is grounded on instrumental motives, such as the initiation and completion of an exchange or the pursuit of common goals, trust can also depend on non-rational factors such as love or altruism and may involve a loose confluence of diverging interests.

In extreme cases, trust is even necessary when people are in desperate situations from which they cannot extricate themselves without help (Coleman, 1990). This exemplifies the scenario of two parties having an asymmetrical dependency in a trusting relation – one is dependent on the other, but not the other way around. In such a situation, as the dependency of trustors on trustees increases, the former will (a) lower information search to assess the latter's trustworthiness; (b) be more inclined to appraised ambiguous information about the latter positively; (c) exaggerate the probability that the latter will reciprocate; (d) be more likely to engage in initial trust acts; and (e) be increasingly prompted to trust carelessly (Weber et al., 2005).

3.3 From offline trust to online trust

Online trust is defined as an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited (Corritore, Kracher, & Wiedenbeck, 2003). Online trust is also viewed as reliance on a firm by its stakeholders with regard to the firm's business activities in the electronic medium, and in particular, its website (Shankar, Urban, & Sultan, 2002). While the first definition applies to online interactions in general, the second definition is more appropriate when understanding online trust in the context of online economic exchanges.

Is there a difference between how people trust others in the physical world and how they trust others when they are in an online environment? Corritore et al. (2003) proposed that to understand online trust one should resort to existing works on offline trust, as results of a substantial number of studies on trust in offline settings are applicable to trust in online environments. They add that the common denominator between the two is their rootedness on exchange, which, in both settings, is hampered by risks, fear, costs, and complexities. Therefore, the notions of trust as an acceptance of and exposure to vulnerability and as an expectation regarding the behavior of the interaction partner are valid when applied in online relationships and exchanges.

Just like in offline interactions, the targets of trust in online transactions also have the burden of presenting themselves as trustworthy parties (Haas & Deseran, 1981). To be assessed as trustworthy, online organizations must work to improve their reputation, performance, and appearance – with appearance corresponding to the design of their website interface, for instance. At the same time, Internet users hold the prerogative to assess the trustworthiness of their online transactional partners based on the criteria of competence, benevolence, and integrity. More importantly, in understanding online trust from a purely economic perspective, the economic definitions of trust (Hosmer, 1995; James, 2002) should be appropriate.

However, differences are also inherent between offline and online trust. Quoting Marcella (1999), Shankar et al. (2002) differentiated offline trust from online trust by focusing on their trust targets. In trusting offline, the object of trust is typically a person or an entity (organization); whereas in an online context, the technology (primarily the Internet) and the organization deploying the technology are the proper objects of trust.

From a marketing perspective, in contrast to traditional commerce, where the objects of customers' trust are only the sellers or the companies they represent (Doney & Cannon, 1997), customers in electronic commerce have to trust not only the website but also the company behind the site, and even an explanation of why the site is trustworthy (Boyd, 2003). These points accentuate the complicated nature of trust in online commercial exchanges.

The unpredictable nature of the Internet breeds environmental uncertainties that spawn risks (Pavlou, 2003). In online transactions two uncertainties are certain: the risk of losing one's money during the exchange and the threat of having one's private sphere penetrated. The inevitability of risks may necessitate the cultivation of trust if one really intends to engage in online exchanges and savor their potential benefits without the constant fear of the risks present.

3.4 Determinants of online trust

The inevitability of a 'first-time' in online situations makes trusting strenuous (Boyd, 2003). This suggests that people who lacked experience with online transactions and with online organizations would have a totally different level of trust compared to those with enough experience. Therefore, if trust among those with experience is grounded on the quality of and satisfaction with their previous transactions, what would be the bases of trust for those without any experience?

Empirical studies on the determinants of trust and perceptions of trustworthiness in online exchanges abound. Different studies identify different trust cues that could influence Internet users' trust in online transactions and in online organizations. According to Grabner-Kraeuter (2002), the willingness of users to make a risky advanced concession (disclosing credit card information, for example) depends on their evaluation not only of the sellers' trustworthiness, but also of the functionality and reliability of the electronic commerce system.

In this chapter, the determinants of trust are categorized into three: Internet user-based, website-based, and organization/company-based. The discussion of the different determinants of trust in online transactions is based on the results of different empirical studies on trust in electronic exchanges, primarily in the context of e-commerce, and sporadically, within the contexts of e-government and e-health.

3.4.1 Internet user-based trust determinants

3.4.1.1 Propensity to trust

Individuals vary in the amount of trust they extend to their exchange partners (Mayer et al., 1995). In the context of online economic exchanges, some customers display a greater disposition to trust anything and anybody and are more likely to trust a web vendor despite having only limited information about it, whereas others need more information to form trusting beliefs (Salam, Iyer, Palvia, & Singh, 2005). However, empirical studies on the impact of propensity to trust on the formation of online trust yielded conflicting results.

Studies have shown that propensity to trust has a positive effect on online trust formation (Gefen, 2000; Teo & Liu, 2007). Gefen (2000) argued

that since propensity to trust is built over a lifelong period and reflects social influence over extended period, it should be expected that trust would vary across cultures. Differences in the degrees of trust in and the rates of adoption of computer-mediated exchanges among different cultures are a given.

Koufaris and Hampton-Sosa (2004), however, found no statistical support for the assumption that propensity to trust affects initial online trust in the company. They posited that when customers have no prior experience with a company, they may ignore their general tendencies to trust others, and instead form their trust beliefs based on their perceptions about the company and its website.

Propensity to trust facilitates either the magnification or the reduction of the impact of website attributes as trustworthiness cues (Lee & Turban, 2001). The moderation effect of propensity to trust is directly related to the formation of trust based on the trust attributes of the system. Thus, it is argued that the higher the person's level of trust propensity, the greater is the impact of the attributes on trust formation.

3.4.1.2 Experience and proficiency in Internet usage

Metzger (2006) attributed customers' perception of risks to their levels of experience with online commerce, as compared to their experiences with traditional forms of exchanges. From this assertion, it can be hypothesized that people who are highly proficient with the web are more likely to have low perceptions of risks in using the web and be more inclined to trust online transactions. Proficiency in web usage can be understood to mean the skills of customers in using computer technology.

Results of a study by Corbitt, Thanasankit, and Yi (2003) showed that customers' level of Internet experience is positively related to the degree of trust in an e-commerce website. The researchers claimed that customers' level of Internet experience is likely to affect their tendency to trust the technology, which may also enhance their trust in electronic commerce.

A study by Aiken and Bousch (2006), however, revealed that the relationship between Internet experience and online trust is positive in the case of novice and intermediate users, and negative in the case of intermediate and expert users. Describing such relationship as an inverted U, the authors claimed that people's trust increases in the early stages when their Internet experience also increases. At higher levels of experience, trust declines when they accumulate more knowledge about possibilities that things could go wrong, which increases their privacy and security concerns.

3.4.2 Website-based trust determinants

3.4.2.1 Perceived ease of use of the website

One of the important variables in the technology acceptance model of Davis (1989) is the perceived ease of using a particular technology – referring to the degree to which people believe that using a particular system would be relatively easy. Perceived ease of use in the context of electronic services centers on the navigational structure of the website, which includes search functions, site maps, product indices, and the overall design and organization of the websites (Lohse & Spiller, 1998). Grabner-Kraeuter (2002) postulated that effective navigation is one of the best ways in communicating trustworthiness in the online exchange environment.

The impact of perceived ease of use on the formation of trust in e-commerce has been supported in several empirical studies (Bart, Shankar, Sultan, & Urban, 2005; Chen, 2006; Flavian, Guinaliu, & Gurrea, 2006; Koufaris & Hampton-Sosa, 2004). A large-scale study on the determinants of trust in different types of websites disclosed that electronic vendors whose websites have easy-to-use features and have the capability to direct their customers to their destinations quickly can easily gain the trust of their customers (Bart et al., 2005).

It has been noted that the ease of using and navigating a website can significantly influence customers' trust in the electronic vendor, especially during the initial encounter, for instance, when customers are still searching for information (Chau et al., 2007). Flavian et al. (2006) argued that low levels of usability may generate technical errors, which could increase customers' feelings of distrust and could discourage them from ever engaging in subsequent online exchanges.

3.4.2.2 Information quality

As Internet users expect that any website should be free from errors (Bart et al., 2005), they are likely to trust websites that contain accurate, current, and complete information (Kim, Song, Braynoy, & Rao, 2005) and those that adhere to the rules of correct spelling, grammar, and syntax (Koehn, 2003). According to Liao, Palvia, and Lin (2006), the content quality of an e-vendor's website (referring to the usefulness, accuracy, and completeness of the information offered) may increase customers' trust in online transactions. They added that since customers are not in the position to touch and feel the item in online shopping, they require detailed and clear information to decide on the purchase.

The quality of information on e-health websites is also crucial for the development of trust in the e-health services. Empirical investigations by Sillence et al. (2004) and Sillence, Briggs, Harris, and Fishwick (2007) revealed that users of e-health sites trusted sites that can demonstrate in-depth knowledge of a wide variety of relevant topics and deliver clear information.

3.4.2.3 Graphical characteristics

Kim and Moon (1998) investigated the impact of a website's graphical characteristics by manipulating elements such as clip arts and colors in the design of an online banking website. The study found out that an interface without a clipart aroused feelings of untrustworthiness on the part of customers, while a screen with three-dimensional, dynamic clipart enhanced the users' feelings of trustworthiness towards the banking system. It was also known that the color layout of the interface is important in augmenting customers' perception of the online bank's trustworthiness.

Colors of low brightness and those that were used symmetrically induced feelings of trustworthiness, while bright colors that were used asymmetrically resulted in a decreased perception of the system's trustworthiness. Since the said study was conducted within a very specific context, one should be cautious in generalizing the effects of colors on online trust.

3.4.2.4 Social presence cues

The virtual nature of online transactions characterized by a deficiency in face-to-face contact and visual cues poses a hindrance to the germination of online trust among Internet users (Ridings, Gefen, & Arinze, 2002). Replicating a physical interaction with its sets of interpersonal cues in the context of online exchange may be a feasible method to promote online trust. It can be assumed that the infusion of social presence in websites for online transactions may increase users' trust in online organizations.

Social presence refers to the degree of salience of the person in the interaction and the consequent salience of the interpersonal relationships (Short, Williams, & Christie, 1976). Within the context of online interaction, social presence can be viewed as the degree of feeling, perception, and reaction of being connected by computer-medicated communication to another intellectual entity through a text-based encounter (Tu & McIsaac, 2002).

The degree of social presence is determined not only by the characteristics of the medium and users' perception (Tu, 2002a; Tu & McIsaac, 2002), but also by users' activities (Tu, 2002a). Perception of online social presence can be influenced by social relationships, trust, user's characteristics and perceptions of online environments, attributes of the communication media, user's computer literacy, use of paralanguage and emoticons, communication styles, task types, and privacy (Tu, 2002b). Social presence has a positive impact on users' identification with online groups and communities (Schimke, Stoeger, & Ziegler, 2007) and on their intention to participate in online interactions (Tu & McIsaac, 2002).

Gefen and Straub (2004) underscored that although a website is devoid of actual human interaction the perception that there is social presence increases online trust. This suggests that the perception of social

presence in a website with its resemblance to an interpersonal interaction is probably important in e-commerce, even though customers usually interact with the site rather than with a flesh-and-blood salesperson. A couple of empirical studies (Cyr, Hassanein, Head, & Ivanov, 2007; Hassanein & Head, 2004) revealed that perceived social presence positively impacts not only users' trust in the website, but also their perceptions of the website's usefulness and the enjoyment they can derive from using the site.

Efforts to heighten the perception of social presence in the websites of e-vendors primarily involved the use of photographs (Riegelsberger & Sasse, 2002; Riegelsberger, Sasse, & McCarthy, 2003; Steinbrueck et al., 2002), although empirical studies yielded incongruent conclusions. Steinbrueck et al. (2002) noted that using photographs in the electronic vendor's website is effective in creating social presence since the said strategy brings the impersonal nature of electronic transaction closer to face-to-face commercial exchange – thereby increasing an e-vendor's trustworthiness.

Riegelsberger et al. (2003), however, discovered that the presence of photos on a website had no effect on online trust, admitting that there is no simple heuristic on the types of photos that could increase online trust. In another experiment, Riegelsberger and Sasse (2002) pointed out that reactions to photographs on websites can range from suspicion to enthusiasm. While some users were positive about the inclusion of photographs on a website, others rejected photographs as they only cluttered the site and did not offer added functionality. Photographs were also considered as attempts at manipulating customers' online trust (Riegelsberger & Sasse, 2002).

3.4.2.5 Customization and personalization capacity

Customization implies that electronic vendors have the ability to tailor products, services, and transactional environments to their target users (Srinivasan, Anderson, & Ponnavolu, 2002). Existing literature tends to use the concepts of customization and personalization to denote the same thing. Therefore, points related to these two constructs in the context of trust in online transactions will be consolidated in this discussion.

Results of a study by Koufaris and Hampton-Sosa (2004) indicated that the willingness of online organizations to customize their products and services is an important determinant of people's initial trust in the organizations. The researchers argued that online organizations with customization or personalization capabilities can be considered as capable of serving their clients better.

Briggs, Simpson, and De Angeli (2004) hypothesized a reciprocal relationship between trust and personalization. Trust is not only a prerequisite for a good personalization practice; good personalization is also a condition for the formation of online trust. However, the results of their survey showed that personalization only had a relatively small impact on trust-creation.

Personalization can also have a detrimental effect on trust formation since it requires the collection of personal information, directly or indirectly, from Internet users. Concerns for online privacy could adversely influence the impact of personalization on online trust formation. However, these propositions could be a starting point in understanding whether or not personalization really influences online trust.

3.4.2.6 Privacy assurances and security features

It has been mentioned previously that first-time online customers have greater concerns about the security of online transactions than their experienced counterparts (Koufaris & Hampton-Sosa, 2004). When customers evaluate the trustworthiness of an organization online, privacy and security are taken as vital criteria in the assessment (Aiken & Bousch, 2006).

Privacy concerns have been pointed out as a significant factor for customers to trust or distrust e-commerce (Hoffman et al., 1999). These concerns include receiving spam mails, being tracked for their Internet usage history and preference through cookies, having their confidential information accessed by third parties through malicious programs, and being at the mercy of companies with the prerogative on how to use customers' personal data (Wang, Lee, & Wang, 1999).

In one survey (Lauer & Deng, 2007) it is known that the introduction of stronger privacy policies in a company's website could result in a higher perception of the company's trustworthiness. A number of studies (Arcand, Nantel, Arles-Dufour, & Vincent, 2007; Jensen, Potts, & Jensen, 2005; Vu et al., 2007), however, revealed that most Internet users do not even bother to consult or read online organizations' privacy statements before disclosing their personal data for different online transactions.

An experiment by Pan and Zinkhan (2006) reported that the mere presence of a privacy policy would be sufficient to persuade Internet users that an online organization can be trusted and would be expected to respect and protect their personal data. To understand this behavior we should refer to the Elaboration Likelihood Model (ELM).

ELM postulates that people are motivated to hold correct attitudes but the amount and nature of issue-relevant elaboration in which they are willing to engage to evaluate a message vary with the individual and situational factors. Therefore, as the motivation and/or the ability to process messages and arguments decreased, peripheral cues, such as the presence of a privacy statement on a website, become important determinants of persuasion (Petty & Cacioppo, 1986), specifically the determinants of the trustworthiness of an online organization.

Another study showed that transaction security significantly affects online trust (Yoon, 2002). This is consonance with the finding of one research that respondents ranked security features as more important than privacy statements, security seals and privacy seals (Belanger, Hiller, & Smith, 2002). However, that same study also noted that the presence of one

of these security and privacy features led to a desire, on the part of customers, for the others as well.

Belanger et al. (2002) further argued that although security is ranked higher than privacy, online organizations should seriously consider including strong privacy statements and security features to earn customers' trust. They attributed the pattern of the ranking (security higher than privacy) to the possibility that security features are better understood and easier to identify than privacy statements, which could mean different things to different people. Nevertheless, they also claimed that these features may not be sufficient to earn customers' trust since other characteristics may also be of influence (e.g., the company's reputation, website cosmetics, and other website features).

3.4.2.7 Third-party guarantees

The application of third-party guarantees to bolster trust in online transactions with online organizations is in consonance with the concept of trust-creation based on the transference process (Doney et al., 1998). Doney et al. (1998) stressed that the formation of trust through transference process requires the identification of proof sources and the establishment of links between the known entities or proof sources (third parties) and the unknown ones (online organizations that the third-party recommends as trustworthy), provided that those third parties that act as proof sources are themselves trustworthy.

Certifications from trusted third parties may compensate for an e-vendor's lack of transactional history with its customer, especially in the initial encounter (Koehn, 2003). Third-party recognitions – in the form of seals of approval such as TRUSTe or BBBOnline – are effective in promoting customers' trust in online shopping. Such seals of approval help in endorsing the privacy and security policies of electronic vendors (Cheung & Lee, 2006).

Kimery and McCord (2002) distinguished three types of third-party assurances: privacy assurance, process assurance, and technology assurance. Privacy assurance gives information about the organization's compliance with privacy policies, while process assurance emphasizes the organization's observance of standards on internal business processes or order fulfilment. An indication of an online organization's use of technologies that enable secure and reliable order and payment handling is referred to as technology assurance.

Results from their study on third-party assurances in online transactions, however, show that third-party assurance seals had no significant effect on customers' view of the e-vendor's trustworthiness. Kimery and McCord (2002) attributed the absence of effects to the participants' relative unfamiliarity with third-party assurance seals.

3.4.3 Company/organization-based trust antecedents

3.4.3.1 Organizational reputation

The existence of a positive organizational reputation results in a more open and trusting relationship between clients and organizations, whereas the opposite is true if the reputation is negative (Smeltzer, 1997). Since reputation stems from organizations' trustworthy behaviors (Hosmer, 1995), repeated failures on the part of organizations to fulfil their intentions could eventually result in the depreciation of their reputation (Herbig, Milewicz, & Golden, 1994).

The definition of reputation within the electronic commerce paradigm can be understood in these two points. First, it is a collective measure of trustworthiness based on referrals or ratings from members of a particular community (Josang, Ismail, & Boyd, 2007). Second, it is an indication of an organization's credibility, which results from the comparison between what an organization promises and what it actually fulfils (Casalo, Flavian, & Guinaliu, 2007). Three important factors precipitate the formation of a positive online reputation: through positive exposure, through third-party assessments such as the rating services proliferating on the web, and indirectly through the linking of websites (Toms & Taves, 2004).

The construction of a positive online organizational reputation can also be anchored on the collection of Internet users' reviews and feedbacks on their experiences with online organizations (Resnick, Zeckhauser, Friedman, & Kuwabara, 2000). Pieces of second-hand information, such as feedbacks from friends and word-of-mouth comments from other customers, can also impact users' online trust (Walczuch & Lundgren, 2004). Thus, online organizations that allow their clients to post reviews on purchased products, for instance, can be regarded as promoting trust (Koehn, 2003).

Results of a number of empirical studies revealed that the positive reputation of an e-vendor (Chen, 2006; McKnight et al., 2002; Teo & Liu, 2007) and word-of-mouth within one's social network, particularly positive referrals, (Kuan & Bock, 2007) significantly influence clients' trust in online organizations. Customers who do not have previous experience with an online vendor also rely on the reputation of that vendor, which the former can use to assess the trustworthiness of the latter (Chen, 2006; Kim, Ferrin, & Rao, 2003; Koufaris & Hampton-Sosa, 2004; McKnight et al., 2002). Within the e-health context, users are more likely to trust websites owned by well-known and well-respected organizations (Sillence et al., 2004, 2007).

3.4.3.2 Offline presence

The Internet propelled the branching out of retailing channels from bricks-and-mortar to pure clicking, which eventually evolved into brick-and-clicks (Ranganathan, Goode, & Ramaprasad, 2003). With the difficulty

on the part of Internet users to trust most online transactions, it can be presumed that online companies with offline presence are in a better position to promote the trustworthiness of their clients' online transactions with them. Kuan and Bock (2007) claimed that customers' trust in the offline presence of the online retailer enhances customer's online trust. They added that customers rely on their offline experiences with the online retailer's physical store as an information channel to build trust.

However, another study indicated that retailer's offline presence, referred to in the aforementioned survey as multichannel integration, is not significantly related to online trust (Teo & Liu, 2007). The researchers argued that that the absence of relation between the two constructs could be due to the low prices of product purchased online, minimal efforts on increasing integration level, and customers not having a clear concept of the integration of communication channels.

3.4.3.3 Experience and familiarity with the organization

People are usually ready to trust those whose trustworthiness has been tested and those who did not fail them before (Sztompka, 1999). This assertion accentuates the relevance of experience in trust formation. Internet users' experiences with online transactions can be positioned in a negative-positive spectrum. The online shopping experience can be enjoyable, gratifying, or satisfying; just as it can also be frustrating, disappointing, or discouraging. Pavlou (2003) maintained that a positive relationship exists between customer satisfaction and trust, since customers who are satisfied with their online shopping experience tend to trust the electronic vendor for a possible second transaction.

Results of a number of empirical studies (Casalo et al., 2007; Flavian et al.,2006; Yoon, 2002) suggested that customers' satisfaction with their previous transactions with a particular online organization determines their trust in that organization. Satisfaction with previous online transactions affects not only users' trust but can also induce greater usage and familiarity (Yoon, 2002).

Familiarity is imperative in the cultivation of trust (Mollering, 2006), since trust is only possible within a familiar world (Luhmann, 1979). The relation between familiarity and trust is grounded on the premise that trust in people and organizations develops when they behave in accordance with trustees' positive expectations of them (Gefen, 2000). Gefen's (2000) experiential survey found out that familiarity significantly influenced online trust, just as it determined clients' online behavioral intentions such as intention to inquire about a product and intention to buy online.

3.5 Discussion, conclusion, and future directions

The success of an online service initiative, whether commercial or non-commercial, depends not only on the subjective benefits it brings but also on the level of trust users have on the aforementioned initiative, the technology used for service delivery, and the party behind the service. Knowing how online trust can be developed and maintained is imperative in an era when organizations increasingly rely on the Internet for the delivery of their goods and services. Failure on the part of those organizations to acquire their clients' trust could significantly thwart users from engaging in online transactions with the organizations.

Different empirical studies on online trust identify different determinants of online trust, primarily, in the context of online commercial exchanges, and secondarily, in the context of online non-commercial transactions. The development of online trust can be influenced either by users' experience with the technology used for the transaction or just by their tendency to trust (Internet user-based trust determinants) or by the quality of the website used for the transaction or the presence of security assurances on the website (web-based trust determinants) or by their experiences with online organizations or by the reputation of those organizations (organization-based trust determinants).

Review of empirical studies on trust, however, discovered contradictions in the results of those studies. For instance, while one study showed that using photographs to increase perceptions of social presence influences online trust, another study offered a totally different conclusion. Disparities in results imply that the effects of some online trustworthiness cues on trust formation do not transcend contextual differences and are, therefore, relative and could depend on the context of a particular online transaction and the parties involved in the transaction. While third party guarantees could enhance trust in online commercial organizations, the impact of the aforementioned factor on trust in government organizations in the digital environment may even be low or absent.

Divergence in research results has strong implications for future research interests, both in the contexts of online commercial exchanges and non-commercial transactions. It is, therefore, justified to assert that the possible effects of different trustworthiness cues on the development of trust in online transactions according to different contexts are issues that merit further investigation.

Important points acquired from a review of different empirical studies on online trust in various contexts served as bases for a number of recommendations for possible research agenda. Only a handful of studies cited in this paper used a comprehensive model in predicting the factors that contribute to the development of Internet users' trust. Using a more complete framework that incorporates all possible personality-based (e.g., experience with the Internet and with online transactions), socio-psychological (e.g., propensity to trust, perception of risks involved in the

exchange), sociological (e.g., reputation, third-party certification), socio-cultural (e.g., culture, education), and technical (e.g., website quality) factors would be very beneficial in empirical attempts at understanding online trust development.

Studies on trust in e-commerce have not given so much attention on the influence of risk perception on trust formation, as shown by the studies that are reviewed in this article. Since risk intertwines with trust, the influence of the latter on the formation of the former could not be discredited. The reality of online risks, primarily the possible loss of online privacy in the case of e-government transactions, for instance, could significantly influence online trust. Thus, including risk perception in a model that aims at determining online trust determinants would result in a more exhaustive theoretical framework of online trust.

There is also an apparent imbalance between studies on trust in e-commerce and trust in non-commercial transactions, such as those in e-government and e-health. While it has been accentuated that trust is crucial in the adoption of e-government services, available studies on trust in that area are still very few, compared to the sizeable number of similar studies in the e-commerce context. Even those trust studies in e-government have not really investigated the determinants of online trust in e-government transactions. The case of trust studies in e-health is similar to that of e-government, as published papers of empirical studies on trust in e-health are also considerably limited. This indicates that trust in the aforementioned area is still on its infancy phase.

Although e-commerce, e-government, and e-health are substantially different in terms of the nature of their operations and their services and in terms of their target clients, their similarities lie on their dependence on the Internet technology for the delivery of their services to their clients. This significantly contributes to the facelessness and intangibility of online transactions, and thereby fuelling heightened perceptions of online risks that could discourage people from doing things online. These commonalities could sufficiently justify the assertion that a comprehensive model that aims at determining trust antecedents in electronic commerce is also applicable in understanding trust formation process in non-commercial online transactions, such as those in e-government and e-health.

4

Trust, information privacy issues, and security concerns in e-government transactions: Results of focus group discussions with Dutch Internet users

Chapters 2 and 3 introduced the concepts of online information privacy and online trust from a multidisciplinary perspective. While the second chapter concentrated on the different information privacy-related behaviors of Internet users, the third chapter focused on various cues and factors that positively influence online trust. This chapter discusses the results of three focus group discussion (FGD) sessions with Internet users from the Dutch region of Twente. The FGDs took an in-depth look into the experiences of Dutch Internet users with e-government and the issues users were confronted with when interacting with government organizations online. The important theoretical points discussed in the previous chapters were partly used to guide the flow of the sessions.

4.1 Introduction

The reality of being able to interact with government organizations online should already make long queues inside government offices a sight of years gone by. Driving to government offices to be subjected to achingly long bureaucratic processes should have been reduced to obsolescence with the emergence of a round-the-clock online government service delivery. Things are getting bought online, so why not renew a driver's license at the comfort of one's location anytime of the day?

As cited in the General Introduction, electronic government roots itself on the ideals of significantly improving services provided to citizens and other agencies and of attaining efficiency in government service delivery (Kumar et al., 2007). Nonetheless, the benefits that can be derived from engaging in online transactions with government organizations, such as the convenience of availing government services unconstrained by time and space (Fairweather & Rogerson, 2006; Kumar et al., 2007) are countered by diverging concerns (or risk perceptions), such as the further usage and the unauthorized processing of personal information disclosed for a particular transaction (Colesca, 2009).

Users' lack of trust in online transactions threatens the acceptance of e-government services (Belanger & Carter, 2008; Dashti, Benbasat, & Burton-Jones, 2009). The advantages of engaging in online transactions with government organizations, in some cases, might not totally outweigh trust issues (Carter & Belanger, 2008; Cullen, 2008) and privacy and security concerns (Al-Awadhi & Morris, 2009), which should be adequately addressed before the delivery of government services online could be widely accepted.

This study primarily aimed at understanding the experiences and concerns of Dutch Internet users in using e-government services. Issues related to online information privacy and trust were also explored. The Netherlands is regarded as a mature information society with high Internet use and broadband characteristics, which are necessary conditions for the deployment of e-government (Capgemini, 2009). Three focus group sessions were conducted with 23 residents of three cities in the eastern part of the Netherlands. The four main questions below provided the backbone for this research:

(a) What are the participants' experiences and concerns with online government transactions?
(b) How would they compare the security and online privacy protection mechanisms of the banks and the government organizations they have transacted with?
(c) How do they manage their information privacy in the virtual environment?

(d) What website features do they consider when assessing the trustworthiness of the organization behind the website used for an online transaction?

The first two questions focused on issues related to the usage of e-government in the Netherlands, while the last two questions dwelt on information privacy and trust issues in online transactions as a preliminary attempt to empirically explore the important postulations advanced in Chapters 2 and 3.

4.2 Methodology

Twenty-three residents of three cities (Enschede, Hengelo, and Almelo) in the Netherlands were invited to participate in one of the three focus group discussion (FGD) sessions. Participants were selected based on their previous experience with online transactions such as electronic banking or availing government services online. The selection of the participants was also founded on the ideal of having a balance in the number of participants in terms of age (young vs. old) and education (high vs. low).

Before the start of every session, participants were asked to complete a questionnaire to determine their levels of trust in different online transactions with different types of organizations (banking, filing of income tax returns, shopping) on a scale of 1 to 10, with 1 indicating very low trust and 10 high trust. Participants were further instructed to indicate two reasons for their ratings.

A standard discussion guide was used for the three sessions. All three sessions were conducted in Dutch and were audio-recorded. Participants were assured that their responses will not be tied to their individual identities to protect their anonymity. The following topics were covered in the discussion guide used, along with the sub-questions for each topic:

1. Experience with online government transactions
    a. What benefits did they derive from such form of transaction?
    b. What were their concerns regarding online transactions with government organizations?
2. Comparison of the perceived security of online transactions with government organizations and banks
    a. How would participants compare the security of their online transactions with banks and government organizations?
    b. How would participants assess the protection of their personal data disclosed for online transactions with banks and government organizations?

3. Behaviors related to the disclosure of personal data for online transactions
    a. How would participants respond to requests for personal data regarded irrelevant for a particular online transaction?
4. Website cues that influence trust in online organization transactions
    a. What website features or elements do participants consider when estimating the trustworthiness of organizations behind the websites used for online transactions?

4.3 Results

4.3.1 Experience with and trust in different online transactions: results of the small-scale survey

Results of the small-scale survey reveal that most of the participants have high levels of experience with online banking and online shopping and relatively sufficient experience with online filing of tax returns, but not so much with online government transactions (e.g. applying for a particular document through a municipality's website). Presented in Table 4.1 is a summary of participants' levels of experience with various online transactions.

Table 4.1. Participants' level of experience with various forms of online transactions.

Online Transactions	**Mean** *(1 – no experience / 5 – much experience)*
Online banking	4.43
Online shopping	3.48
Online filing of tax returns	3.09
Online municipal services (e.g. passport application)	2.87

In terms of their levels of trust in various online transactions, almost all participants reported high trust in online banking, except for one who admitted not using it due to lack of trust in such method of banking. Their levels of trust in online municipal transactions, online filing of tax returns, and online shopping were also relatively high. Table 4.2 shows participants' ratings of the trustworthiness of different online transactions, on a scale of 1 to 10 and the percentage of participants who claimed to be using a particular online service.

Table 4.2. Participants' ratings of the trustworthiness of various online transactions.

Online transactions	**Mean** *(1: not very trustworthy / 10: very trustworthy)*	**% of users among FGD participants (N=23)**
Online transaction with banks	8.95	96
Online transaction with municipalities	7.84	83
Online transaction with the tax service office	7.67	78
Online transaction with Internet shops	7.14	91

Participants who gave high trust ratings for their transactions with government organizations cited that they believed government organizations will deal with their transactions correctly.

I trust that the municipality will deal with our online transactions well.

Those who claimed to trust their transactions with municipalities and the tax service office also attributed their trust to a positive experience with and knowledge of such transactions. This confirms the assertion that people are often willing to trust those who did not fail them before (Sztompka, 1999) and further validates previous findings that users' satisfaction with their previous transactions with organizations contributed to their trust in those organizations (Casalo, Flavian, & Guinaliu, 2007; Flavian, Guinaliu, & Gurrea, 2006; Yoon, 2002).

I have experience with and knowledge of online transactions with government organizations.

So far, my transactions with government organizations have always gone well.

I don't have bad and negative experiences with transacting with government organizations online.

However, there were also participants who expressed lack of trust in online transactions with government organizations, especially those that required the disclosure of personal data. Low trustworthiness ratings were justified by apprehensions regarding the usage of personal data outside of the original reasons for their collection and the ease of connecting those data with other digital data accessible elsewhere for profiling.

I have the feeling that the municipality does more with people's personal data than what they are meant for.

I am concerned about the fact that my personal data can easily be linked with other data online.

Except for one who has never done online banking, all participants indicated high trust scores for their online transactions with banks. A positive experience with online banking is often cited as the main reason for their high levels of trust in the aforementioned transaction.

I do my banking exclusively through the Internet. So far nothing has ever gone wrong.

I never had any problem with Internet banking.

They also emphasized the importance of an effective security technology as crucial in enhancing their trust in online banking. A feeling of security in using online banking also contributed to their trust in such form of transaction.

I am confident that banks take online transaction security very seriously.

My bank uses security technologies.

I feel safe when transacting with my bank online.

Some participants also believed that banks will do whatever is necessary to be trustworthy. This seems reasonable since failures on the part of organizations to fulfill their intentions would inevitably result in the depreciation of their reputation (Herbig, Milewicz, & Golden, 1994), which would most likely obliterate people's trust in organizations and negatively affect their intention to transact with those organizations.

A bank does a lot to ensure that everything works well.

Banks should do everything they can to be trustworthy.

Competition between banks makes a mistake catastrophic.

Online shopping, however, could not really acquire the complete trust of participants. Although, buying online is considered convenient, issues regarding how customers' personal data will be used once shared to complete an online purchase also surfaced. Participants also believed that security mechanisms in online shopping are not adequate.

The result of my transaction [with an online shop] was good, but I wonder what will happen to the information I supplied for the transaction.

The security of online shops is weak.

4.3.2 Experiences and concerns with online government transactions

Participants who admitted to have transacted with government organizations online emphasized the benefits that can be derived from such form of transaction. Convenience topped the list of the perceived advantages of availing government services electronically. Participants also indicated the possibility for them to transact with a government organizations online whenever they want to as a strong motivation for them to engage in such form of transaction.

I can transact with the government organization whenever I want to.

Transacting with a government organization online is easy and convenient. I don't have to cycle to the organization's office.

However, despite the benefits that online government transactions offer, there were some participants who expressed uncertainty whether or not online transactions will be processed and handled adequately.

You are not sure whether or not an online request or application for a particular document will be dealt with.

Participants' opinions of the security and protection of online transactions with government organizations were rather polarized. Some participants were convinced that government organizations are using appropriate and strong security mechanisms to ensure the safety of online transactions.

I assume that transactions with government organizations are well protected.

I got the impression that a lot has been invested for the security of online government transactions. I have no objections whatsoever in transacting with a government organization through the Internet.

I personally have never worried about it [transacting with a government organization online]. I think that everything is well protected.

Nonetheless, there were those who strongly believed that divulging personal data to avail government services online is risky. The apprehension is partly attributed to Internet users' lack of knowledge of the system behind the collection of citizens' personal data. Uncertainty regarding the safety of personal data shared to a government organization online was also cited.

I do not know what kind of system is used for the collection of personal data.

The [electronic] patient record is also not safe. How would you know that [citizens'] personal data are safe with government organizations? There have been complaints about the security of personal information [in government databases]. I would prefer that government organizations don't have my personal data simply because they are private. I don't want a government organization to know everything about me.

Another apprehension regarding online government transactions that require the disclosure of personal data is the possibility for external parties to acquire unauthorized access to citizens' personal data. Al-Awadhi and Morris (2009) advanced that beliefs in the inadequacy of

security for e-government services would spur Internet users to suppose that their personal data once disclosed online would be vulnerable to alteration and abuse by hackers.

> *Personal data shared digitally can be accessed and hacked. Once this happens, they [unauthorized third parties] will have all the personal data of citizens.*

Although most FGD participants admitted to have transacted with government organizations online, considering its benefits, there were those who preferred offline transactions over those done online. The need to be assured that initiated transactions will be dealt with properly primarily influenced participants' preference for transacting through the government organization's physical outlet over its electronic channel.

> *When you transact with a government organization online, you do not know exactly whether or not you have submitted the necessary documents. If you go to the municipal office, you will know that things will be arranged right away.*

The lack of physical presence also inhibited some participants from engaging in electronic transactions with government organizations. According to one participant, she would feel more seriously treated if she goes to the office of a government organization than if she transacts with it online. The need for physical encounter in government transactions has been identified as crucial in influencing people's preference for offline government transactions (Cullen, 2008).

> *If you see a person face-to-face and you make a complaint, then there is a sort of pressure on the person – that he or she has to take action. Complaining through an e-mail is not very personal. The complaint will be read, but often it is not addressed immediately by government agents. When you visit the office of the government agency, you get to meet the government agent and communicate with him or her personally.*

4.3.3 A comparison of the security of online transactions with government organizations and banks

Online banking is evidently popular among the FGD participants as it attracted more users than electronic government services *(refer to Table 4.1)*. A number of participants indicated that the security measures of their banks are better than those employed by government organizations. One participant noted that banks should be very careful not to deploy mediocre security mechanisms and mess with clients' trust because such actions could drastically damage banks' position in the market and their relationships with clients. The statement below strongly echoes the belief

that government organizations are somehow unconcerned about maintaining a positive image and gaining citizens' trust.

> *I trust banks more than government organizations because if banks commit a big mistake they can lose many clients. Government organizations can just allow a mistake to happen. They will get bad publicity, but what can you do about it? The bad publicity will have no negative consequences. So in that sense, I have more trust in the bank because they have a bigger stake in ensuring that transactions with them go well.*

Participants reported that their banks employ various authentication mechanisms, including the use of random codes they acquired from a list or those sent to them as a short message service (SMS) or codes generated by portable devices provided by their banks. The use of these codes alongside the usual user name and password to log in apparently gives participants a feeling of security regarding their online banking transactions.

> *I think that online banking is safer because of the use of codes. There is no logic to a code and it could not be predicted. It really is a momentary code. User names and passwords are easier to crack.*

However, a number of participants were also doubtful about the safety of their personal data. They believed that banks habitually share their clients' personal data to third parties for marketing or commercial purposes.

> *I have the idea that personal data [with banks] are not safe. I once got an offer for a credit card from a bank. I don't know if the bank shared my data to third parties. But you know what, they also do it with zip codes. Then you will get specific offers on the basis of your zip code, while another zip code does not get the same offer. It seems that banks do something like that.*

> *One time I was in the 'red figures'. A week after I got a flyer for a personal credit. Every year I still get an offer for a personal credit.*

4.3.4 Behaviors related to the disclosure of personal information online

As discussed in Chapter 2, Internet users' behaviors related to the disclosure of personal data for online transactions or exchanges can be constructed in a three-point scale, with the first end-point representing full disclosure and the other end-point for information withholding. In the middle of these two points would be incomplete data disclosure and information falsification.

Both information withholding and information falsification are regarded as behavior-based strategies Internet users employ to protect their online information privacy (Kobsa, 2007; Metzger, 2007). In a way, users' refusal to share personal data online can be viewed as an attempt to exercise control over their data (Milne, Rohm, & Bahl, 2004). A number of participants claimed to have refused to share personal data online when they felt that the requested data were irrelevant for the transaction.

> *No, I won't go further [transact online]. I am not going to lie because they are asking for things I don't want to share.*

> *Whenever I am requested to supply personal information that I think is not necessary for a transaction, I will not continue with the transaction. I don't trust it.*

Fears that contact information would be used for sending unsolicited information also prompted participants to falsify such information. For instance, some participants admitted that they had given out fictitious addresses for transactions which asked for the aforementioned information, especially when the information is considered irrelevant for such transactions. To avoid the annoyance of receiving spam mails, some participants also maintained email accounts that they can use for interacting with some websites, perhaps those that offer unwanted services or those that could not be trusted.

> *I have a serious e-mail account and a Hotmail account where all spam mails go to. I never open that and after a month everything is gone.*

> *I have two e-mail addresses - one for things that I don't care about and another for important and private information.*

4.3.5 Website elements that increase trust in online transactions

Since Internet users are deprived of an interaction with a flesh-and-blood salesman or a government agent in online transactions, the website becomes the first and most important point of contact for users. Empirical studies that investigated the impact of different website elements on users' trust in online transactions and online organizations abound. For instance, it is revealed that the ease of using a website (Bart et al., 2005; Chen, 2006; Flavian, Guinaliu, & Gurrea, 2006; Koufaris & Hampton-Sosa, 2004) and the quality of information on a website (Liao, Palvia, & Lin, 2006) can increase users' trust in transacting with a particular organization through its online channel.

During the focus group sessions, a number of website elements were cited as important indicators of website trustworthiness: the professional look and feel of the website, indications of transaction security

(such as the yellow padlock logo), the presence of online privacy statements, and the availability of third-party certifications on websites.

> *For me, the professional quality of the website is crucial in giving me a feeling of trust. Not how fast the website is, but how it is constructed. You can see whether the website is made by an amateur or a professional.*
>
> *I watch, among other things, for the padlock symbol. I also check if there is a statement of how trustworthy the organization is. One should also look for a privacy statement carefully.*
>
> *A website with a privacy statement gives me a feeling of trust.*
>
> *I consider security indications such as those by a web shop and an online store registered with a Dutch accrediting organization. If I don't see them [on the website], I won't order. I also consider the structure of the website.*

A professionally designed website could either mean that it is aesthetically appealing or that it is navigable or even both. Karvonen (2000) claimed that when interacting with a website, any knowledgeable user will look for and recognize the 'high tech' features of the web service through the visual layout of the pages, which will act as visual cues or signs of the website's refinement (and professional look) and will eventually trigger an aesthetic experience. The author adds that the 'beauty' of a web design can cultivate online trust.

A professionally designed website may also mean that it is easy to navigate or contains easy to use features. Bart et al. (2005) cited that organizations whose websites have features that foster 'an ease of use' experience for users and have the ability to direct their clients to their destinations in a snap can effortlessly acquire their clients' trust. Since privacy and security concerns plagued online transactions, especially those that require users to share their personal data online, it is important that Internet users are constantly assured of the safety and protection of their online transactions and personal data disclosed for those transactions.

4.4 Discussion

In contrast to an online shop which has to survive tough competition, a government organization that channels its services online only has to compete with itself. If, for some reasons, the online service delivery system of a government organization does not appeal to or is not trusted by Internet user, they always have the option to engage in an offline transaction with the organization. However, if almost everybody will just opt to transact with government organizations through their physical outlets, the investments apportioned for building the infrastructure of an e-government service would just head straight to the sewage.

Studies reveal that although the widespread acceptance of e-government services partly relies on the expected benefits of online transactions (Al-Awadhi & Morris, 2009), trust issues and privacy concerns are serious factors that might considerably lower Internet users' inclination to engage in online government transactions (Capgemini et al., 2009; Carter & Belanger, 2008; Cullen, 2008). Participants in this study confirmed that despite the many benefits of e-government services, primarily convenience and time-saving, they are still concerned about the success and safety online government transactions.

While some participants were convinced that government organizations employ adequate security technologies to ensure the safety of their transactions and the protection of their personal data, a few expressed concerns regarding the probability of having their personal data used for purposes outside the original reasons for the collection. Perceived benefits derived from transacting with government organizations online, therefore, are countered by perceptions of the risks involved in the disclosure of personal information for a transaction.

Furthermore, despite the apparent advantages of transacting with government services online, a number of participants still preferred offline transactions with government agencies over Internet-based transactions. The need to be assured that initiated transactions will be successfully completed, considering the apprehensions that those done online may not be successful, and the need for interaction with a flesh-and-blood government agent primarily contributed to participants' reluctance to transact with government organization online.

Participants were also aware of the various trust cues that transactional sites offered, such as the little *lock* icon for secure websites, privacy statements, and website quality. Nevertheless, they also used an array of privacy risk-reducing strategies, such as having more and less secure username-password combinations for different types of websites. Participants would not also hesitate to stop an online transaction that requests for personal data that are not relevant for the transaction.

4.5 Conclusion

Online trust is indisputably important since risks and uncertainties are inherent in most online transactions, including those initiated with government organizations. So long as online transactions remain anonymous, intangible, and faceless, agenda for research on online trust are not expected to run out anytime soon. With most developed and developing countries investing inestimable amount of time and resources to build online government service infrastructures, it is highly imperative that sufficient attention should be given to trust and privacy risk research in e-government services.

The focus group discussions aimed at exploring Dutch Internet users' experiences and concerns with e-government us

age, their information privacy behaviors, and the determinants of their trust in organizations online. While participants' responses were far from exhaustive, they are certainly useful for acquiring a deeper understanding of trust and privacy issues within the context of e-government in the Netherlands. Data collected through this qualitative research also guided the construction of the research instruments used for the studies reported in Chapters 5 and 6.

5

Shall I tell you where I live and who I am? Factors influencing the behavioral intention to disclose personal information for online government transactions

This chapter reports the results of a large-scale online survey that empirically tested the theoretical points discussed in Chapter 2. The survey with 2,202 Dutch Internet users reveals that trust in government organizations, specifically in terms of their processing and usage of citizens' personal data, is a very important factor influencing personal information disclosure intention among users with and without e-government experience.

Low perceptions of risks, high expectations of the benefits of e-government services, and strong beliefs in the adequacy of legal protection mechanisms could also increase users' intentions to share personal data for e-government services. The negative relation between trust and risk perceptions is also established, as citizens' trust in government organizations could reduce perceptions of the risks involved in an online sharing of personal information.

This chapter is based on a manuscript by Beldad, A., Van der Geest, T., De Jong, M., & Steehouder, M., which is currently under review.

5.1 Introduction

Like most electronic commercial exchanges, availing government services online is intertwined with personal information disclosure. Scheduling an appointment for a passport application or filing an income tax return online necessitates the sharing of personal information before a transaction can be processed and completed. Certainly this is nothing new since transacting with a government organization offline implies that one is obliged to complete paper-based forms. Completing electronic forms to commence a transaction with a government organization through its website, however, is an entirely different story.

Online sharing of personal information either to a web shop or government organization is not risk-free. This is not to say that disclosing personal information offline is safe. In fact, the risks involved in the sharing of personal information, whether online or offline, are thriving. But considering the sophistication of technologies that enable third parties to effortlessly gain unauthorized access to people's data stored in organizational electronic databases and aid organizations - as recipients of personal data - to relay such data to other entities within the digital environment, one can only speculate whether or not engaging in electronic transactions precipitating information sharing is a safe option.

Perceptions of the risks involved in online information sharing could strongly deter Internet users from sharing personal information for electronic transactions. The opposite can be expected, however, if risk perceptions are low or negligible, and if the levels of Internet users' trust in organizations that collect personal data are high. Nevertheless, disclosure can still be expected despite high perceptions of risks and low trust if benefits can be derived from online information sharing. Beliefs in the adequacy of legal protection to ensure the non-violation of online exchanges and the quality of Internet users' previous online transactional experience could also increase intentions to disclose information.

Although a number of studies on e-government focused on adoption (Carter & Belanger, 2005; Gefen et al., 2002; Gilbert, Balestrini, & Littleboy, 2004), in this study adoption is viewed in terms of citizens' willingness to disclose personal data for e-government services. This perspective is predicated on the fact that the completion of an electronic form, which presses citizens to supply personal information, precedes the actual online transaction with a government organization. For instance, an online application for a permit can only be processed when the applicant's personal data are supplied to the responsible agency. Those who find online personal information disclosure bothersome may refuse to share what is requested resulting in the failure of the online transaction, which would mean non-adoption of an e-government service.

Most empirical studies on the determinants of online personal information disclosure, however, have been pursued within the context of e-commerce; while those within e-government are remarkably few. This

study primarily aims at determining the impact of different factors hypothesized to influence online information disclosure for e-government services among Dutch Internet users - with and without online government transaction experience. The necessary data to test the research hypotheses and models were collected through an online survey implemented by two research agencies based in the Netherlands.

5.2 Risk perceptions as deterrents to information disclosure intention

Risks are inherent in online exchanges and transactions considering their distant and impersonal nature (Pavlou, 2003). For instance, though e-commerce and e-government differ in terms of their structures, target audience, and objectives (Belanger & Carter, 2008; Jorgensen & Cable, 2002), both are afflicted with risks, even if Internet users may perceive more risks in electronic commercial exchanges than in online government transactions (Belanger & Carter, 2008). Whereas the risks inherent in online commercial exchanges rest on the probability of losing one's money and one's online privacy resulting from data abuse and misuse, the second point can be highlighted as a prominent risk in e-government services.

The difficulty in capturing risk as an objective reality (Pavlou, 2003; Warkentin et al., 2002) spurs the emphasis on perceived risks, defined as people's subjective expectation of suffering a loss in pursuit of a desired outcome (Pavlou, 2003 citing Bauer, 1960). When risks are perceived to be low, people may be driven to engage in an action; while high perceptions of risks may discourage them from performing a similar action (Das & Teng, 2004). In fact, in several studies, perceptions of risks had been found to negatively impact attitudes towards electronic transactions (Van der Heijden, Verhagen, & Creemers, 2003) and intentions to engage in online commercial exchanges (Chen & He, 2003; Herrero Crespo et al., 2009; Teo & Liu, 2007); just as they also lower citizens' inclination to avail government services online (Schaupp & Carter, 2010). Perceptions of the risks involved in online disclosures of personal data could also discourage Internet users from divulging such data for electronic transactions (Malhotra, Kim, & Agarwal, 2004; Norberg, Horne, & Horne, 2007; Treiblmaier & Chong, 2007) and negatively impact their attitudes towards information disclosure (Zimmer et al., 2010a).

While there are several dimensions of perceived risks (e.g. financial, performance, psychological) (Featherman & Pavlou, 2003; Lim, 2003), one that is of interest for this study is perceived privacy risk, defined as the potential loss of control over personal data that are used without the knowledge and permission of the person to whom the data pertain (Featherman & Pavlou, 2003). When perceptions of privacy risks are high, one can expect that Internet users' disposition to disclose personal information would be low. The first hypothesis is grounded on this premise.

Hypothesis 1. Perceptions of the risks involved in disclosing personal data online negatively influence Internet users' intention to disclose personal data for e-government services.

5.3 Trust as a catalyst for disclosure intention and risk perception reduction

Personal information disclosure precedes the initiation of an online transaction and refusal to disclose information would expectedly result in the failure of the transaction. The risks that are 'out there', while curbing people's willingness to do things online, expedite the cultivation of trust. Risk necessitates trust since the relevance of the latter is founded on the existence of the former (Koller, 1988; Lewis & Weigert, 1985). This has been one of the mainstream views on the relation between the two concepts. Nonetheless, trust is also regarded as an antecedent of risk-taking in any relationship or interaction (Mayer, Davis, & Schoorman, 1995), a perspective emphasizing the important role of trust as an impetus for the performance of a particular behavior despite the risks.

With the primary risk of having personal data abused either by a government organization or by external parties, one can only speculate that citizens' trust in a particular organization would be hinged on their assessment of the organization's ability to protect citizens' personal data and the organization's willingness to treat such data with utmost respect. While the first criterion addresses concerns that personal data shared for transactions with a government organization can be illegally accessed by external parties, the second criterion is directed at public apprehensions that whatever data collected by an organization can be used for commercial purposes. In this case, trust is crucial because of the risk of having one's online privacy intruded due to information abuse.

Whereas the perceived risks in online exchanges could reduce people's inclination to initiate online exchanges, their levels of trust in online organizations have been found to significantly increase their willingness to transact with those entities. Trust is crucial in increasing Internet users' intention to engage in online commercial transactions (Buttner & Goritz, 2008; Everard & Galleta, 2005; Gefen, 2000; Keh & Xie, 2009; Kim, Ferrin, & Rao, 2008) and avail online commercial services (McKnight, Choudhoury, & Kacmar, 2002). Several studies on e-government have also indicated that trust is an essential ingredient for the acceptance and adoption of online government services (Belanger & Carter, 2008; Carter & Belanger, 2005; Colesca & Dobrica, 2008).

Trust in organizations within the online environment is also an important driver for Internet users' willingness to disclose personal information for computer-mediated transactions (Malhotra et al., 2004; McKnight et al., 2002; Schoenbachler & Gordon, 2002; Dinev & Hart, 2006; Zimmer et al., 2010b). While the view of risks and risk perceptions fuelling

trust retains its validity, it is also strongly probable that trust in organizations can trigger a decline in risk perceptions, as shown in a number of studies (Gefen et al., 2002; Van der Heijden et al., 2003; Jarvenpaa & Tractinsky, 1999; Kim et al., 2003, 2008; Malhotra et al., 2004). Two research hypotheses spring from these arguments.

> *Hypothesis 2. Trust in government organizations in terms of their processing and usage of citizens' personal information positively influences Internet users' intention to disclose personal data for e-government services.*

> *Hypothesis 3. Trust in government organizations in terms of their processing and usage of citizens' personal information negatively influences Internet users' perceptions of the risks involved in disclosing personal data for e-government services.*

5.4 Information disclosure due to expected benefits

Even with high perceptions of privacy risks and without trust, citizens would still opt to share personal information to avail a particular government service online. Viewed from a calculus-based perspective (Laufer & Wolfe, 1977), people's decisions to share personal data online, despite the risks of having their online privacy compromised, are driven by expectations of tangible or intangible benefits (Berendt, Gunther, & Spiekermann, 2005; Norberg & Dholakia, 2004) and by a belief that the benefits of information disclosure outweigh the estimated costs of the disclosure act (Culnan & Bies, 2003; Olivero & Lunt, 2004).

Tangible benefits for the disclosure of personal information online could be vouchers, cash, or gift items. Rewards in the form of monetary vouchers, for instance, have a positive impact on Internet users' willingness to provide accurate personal information (Xie, Teo, & Wan, 2006). Intangible benefits include the convenience of doing things online such as electronic shopping, gaining access to a range of Internet services such an emailing and joining online social networks, and experiencing the comforts of personalization and personalized services – all requiring the disclosure of personal information.

Expected benefits that can be derived from e-government are purely intangible such as the convenience of transacting online anytime, anywhere and the possibility to save time and energy by availing government services through the Internet. One can, therefore, assume that Internet users' appraisal of the advantages of availing government services online could increase Internet users' willingness to share personal information for the completion of electronic government transactions. This leads to the fourth hypothesis.

Hypothesis 4. Expected benefits of e-government services requiring personal information positively influence Internet users' intention to disclose personal data for e-government services.

5.5 When legal protection is adequate…

While most countries do not have comprehensive personal data protection laws, countries within the European Union have their own laws to ensure the protection of their citizens' personal information. The European Union institutionalized the protection of personal data through Directive 95/46 EC. In the Netherlands, EU Directive 95/46 is implemented through the *Wet Bescherming Persoonsgegevens* (Dutch Data Protection Act).

Bellman et al. (2004) asserted that the existence of a law on the protection of personal data considerably impacts people's levels of concern regarding information privacy. A survey with respondents from 38 countries revealed that users from countries without privacy regulations expressed greater concerns regarding data errors and online transaction security than users from countries that have implemented similar regulations (Bellman et al., 2004).

Such finding nurtures the assumption that if users are aware of the existence of laws that protect their personal information and if they believe that legal protection is adequate to protect their interests online they would be highly inclined to perceive low levels of risks involved in information disclosure, which would increase their willingness to share personal information for an online transaction. Hypotheses 5 and 6 emanate from the arguments just cited.

Hypothesis 5. Beliefs in the adequacy of a legal protection for online transactions requiring personal data positively influence Internet users' intention to disclose such data for e-government services.

Hypothesis 6. Beliefs in the adequacy of a legal protection for online transactions requiring personal data negatively influence Internet users' perceptions of the risks involved in disclosing such data for e-government services.

Structural assurances, in the form of regulations and legal protection mechanisms, are believed to influence the germination of a trusting belief, also termed institutional-based trust (McKnight, Cummings, & Chervany, 1998). Institutional-based trust refers to an expectation that third-party institutional mechanisms are in place to ensure the success of computer-mediated transactions (Pavlou & Gefen, 2004). While it is known that legal frameworks significantly increase trust in online commercial exchanges (Cheung & Lee, 2006), it could also be stipulated that a belief in the adequacy of legal protection would stimulate trust in government organizations. This leads to the next hypothesis.

Hypothesis 7. Beliefs in the adequacy of legal protection for online transactions requiring personal data positively influence trust in government organizations in terms of their processing and usage of citizens' personal data.

The seven hypotheses will be tested first with Internet users who have not transacted with government organizations online, although the hypotheses just introduced will also be included in the sub-study involving respondents with e-government experience. Figure 1 shows the schematic representation of the interaction among the seven hypotheses, which also serves as the structural model for personal information disclosure among respondents without e-government experience.

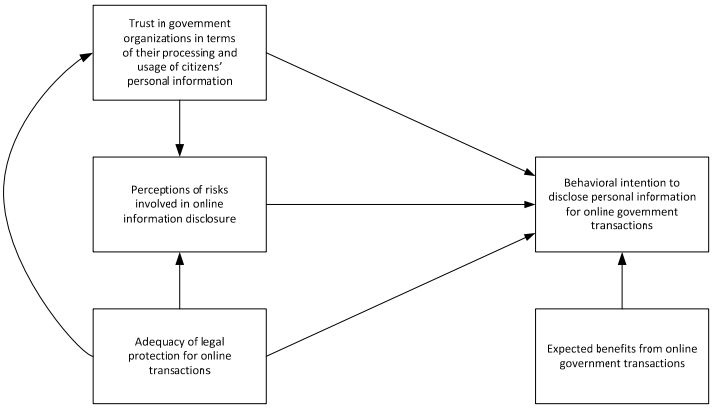

Figure 5.1. Structural model of online information disclosure for e-government services among respondents without e-government experience.

5.6 The role of previous online transaction experience

Information disclosure intentions rooted on calculations of benefits and assessments of risks, coupled with estimations of the trustworthiness of the information recipient, can be seen as too rational. However, disclosure intentions are sometimes founded on non-rational grounds such as previous online transaction experience. The levels and the depth of Internet users' relationship with online organizations are regarded as important triggers for non-rationally grounded disclosure decisions (Olivero & Lunt, 2004).

One can claim that even with less trust and despite perceptions of high risks, information disclosure can be expected from those with prior online transaction experience with a particular organization. It is argued that Internet users with adequate experience in online transactions would be less concerned about online information privacy (Bellman et al., 2004; Cho, Rivera-Sanchez, & Lim, 2009), in general, and less concerned about

privacy risks such as improper access to and unauthorized secondary usage of personal data (Bellman et al., 2004), in particular.

However, the view that online transaction experience inflates disclosure intentions is too vague to be valid. People may have adequate online transaction experience, but if the experience has been unpleasant most of the time, behavioral intentions might be constricted. Having an online transaction experience alone does not suffice. The experience should be satisfying or enjoyable. Internet users' satisfaction with their online transactions is positively related to their trust in organizations for a possible second transaction (Pavlou, 2003). Trust, as previously mentioned, increases Internet users' inclination to engage in exchanges despite the risks. This assertion emphasizes that the impact of a positive experience on behavioral intention, for instance to disclose information, is mediated by trust in the online organization.

Nonetheless, even with less trust in an organization, one's positive experience with that organization may also prompt a behavioral intention to engage in an exchange with the same organization. Studies on online information disclosure behaviors have glaringly disregarded the impact of Internet users' previous online transaction experience on their intentions to share personal information for online transactions. These studies seemed to assume that the determinants of online information disclosure would not vary among Internet users, whether or not they have any online transaction experience.

The inclusion of 'quality of previous online experience' as a possible factor influencing the behavioral intention to disclose information online is based on the premise that those who are happy and satisfied with the outcomes of their online transactions would not hesitate to disclose personal information whenever asked for the initiation and completion of online exchanges. The arguments just articulated resulted in the following hypotheses:

> *Hypothesis 8. A positive online government transaction experience positively influences the behavioral intention to disclose personal information for e-government services.*
>
> *Hypothesis 9. A positive online government transaction experience positively influences trust in government organizations in terms of their processing and usage of citizens' personal information.*
>
> *Hypothesis 10. A positive online government transaction experience negatively influences perceptions of the risks involved in online personal information disclosure for e-government services.*

Figure 2 shows the schematic representation of the 10 hypotheses that will be tested using data from respondents with e-government experience. This is also the structural model for personal information disclosure intention among experienced respondents.

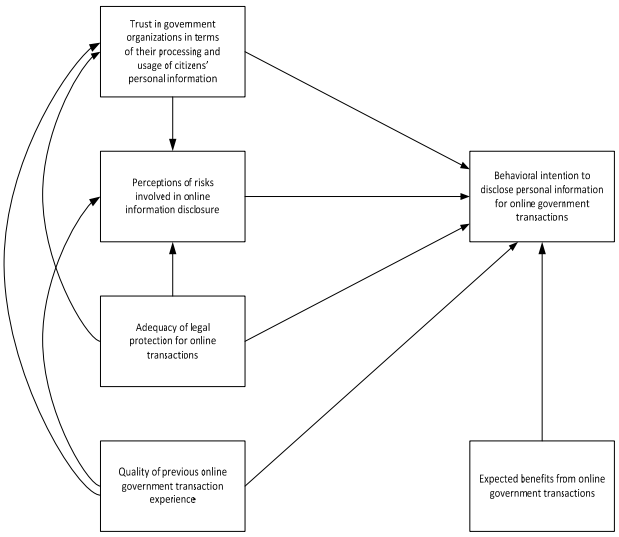

Figure 5.2. Structural model of online information disclosure for e-government services among respondents with e-government experience.

With data from respondents who have transacted with government organizations and those who have not, the study will also look into the differences in respondents' levels of trust in government organizations, risk perceptions, estimations of e-government benefits, and online information disclosure intention. Four additional hypotheses will be tested.

Hypothesis 11. Trust in government organizations in terms of their processing and usage of citizens' personal data differs significantly among respondents with and without e-government experience.

Hypothesis 12. Perceptions of the risks involved in online personal information disclosure for e-government services differ significantly among respondents with and without e-government experience.

Hypothesis 13. Estimations of the expected benefits that can be derived from e-government services differ significantly among respondents with and without e-government experience.

Hypothesis 14. Behavioral intentions to disclose personal information for e-government services differ significantly among respondents with and without e-government experience.

5.7 Methodology

5.7.1 Survey respondents

Data necessary to test the research hypotheses and the research models were collected through an online survey implemented by two research agencies in the Netherlands. Both research agencies sent a link to the online questionnaire to approximately 3,500 members of their research panels, which are representative samples against the Dutch national census. A total of 2,202 completed online questionnaires were collected after the duration of the large-scale online survey, resulting in a response rate of 63 percent. A balance in the male/female ratio in the sample was achieved, while more than half of the respondents (N=1,354, 61.4%) were over 45 years old. Those with Internet experience of 11 years or more accounted for 52.2% (N =1,150) of the entire sample. Table 1 shows the complete demographic information for the survey respondents.

Table 5.1. Complete demographic information of survey respondents.

Demographic characteristics		Freq.	%
Gender	male	1100	50.0
	female	1102	50.0
Age	18 to 24 years old	103	4.7
	25 to 34 years old	281	12.8
	35 to 44 years old	464	21.1
	45 to 54 years old	534	24.2
	55 to 65 years old	516	23.4
	66 years and older	304	13.8
Internet experience	1 to 5 years	161	7.3
	6 to 10 years	891	40.5
	11 to 15 years	903	41.0
	16 years or more	247	11.2
Experience with e-government services	I have used a government website to do an online transaction.	1646	74.7
	I have used the government website to look for information search only.	409	18.6
	I have not used a government website to do an online transaction.	147	6.7
	TOTAL	**2,202**	**100**

5.7.2 Survey instrument

Respondents' demographic information were collected in the first part of the questionnaire. The second part of the instrument was apportioned for items measuring the different variables of the research. Except for the items for the variable 'trust in government organizations in terms of their processing and usage of citizens' personal data', which were measured on ten-point Likert scales (10 for very high trust; 1 for very low

trust), all the items for the other variables (risk perceptions, adequacy of legal protection, expected benefits of e-government services, and intention to share personal information) were measured on five-point Likert scales (from strongly agree to strongly disagree).

Almost all items included to measure the study's constructs were based on the responses given during three focus group sessions conducted four months prior to the implementation of the online survey. Items for 'behavioral intention to disclose personal data', however, were newly formulated for the study. The items that were included for the different research constructs, originally formulated in Dutch, are shown on Table 3.

A question on whether or not respondents have used the websites of government organizations to avail government services facilitated the segregation of those with e-government experience from those without. Those with e-government experience were directed to the online questionnaire that included items pertaining to the quality of their online government transaction experience. Approximately two-thirds (N=1,646) of survey respondents have used government websites to avail government services, while those who have used government websites for information search only (which does not require information disclosure) and those who have never used government websites for transactions comprised about 25 percent of the sample (N=556).

5.8 Data analysis

Structural Equation Modeling (SEM), a comprehensive statistical approach to test hypotheses about relations among observed and latent variables (Hoyle, 1995), using AMOS 18.0, was used to perform confirmatory factor analysis on the constructs of the study, to address the research hypotheses (Hypotheses 1 to 9), and to test whether or not the research model fits the data. T-tests were used to test hypotheses 11 to 14.

With SEM, the factors influencing online information disclosure for online government transactions are identified and the effects of trust in government organizations and beliefs in the adequacy of legal protection on Internet users' perceptions of the risks involved in personal information disclosure for e-government services are determined. SEM also enabled the determination of the effects of the quality of users' online government transaction experience on risk perceptions and trust in government organizations.

The two-step approach advanced by Anderson and Gerbing (1988) was employed. In accordance with this approach, the measurement model was first assessed with confirmatory factor analysis prior to testing the hypotheses with structural equation modeling, which aimed at determining model fit or how well the model as a whole explains the sample data (Byrne, 2010; Kline, 2005). Several indices have been proposed to determine model fit, although there is little consensus regarding the best index of

overall fit in the evaluation of structural equation models (Hoyle & Panter, 1995).

It is recommended that chi square (X^2) values should always be reported, alongside degrees of freedom and probability levels (Hoyle & Panter, 1995; Markland, 2007). However, X^2 is sensitive to sample size (Byrne, 2010; Kline 2005), as models tested on a larger size are more likely to fail or be rejected through the X^2 goodness-of-fit test (Barrett, 2007; Blunch, 2008). Reduction of the sensitivity of X^2 to sample size is normally performed by dividing the value of X^2 by degrees of freedom (X^2 / d*f*) resulting in a value referred to as normed chi-square (NC) (Kline, 2005). NC values of 5 of less could be interpreted as acceptable (Wheaton et al., 1977).

Other fit indices used to assess model fit include Normed Fit Index (NFI), Non-Normed Fit Index (NNFI) or the Tucker-Lewis Index (TLI), Incremental Fit Index (IFI), Comparative Fit Index (CFI), and root mean square error of approximation (RMSEA) (Schreiber et al., 2006). Preference, nevertheless, is given to TLI, CFI, and RMSEA for one-time analyses, that is when there are no modifications made to the model (Schreiber et al., 2006). Values close to .95 for TLI and CFI and a cut-off value of 0.06 for RMSEA are required before a conclusion that there is a relatively good fit between the hypothesized model and observed data can be made (Hu & Bentler, 1999).

5.9 Results

5.9.1 Instrument reliability

Prior to testing the research hypotheses, construct reliability was determined by calculating the constructs' Cronbach's alpha scores. Alpha values above .70 indicate acceptable reliability (Hinton, 2008). Table 2 shows that the reliability levels of the constructs for this study meet the proposed criterion.

Table 5.2. Reliability scores and mean and standard deviation values of the research constructs.

Variables	No. of Items	With e-government experience (N = 1,646)			Without e-government experience (N = 556)		
		a	*Mean*	*SD*	*a*	*Mean*	*SD*
Trust in government organizations in terms of their processing and usage of citizens' personal data	3	.918	7.00	1.53	.926	6.26	1.74
Perceptions of the risks involved in disclosing personal information online	3	.830	2.81	1.05	.867	2.78	1.15
Expected benefits of online government transactions	4	.864	4.02	0.72	.902	3.05	1.28
Beliefs in the adequacy of legal protection for online transactions	2	.790	3.51	1.03	.791	3.12	1.11
Quality of previous e-government experience	2	.810	3.81	0.76	-	-	-
Behavioral intention to disclose personal information	3	.872	3.39	0.74	.904	3.05	0.83

5.9.2 Differences in trust, risk perceptions, beliefs in expected benefits, and disclosure intention among respondents with and without e-government experience

Respondents who have availed government services online have higher levels of trust in government organizations (in terms of how they will process and use citizens' personal data) ($t = 8.92$, $df = 859.89$, two-tailed, $p < .001$) and higher estimations of the benefits of e-government ($t = 17.17$, $df = 678.81$, two-tailed, $p < .001$) than those who have never transacted with government organizations online. Behavioral intentions to disclose personal data for e-government are also higher among those with online government transaction experience than those without ($t = 8.49$, $df = 867.80$, two-tailed, $p < .01$).

Perceptions of the risks involved in online sharing of personal information, however, do not differ significantly among respondents with and without e-government experience, which implies that risk perceptions are not dependent on online transaction experience. The findings, therefore, support Hypotheses 11, 13, 14, but not Hypothesis 12.

5.9.3 Tests of the measurement models

Confirmatory factor analysis (CFA) was performed to determine whether or not observed items assigned to subscales actually load into their related factors (latent variables). Covariation among the latent variables was allowed but not among error variances. The measurement model used for respondents with e-government experience is composed of 6 latent variables (trust in government organizations, perceptions of risks, expected benefits, legal protection, quality of previous online transaction experience, and disclosure intention) with 17 observed items. The measurement model for those without e-government experience has 5 latent variables (less quality of previous experience) with 15 observed items.

Evaluations of the fit of the measurement models for respondents with and without e-government experience were based on four indices: X^2, TLI, CFI, and RMSEA. Confirmatory factor analysis shows that the measurement model for respondents with e-government experience generated a highly acceptable fit, $X^2(104) = 381.76$, $X^2/df = 3.67$, TLI = .98, CFI = .98, RMSEA = .04. The measurement model, tested with data from respondents without e-government experience, also yielded an excellent fit, $X^2(80) = 129.18$, $X^2/df = 1.62$, TFI = .99, CFI = .99, RMSEA = .03. Factor loadings of the observed items into their latent variables are shown on Table 3.

Table 5.3. Factor loadings of the observed items into their latent variables.

Latent Variables	Observed Items	Factor Loadings	
		With e-gov experience	*Without e-gov exp.*
Trust in government organizations	The government	.944	.942
	Municipalities	.903	.910
	The tax service office	.822	.850
Perceptions of the risks involved in disclosing personal information online	Government organizations could sell my personal data to third parties.	.724	.819
	Government organizations could abuse my personal data.	.860	.920
	Government organizations could give third parties access to my personal data without my knowledge and consent.	.783	.754
Adequacy of legal protection	Online government transactions that require personal information sharing are adequately protected by the law.	.784	.814
	The Dutch privacy protection law is good enough to protect citizens' personal data shared for online transactions with government organizations.	.834	.805
Expected benefits of e-government services	Online transactions with government organizations save time.	.814	.883
	I find it advantageous that I can transact with government organizations online anytime I want to.	.827	.807
	Online transactions with government organizations are convenient.	.855	.862
	Online transactions with government organizations are fast.	.696	.796
Quality of previous online government transactional experience	My online transactions with government organizations have always gone well.	.920	_
	I have no negative experiences in transacting with government organizations online.	.745	_
Behavioral intention to share personal information for e-government services	I would feel comfortable sharing my personal data to the websites of government organizations.	.831	.867
	I would not hesitate supplying my personal data through the websites of government organizations.	.859	.876
	I would feel secure in disclosing my personal data to the websites of government organizations.	.817	.869

5.9.4 Test of the structural model with data from respondents without e-government experience

The four indices used to assess the fit of the measurement models were also employed to determine the fit of the structural models. The test of the structural model for the behavioral intention to disclose personal information for e-government services among respondents without e-government experience resulted in a good fit, $X^2(83) = 259.60$, $X^2/df = 3.13$, TLI = .96, CFI = .97, RMSEA = .06 (CI: .05, .07). Model modification was deemed unnecessary due to the acceptable fit of the model. The next step, therefore, is to look into the different path coefficients corresponding to the research hypotheses.

Trust in government organizations in terms of their processing and usage of citizens' personal data has a strong positive influence on the

behavioral intention to disclose personal information among respondents without e-government experience (b = .39). This supports Hypothesis 2. Internet users' trust in government organizations also precipitate a decline in their perceptions of the risks involved in online information disclosure (b = -.31).

A negative relation between risk perceptions and disclosure intention exists (b = -.23), which implies that when perceptions of the risks involved in online information disclosure are low intentions to share personal information will increase. This supports Hypothesis 1. Though not as influential as trust, expected benefits that can be derived from e-government services necessitating online information disclosure also have a positive impact on disclosure intention (b = .17), prompting the acceptance of Hypothesis 4.

Beliefs in the adequacy of legal protection of online transactions requiring personal data could also increase Internet users' intention to disclose personal information for online government transactions (b = .17), just as such beliefs could also foster trust in government organizations (b = .38). However, contrary to what was expected, beliefs in the adequacy of legal protection have no effect on the depreciation of risk perceptions, precipitating the rejection of Hypothesis 6. Figure 3 shows the tested structural model with its path coefficients and levels of significance.

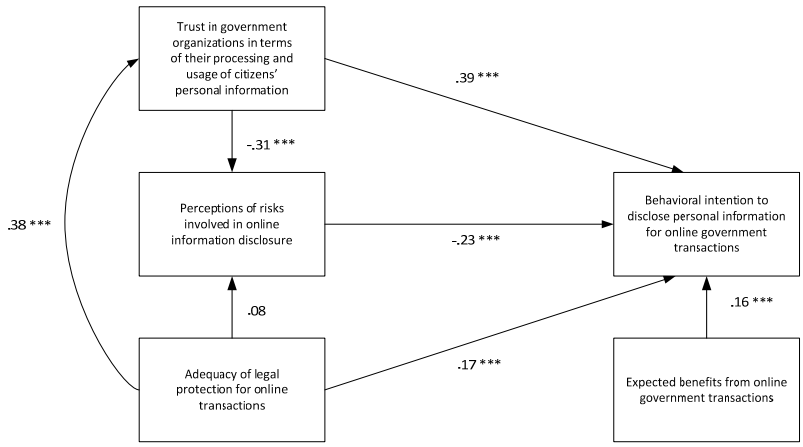

*Figure 5.3. Standard path coefficients of the model for the determinants of online personal information disclosure among respondents without e-government experience (*** $p < .0001$).*

5.9.5 Test of the structural model with data from respondents with e-government experience

Results of the test to determine the fit of the model with data from respondents with e-government experience (Figure 5.4) indicate that this particular has an inadequate fit, X^2 (109) = 924.36, X^2/df = 8.48, TLI = .94, CFI = .95, RMSEA = .07 (CI: .06, .07). A review of the modification indices

revealed that model fit could be considerably improved by allowing a couple of latent variables to correlate with each other.

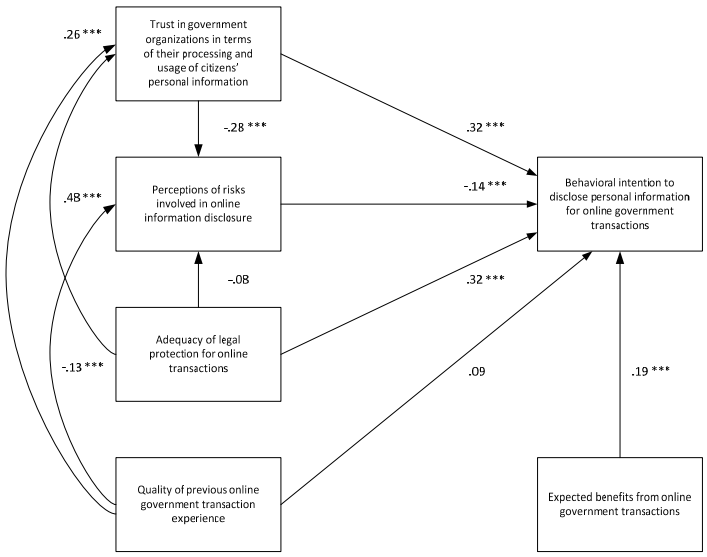

*Figure 5.4. Standard path coefficients of the original model for the determinants of online personal information disclosure among respondents with e-government experience (*** $p < .0001$).*

In modifying the original model, 'quality of previous online government transaction experience' and 'expected benefits from e-government' were allowed to correlate with each other. A path was also introduced from 'quality of previous online government transaction experience' to 'beliefs in the adequacy of legal protection'. The test of the modified model (Figure 5.5) yielded a substantially improved and acceptable fit, X^2 (107) = 488.15, X^2/df = 4.56, TLI = .97, CFI = .98, RMSEA = .05 (CI: .04, .05).

Among respondents with e-government experience, trust in government organizations in terms of their processing and usage of citizens' personal data (b = .31) is still a very important determinant of the behavioral intention to supply personal information for online government transactions. Thus, Hypothesis 2 is accepted. The effect of trust in lowering risk perceptions (b = -.28) is also substantiated, confirming Hypothesis 3.

Alongside trust, beliefs in the adequacy of legal protection for online transactions also have a strong positive effect on disclosure intention (b = .31), which also supports Hypothesis 5. Hypothesis 1 is also accepted since low risk perceptions (b = -.13) can trigger information disclosure intentions. Expectations of the benefits of transacting with government organizations online (b = .18) also positively influence respondents' willingness to share personal information through government websites, resulting in the acceptance of Hypothesis 4. However, an appraisal of the

adequacy of legal protection does not result in a decline of risk perceptions, leading to the rejection of Hypothesis 6.

The quality of users' previous online government transaction experience both lowers their perceptions of the risks involved in personal information disclosure (b = -.12) and increases their trust in government organizations (b = .23). Thus, Hypotheses 9 and 10 are accepted, respectively. The correlation between the quality of respondents' previous e-government experience and their appraisal of the benefits of e-government is also high. This implies that those who are satisfied with their online government transactions are more inclined to have high estimations of the advantages of availing government services online.

A significant value (b = .41) for the path from 'quality of previous e-government experience' to 'adequacy of legal protection' seems to signify that a satisfying online transactional experience augments belief in the adequacy of legal mechanisms to protect online transactions. Indicated in Figure 5.5 are the path coefficients with significance levels for the tested structural model using data from respondents with e-government experience.

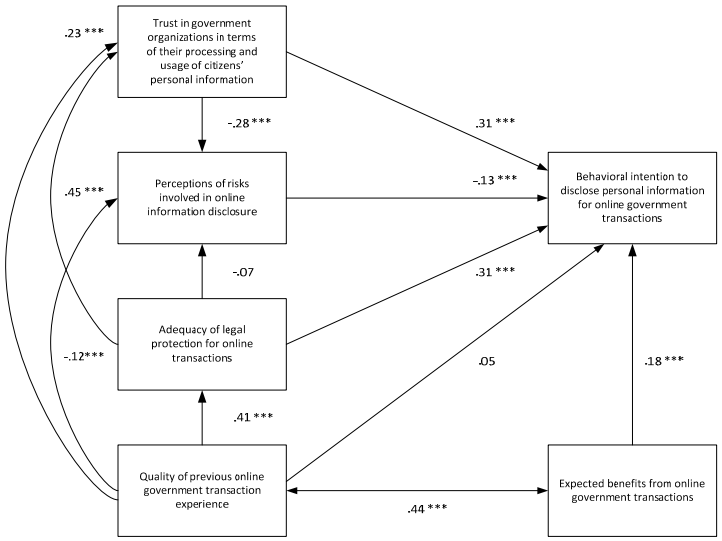

*Figure 5.5. Standard path coefficients of the modified model for the determinants of online personal information disclosure among respondents with e-government experience (*** p < .0001).*

5.10 Discussion

The significance of trust in increasing behavioral intentions, despite the risks, is irrefutable. In fact, trust is viewed as a willingness to take risk (Mayer et al., 1995). While risk and trust are often theorized to be inseparable, the relationship between the two is unclear (Das & Teng, 2004). It can be postulated, however, that high levels of trust and low perceptions

of risk could propel the performance of a behavior, for instance sharing pieces of personal information for online transactions.

Results of this study clearly indicate that regardless of whether or not citizens have any experience with online government transactions, their levels of trust in government organizations are instrumental in influencing their intentions to supply personal information for online government services. The risks involved in the sharing of personal information, such as selling or sharing of people's personal information to third parties, may shove Internet users' to critically assess the trustworthiness of a particular government organization. Such estimation of trustworthiness is an indication of an expectation that the organization has the ability and the willingness to protect citizens' personal information shared for an application of a government document, for instance.

The impact of trust on disclosure intention is considerable among Internet users without e-government experience. This suggests that whenever inexperienced citizens are deciding to share their personal information for an e-government service for the first time they primarily consider their levels of trust in a government organization as important motivators for their intentions to share personal information.

As expected, Internet users' trust in government organizations could spur a decline in their perceptions of the risks involved in online personal information disclosure. This is in consonance with the assertion that trust does not only instigate a reduction in risk perceptions (Kim et al., 2008) but also helps people overcome such perceptions (Salam et al., 2003) and moderates their sensitivity to risk considerations (Grazioli & Jarvenpaa, 2000). Since perceptions of the risks involved in online information sharing could substantially deter citizens from divulging their data, thereby resulting in their strong reluctance to avail a particular government service online, government organizations should persistently strive to combat such perceptions by fortifying their images as trustworthy recipients of citizens' personal data.

Certainly when risk perceptions are low, citizens' intention to disclose their personal data for e-government services would expectedly increase. While it is true that low perceptions of risks and high levels of trust could result in online information disclosure, expected benefits that can be derived from e-government services necessitating information sharing and beliefs in the adequacy of legal protection are also strong information disclosure determinants. The impact of legal protection on disclosure intention is more pronounced among those with e-government experience than those without.

Though expected benefits from e-government positively impact information disclosure, the influence of the aforementioned variable is less compared to that of trust, signifying that trust considerations outweigh estimations of the advantages of online transactions requiring personal data. Therefore, even with the advantages of availing government services online, intentions to engage in such a transaction preceded by information

disclosure would be less if trust in a government organization in terms of its usage and processing of citizens' personal information is low.

It was initially postulated that the quality of Internet users' online government transaction experience would have a significant impact on their willingness to share personal data for e-government services. Data analysis, however, reveals that the aforementioned factor has no impact on information disclosure. Nevertheless, a comparison of disclosure intention among those with previous e-government experience and those without indicates that Internet users who have already availed government services online are more predisposed to share their personal data online than those who have not. This appears to makes sense since those who have e-government experience also reported to have higher levels of trust in government organizations than those devoid of any online government transaction experience.

The quality of Internet users' e-government experience significantly increases trust in government organization and lowers perceptions of the risks involved in online information sharing. Satisfied Internet users, it can be argued, are more inclined to trust government organizations in terms of their processing and usage of citizens' personal information and are less predisposed to believe in the risks involved in sharing personal information for e-government services. Risk-taking, as expressed in the performance of a trusting behavior (e.g. engaging in an online transaction), that results in a positive outcome (satisfying experience) eventually leads to the enhancement of the transaction partner's trustworthiness (Mayer et al., 1995).

A positive relationship also exists between the quality of respondents' previous online government transaction experience and their approximation of the adequacy of legal protection for online transactions requiring information disclosure. This implies that a positive appraisal of the sufficiency of legal mechanisms to ensure the protection of online transactions requiring personal information is rooted on the positive transaction experience of Internet users. Probably Internet users attribute the positive outcomes of their online transactions to the potency of legal mechanisms to guarantee that online transactions are carried out competently and honestly.

Happy and satisfied Internet users are also prone to highly estimate the benefits of e-government services, as indicated by the strong correlation between quality of online transaction experience and expected benefits of availing government services online. While a positive experience does not really impact information disclosure, it is highly plausible that its influence could be mediated by expectations of e-government benefits, which as data analysis reveals, positively influence online personal information sharing.

Beliefs in the adequacy of legal protection could also improve citizens' trust in government organizations in terms of their processing and usage of citizens' personal information. This is valid for those with and without e-government experience. Nonetheless, the proposition that a belief

in the sufficiency of legal protections would result in the reduction of risk perceptions is not statistically confirmed.

The effect of legal protection on the reduction of risk perceptions may not be entirely direct and could probably be channeled through trust in government organizations, considering how it is influenced by a belief in the adequacy of legal mechanisms protecting online transactions requiring information disclosure. As proposed by Salam, Rao, and Pegels (2003), institutional trust, cultivated partly by a confidence in structural guarantees (e.g. laws) as effective mechanisms to ensure transactional success, is instrumental to the reduction of risk perceptions in the online environment.

5.11 Implications and recommendations

Since the current study heavily relies on a Dutch sample, the generalizability of the findings could be constrained. There is no refuting that the effects of the different determinants of online information disclosure would considerably vary across different cultural groups. For instance, while trust is crucial in amplifying behavioral intentions to share information online in the Netherlands, where levels of trust are high (Rothstein & Eek, 2009), the effect of the aforementioned factor could be different in countries where levels of trust are low.

It is, therefore, recommended that a similar study with different samples be conducted. Replicating the study with respondents from other countries will not only determine whether or not differences in the determinants of disclosure intention exist but will also provide valuable insights into the extent to which culture impacts trust, risk perceptions, estimation of e-government benefits, and disclosure intentions.

The perceived risks involved in disclosing personal information online, as identified in the survey instrument, only focused on potential risks that can be attributed to the possible exploitative actions of government organizations. However, the risks related to online information sharing are also attributable to malicious third parties with the right technology to gain unwarranted access to people's personal data for reasons unknown. Risk perceptions are hypothesized to negatively impact information disclosure intentions. Since this research somehow missed looking into risk perceptions in a bimodal fashion, further research on the impact of risk perceptions on information disclosure could also tinker on the impact of perceptions of risks, attributed both to organizations collecting personal data and to external parties, on people's willingness and inclination to share personal data for e-government services.

Although 'quality of online transactional experience' has been included as a non-rational information disclosure determinant, other possible factors within the frame of non-rational information disclosure, such as habits and Internet proficiency, need to be explored for future research. The 'trust' construct could also be refined by re-conceptualizing it in terms of the perceived ability and good intention of government

organizations to protect citizens' personal data. Therefore, the trustworthiness criteria should be emphasized as components of trust in a government organization.

In the present study, trust in government organizations is only measured in terms of the estimated trustworthiness of different types of government organizations, especially in terms of their processing and usage of citizens' personal information. Since the impact of trust on online information disclosure is evidently indubitable, future research can also explore the factors that could influence the enhancement of trust in a particular government organization.

While the current study extends the possibilities for research on information disclosure within the context of e-government, the results of this investigation have significant implications for those involved in the construction, implementation, and management of e-government services. Trust, as already noted, is undeniably crucial in augmenting citizens' willingness to engage in online government transactions via their positive disposition to share personal information online, just as trust proves compelling in reducing risk perceptions. It is, therefore, imperative for any government organization that channels its services online to win the trust of its target clients by fortifying its image as a trustworthy entity.

Although a positive online transaction experience does not directly translate into citizens' willingness to disclose personal information, its effects are noteworthy since it does not only enhance citizens' trust in government organizations and decreases risk perceptions but also amplifies an appraisal of the benefits of e-government services. Since high levels of trust, low risk perceptions, and high estimations of e-government benefits could result in a heightened intention to disclose information online, it could, therefore, be surmised that a positive online transaction experience indirectly impacts intentions to engage in online government transactions, preceded by a willingness to divulge personal data. Government organizations, therefore, ought to ensure that citizens who opt to avail government services online are highly satisfied with their transactions.

5.12 Conclusion

The coupling of online transactions with information disclosure is somehow inevitable since the success of the former depends on the latter. Requesting documents and scheduling appointments are proximate to impossible if personal data relevant for a particular transaction are not supplied or disclosed correctly. Because personal data have also become valued commodities, sharing them online is increasingly regarded risky. The perceived risks involved in an online sharing of personal information have been empirically proven to abate Internet users' inclination to engage in electronic exchanges and transactions compelling information disclosure.

What is certain, as this study shows, is that low perceptions of risks and high levels of trust in government organizations have strong

repercussions for Internet users' intention to disclose personal data online. Trust in government organizations, in particular, has been found to play a very crucial role in augmenting disclosure intentions of users with and without e-government experience. Nonetheless, information disclosure intention would expectedly increase if legal protection mechanisms are believed to be adequate in protecting online transactions requiring personal data and if those transactions are assessed to be beneficial and advantageous.

The significance of a previous experience also matters. While a positive transactional experience does not directly translate into increased disclosure intention, those who have transacted online are more predisposed to share their personal data for e-government services than those without. The second point apparently makes sense since experienced users are also more trusting of government organizations and are more positive about the benefits of e-government that those who are not.

6

A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online

The large-scale online survey described in the previous chapter accentuated that aside from the expected benefits of e-government services that require personal data, Internet users' trust in government organizations in terms of their usage and processing of citizens' personal data is an important factor influencing the behavioral intention to disclose personal data for e-government services. Different cues and factors that could enhance online trust were identified in Chapter 3. Results of the FGDs described in Chapter 4 indicated that participants considered different cues when assessing the trustworthiness of organizations behind the websites used for transactions.

This chapter discusses the results of another large-scale Internet survey (with 1,156 respondents) that investigated the cues and factors that could positively influence Dutch Internet users' trust in government organizations in terms of their usage and processing of citizens' personal data. Confidence in online privacy statements, as indicated by the results of this study, significantly increases trust in government organizations among Dutch Internet users with and without previous e-government experience. Among those with e-government experience, the quality of their online government transaction experience and a positive government organizational reputation can also enhance their trust in government organizations, specifically in terms of how they process and use citizens' personal data.

This chapter is based on a manuscript by Beldad, A., Van der Geest, T., De Jong, M., & Steehouder, M., which is currently under review.

6.1 Introduction

The survey described in the previous chapter revealed that trust is an important factor influencing Dutch Internet users' intention to disclose personal data for e-government services. The significance of trust is rooted on the risks inherent in online transactions. In online transactions with government organizations, one risk that should not be discounted is the risk of having personal data shared for online e-government services abused and misappropriated either by government organizations or by external third parties. Trust in the other party involved in the transaction, as initially pronounced in Chapter 5, somehow precipitates the reduction of risk perceptions related to a transaction with another party.

Cultivating clients' trust has become a prominent organizational agendum. For online commercial organizations, winning their clients' trust is a prerequisite for survival in a competitive environment. Customers who do not trust a particular online commercial organization can easily defect to a competitor assessed to be more trustworthy. In online commercial transactions, Internet users have a range of choices because products and services offered online are seldom monopolized by a particular organization.

The case is different in government transactions. Citizens have to file their income taxes annually, for instance, and they can only do it with the tax service office, which happens to be the sole entity designated to handle such matter. A government organization that channels its services online does not compete with other organizations. It competes with itself, particularly in terms of its mode of service delivery. When the delivery of government services online does not appeal to citizens, for lack of trust in or lack of knowledge of the said delivery mode, they always have the option of availing the same services offline.

While creating online trust is deemed problematic (Weckert, 2005), empirical studies on the determinants of Internet users' trust in organizations and in transactions with them, particularly in a commercial setting, proliferate. Trust cues such as a positive organizational reputation and security features have been found effective in cultivating Internet users' trust in organizations and in transactions through their websites.

Although research on trust in e-government is dawning, investigations into the determinants of trust in e-government are notably few. In this study, the impact of the factors hypothesized to positively influence trust in government organizations in terms of their processing and usage of citizens' personal data were determined. An online survey with respondents residing in one of the municipalities in the Netherlands was implemented to address the hypotheses of the research.

6.2 Trust within the digital environment

Availing online government services implies completing electronic registration forms. This subtly forces citizens to disclose personal information before a particular transaction can proceed and be completed. However, citizens may be getting more conscious about the risks involved in disclosing personal data online. Whatever personal information shared to an organization digitally could either be exploited by the organization collecting the information or by third parties that can easily acquire unauthorized access to such information using the most advanced technology available. The commoditization of personal data increases their susceptibility to abuse.

With risks or the belief in their existence comes the urgency to cultivate trust. In the context of online exchanges, Internet users must trust organizations before they can relish the benefits of transacting with those organizations online. The importance of trust in online transactions would constantly push organizations to improve and maintain their trustworthiness to gain people's loyal patronage of their products or services.

6.3 Cues and factors influencing trust in organizations in the digital environment

While not entirely a new phenomenon, transacting with organizations online has not yet attained the status of a socio-cultural norm. There certainly are many Internet users who have not yet engaged in computer-mediated exchanges. These are potential first timers who are bound to confront difficulties in trusting (Boyd, 2003). Whereas those with online transaction experience could somehow ground their trust on the quality of their previous transactions, those devoid of a similar experience would have to resort to other factors for trusting decisions.

Different empirical studies identify different cues or factors that could contribute to the formation of online trust. As discussed in Chapter 3, these cues or factors can be categorized into three: Internet user-based (propensity to trust, Internet experience), organization-based (quality of online transactional experience, organizational reputation), and website-based (website quality, website security, privacy statements). Most studies on trust determinants had been pursued within the context of online commercial exchanges. However, a number of those determinants are still applicable in understanding the development of trust in e-government.

6.3.1 Trust propensity

People significantly vary in their levels of trust (Mayer et al., 1995). Such variations in trust propensity or disposition, referring to the tendency to be willing to depend on others across a broad spectrum of situations and

persons (McKnight, Choudhoury, & Kacmar, 2002; McKnight, Cummings, & Chervany, 1998) are also evident in online economic exchanges wherein some people would display a greater disposition to trust anything and anybody and are more likely to trust online entities despite having limited information about them, while others would require more information about the trust target before deciding to trust (Salam et al., 2005). Low levels of trust propensity could be assumed to eventuate in minimal trusting decisions, while high levels of trust propensity could propel an increase in trusting decisions. The first hypothesis is founded on this proposition.

> *H1: Internet users with high levels of trust propensity have high levels of trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.3.2 Internet experience

A couple of studies indicated that high levels of Internet experience are associated with low levels of trust in online organizations (Aiken & Bousch, 2006; Jarvenpaa, Tractinsky, & Saarinen, 1999). A possible explanation is that with high levels of Internet experience, users may have already accumulated sufficient knowledge of possibilities that things could go wrong online (Aiken & Bousch, 2006).

Nonetheless, another study advanced that people's level of Internet experience is likely to affect their tendency to trust the Internet technology, thereby enhancing their trust in Internet-based transactions (Corbitt, Thanasankit, & Yi, 2003). The assertion can bank on the supposition that more knowledge of and experience with the Internet could spur greater confidence in using the Internet, which would inflate online trust (Bart et al., 2005). This is consonance with the view of the Internet as an 'experience technology', which implies that as experience online continues to build the likelihood for users to develop learned trust in the Internet would expectedly increase (Dutton, 2010). These arguments serve as a springboard for the second hypothesis.

> *H2: Internet users with high levels of Internet experience have high levels of trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.3.3 Organizational reputation

When a party, whether an individual or an organization, has a good reputation one will quickly develop trusting beliefs about that party even in the absence of firsthand knowledge (McKnight, Cummings, & Chevarny, 1998). In fact, users without any prior experience with an online organization consider the organization's reputation as an indicator of its trustworthiness (Chen, 2006; Kim, Ferrin, & Rao, 2003; Koufaris &

Hampton-Sosa, 2004; McKnight, Choudhoury, & Kacmar, 2002). Highly reputed organizations are regarded to act honestly in their daily operations, consider not only their interests but also of their exchange partners when making decisions, and be competent. These considerations could substantially reinforce their trustworthiness (Keh & Xie, 2009).

Organizations with a reputation to protect are not expected to engage in opportunistic behaviors (Herbig, Milewicz, & Golden, 1994), like selling their clients' personal information to third parties. Indeed, Internet users will not hesitate to disclose their personal information to well-known online organizations with an image to maintain (Olivero & Lunt, 2004).

Ganesan (1994) cites that organizational reputation can be assessed in terms of organizational fairness, concern, and honesty – criteria that closely resemble the indicators of trustworthiness as identified by several authors (e.g. Barber, 1983; Luhmann, 1979; Mayer et al., 1995; McKnight et al., 1998). This coincides with the view of reputation as a collective measure of the trustworthiness of a particular party based on other people's referrals (Josang, Ismail, & Boyd, 2007).

> *H3: Internet users' positive evaluation of government organizations' reputation positively influences users' trust in those organizations in terms of their processing and usage of citizens' personal data.*

6.3.4 Positive online transaction experience

Trust viewed as a prediction process, in consonance with the definition of trust as an expectation regarding the behavior of an exchange partner, implies that one party trusts another based on prior experiences demonstrating that the other party's behavior is predictable (Doney, Cannon, & Mullen, 1998). Sztompka (1999) stated that people readily trust those whose trustworthiness has been tested and those who did not fail them before. This underscores the importance of experience in the formation of trust in the other party.

A positive experience, which depends partly on one's level of satisfaction with the transaction or exchange, strongly relates with trust (Pavlou, 2003). People who are satisfied with their previous online transaction experience tend to trust the transactional partner for future exchanges (Casalo et al., 2007; Flavian et al., 2006; Pavlou, 2003). These arguments resulted in the fourth hypothesis.

> *H4: Internet users' positive experience with online government transactions positively influences users' trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.3.5 Perceived website quality

Users would be more inclined to trust organizations with websites that are professionally designed. A professionally designed website signifies that it is easily navigable. Users tend to trust organizations with websites having features that foster an 'ease of use experience' and enable them to reach their destinations quickly (Bart et al., 2005). Chau et al. (2007) claimed that the ease of using and navigating a website significantly influences customers' trust in an electronic vendor, especially during an initial encounter, for instance, when customers are still searching for information.

Information on websites can also be crucial for the appraisal of the credibility of websites (Fogg et al., 2003). The researchers noted that aside from information accuracy, information usefulness also matters when Internet users are at the point of determining whether or not a website is credible or trustworthy. Information on websites can be regarded as useful when they are able to address the needs of Internet users. An example would be contact information. Government websites that are navigable and that contain information, which Internet users can use to communicate with government organizations, could be regarded as trustworthy. These claims precipitate the fifth hypothesis.

> *H5: The quality of a government website positively influences Internet users' trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.3.6 Website security

Security is an important concern on e-government agenda (Blakemore et al., 2010). Apprehensions regarding unauthorized third-party access to users' personal data in organizational databases could prompt Internet users to look for an indication of the deployment of security technologies, such as encryption and authentication mechanisms. Koufaris and Hampton-Sosa (2004) pointed out that the presence of security mechanisms could significantly affect users' trust in initial online exchanges.

Security features are regarded as more important than privacy statements in building users' trust, since the former is easier to recognize and understand than the latter (Belanger, Hiller, & Smith, 2002). Security, aside from privacy, is regarded an important baseline from which Internet users appraise the trustworthiness of an online entity (Urban, Amyx, & Lorenzon, 2009). Streaming from these assertions is the sixth hypothesis for this study.

> *H6: The availability of security features on government websites positively influences Internet users' trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.3.7 Privacy statements

Risk perceptions related to the disclosure of personal data could prompt Internet users to clamor for an assurance that their personal data once disclosed will not be abused, but instead treated confidentially and with respect. In most cases, online privacy statements are the only sources of information for users to be adequately informed of organizational usage and processing of people's personal data (Vail, Earp & Anton, 2008). Internet users who are very concerned about their information privacy would be expected to consult online privacy statements before opting to disclose personal information (Jensen & Potts, 2004; Pan & Zinkhan, 2006).

Although privacy statements are seldom never read or consulted (Arcand et al., 2007; Beldad, De Jong, & Steehouder, 2010; Jensen, Potts, & Jensen, 2005; Meinert et al., 2004; Myerscough, Lowe, & Alpert, 2006), their mere presence on a website could already influence users' trust in an online organization (Lauer & Deng, 2007; Meinert et al., 2004; Pan & Zinkhan, 2006) and increase the assessed dependability of the organization (Schoenbachler & Gordon, 2002). However, Internet users must have confidence in online privacy statements first before the aforementioned documents can increase users' trust in organizations behind those websites. This claim spurs the seventh hypothesis of the research.

> *H7: Internet users' confidence in privacy statements on government websites positively influences users' trust in government organizations in terms of their processing and usage of citizens' personal data.*

6.4 Methodology

6.4.1 Survey participants

A research agency affiliated with the Dutch municipality of Zwolle was contracted to implement an online survey for two weeks to collect the data necessary to address the research hypotheses. A link to the Internet-based questionnaire was sent to the 2,500 members of the research panel. A total of 1,156 completed online questionnaires were returned, resulting in a response rate of 46.42 percent.

A balance in the male/female ratio in the sample was achieved. Respondents' age ranged from 18 to 86 years, with a mean of 48.26 (SD = 14.79). In terms of Internet experience (measured in years), close to two-thirds of the participants indicated that they have been using the Internet for 9 to 16 years already (N = 840, 72.7%). Table 6.1 presents the complete demographic information of the survey participants.

Table 6.1. Demographic information of survey respondents (N = 1,156)

Demographic characteristics		Freq.	%
Gender	Male	579	50.1
	Female	577	49.9
Age	18 to 24 years old	61	5.3
	25 to 34 years old	166	14.4
	35 to 44 years old	263	22.8
	45 to 54 years old	258	22.3
	55 to 64 years old	239	20.7
	65 years or older	169	14.6
Internet experience	1 to 4 years	20	1.7
	5 to 8 years	209	18.1
	9 to 12 years	498	43.1
	13 to 16 years	342	29.6
	16 years or more	87	7.5

6.4.2 Survey instrument

In the first part of the survey, data on respondents' demographic characteristics were collected. The second part of the survey contained questions pertinent to the variables of the study. Tables 6.2 and 6.3 show the items or statements comprising the different constructs. The statements were originally formulated in Dutch. Except for the items included in the variable 'trust in government organizations in terms of their processing and usage of citizens' personal data', which were measured on ten-point Likert scales (10 for *very high trust*; 1 for *very low trust*), most of the items for the other variables were measured on five-point Likert scales (from *strongly agree* to *strongly disagree*) with some items having an 'I have no idea' option.

Most of the items were newly formulated for this particular study and were based on the responses given during three focus group discussion (FGD) sessions conducted four months prior to the implementation of the survey. However, items comprising 'propensity to trust', which included trust in and reliance on other people and a belief that people have good intentions, were derived from the instruments of Gefen (2000) and Gefen and Straub (2004).

Two statements to measure organizational reputation ('Government organizations have the reputation of being honest….' and 'Government organizations have the reputation of being concern…') were derived from the instrument of Ganesan (1994). A third statement 'Government organizations have the reputation of being competent…' was eventually added to measure organizational reputation.

'Quality of previous online transaction experience' was measured in terms of whether or not Internet users were satisfied with and positive about their e-government exchange encounters. The construct 'confidence in privacy statements on government websites' focused on the notion of privacy statements as potent instruments for increasing beliefs that organizations that post those documents on their websites will not exploit their clients' personal data and that they can be trusted with those data.

'Website security' was measured in terms of whether or not government organizations employ the necessary technology to protect citizens' personal data and have the ability to authenticate the identities of Internet users who used government websites for transactions. For 'website quality', statements on the ease of navigating government websites and the availability of relevant information (e.g. contact information) on the websites were included.

Respondents with e-government experience were segregated from those without through a question on whether or not they have transacted with a government organization through its website. Those who have availed government services online (N = 959) were directed to the questionnaire that included two items to measure the quality of their previous online government transactions.

6.5 Results

6.5.1 Factor analysis of the items comprising the variables for the survey instrument designed for respondents with e-government experience

A principal component analysis was conducted on the 20 items comprising the online questionnaire for respondents with previous online government transaction experience. The value of the Kaiser-Meyer Olkin Measure of Sampling Adequacy was pegged at .85, which was higher than the recommended value of .60 (Kaiser, 1974), while the Bartlett's Test of Sphericity X^2 (231) = 9,996.80, $p < .001$ revealed that the correlations among the 20 items were sufficiently high for principal component analysis.

Eigenvalues for the seven components were above the Kaiser's criterion of 1 and in combination accounted for 72.16 percent of the variance. Shown in Table 6.2 are the factor loadings after rotation of the items for the questionnaire designed for respondents with e-government experience. Items below .40 were intentionally removed from the table.

Table 6.2. Results of factor analysis (with VARIMAX rotation) of the items for the survey instrument designed for respondents with e-government experience

Construct	Items	Component						
		1	*2*	*3*	*4*	*5*	*6*	*7*
Quality of previous online government transaction experience	My online transactions with government organizations have always been good.						.86	
	I have no negative experiences in transacting online with government organizations.						.90	
Propensity to trust	I trust people in general.		.83					
	I tend to count upon other people.		.73					
	I generally have faith in humanity.		.83					
	I feel that other people have generally good intentions.		.83					
Reputation	Government organizations have the reputation of being competent in carrying out online transactions with citizens.				.77			
	Government organizations have the reputation of being honest in carrying out online transactions with citizens.				.85			
	Government organizations have the reputation of taking the interests of the citizens into consideration during online transactions.				.79			
Confidence in online privacy statements	I feel confident that government organizations will not abuse my personal data when their websites have privacy statements.			.78				
	I am sure that government organizations will treat my personal data confidentially when their websites post privacy statements.			.82				
	It is my belief that government organizations that post privacy statements on their websites can be trusted with my personal data.			.81				
Website security	The websites of government organizations use appropriate technologies to protect users' personal data from unauthorized third-party access.					.74		
	The websites of government organizations have the ability to authenticate users for security purposes.					.74		
	The websites of government organizations work very well technically					.74		
Website quality	Websites of government organizations are easy to navigate.							.85
	Websites of government organizations contain relevant information, such as information on how I could contact them.							.83
Trust in government organizations in terms of their processing and usage of citizens' personal data	Trust in the government, in general, in terms of its processing and usage of citizens' personal data.	.89						
	Trust in municipalities in terms of their processing and usage of citizens' personal data.	.90						
	Trust in the tax service office in terms of its processing and usage of citizens' personal data.	.89						

6.5.2 Factor analysis of the items comprising the variables for the survey instrument designed for respondents without e-government experience

A principal component analysis was also conducted on the 18 items comprising the online questionnaire for respondents without online government transaction experience. The value of Kaiser-Meyer Olkin Measure of Sampling Adequacy was .80. Correlations among the 18

itemswere also high for principal component analysis as shown by the Bartlett's Test of Sphericity X^2 (190) = 2,505.91, p < .001.

The six components also had *eigenvalues* above the Kaiser's criterion of 1 and explained for 76.09 percent of the variance. Presented in Table 6.3 are the factor loadings after rotation of the items for the questionnaire designed for respondents without e-government experience. Items below .40 were also intentionally removed from the table.

Table 6.3. Results of factor analysis (with VARIMAX rotation) of the items for the survey instrument designed for respondents without e-government experience

Construct	Items	Component					
		1	*2*	*3*	*4*	*5*	*6*
Propensity to trust	I trust people in general.			.83			
	I tend to count upon other people.			.71			
	I generally have faith in humanity.			.86			
	I feel that other people have generally good intentions.			.83			
Reputation	Government organizations have the reputation of being competent in carrying out online transactions with citizens.	.91					
	Government organizations have the reputation of being honest in carrying out online transactions with citizens.	.91					
	Government organizations have the reputation of taking the interests of the citizens into consideration during online transactions.	.88					
Confidence in online privacy statements	I feel confident that government organizations will not abuse my personal data when their websites have privacy statements.				.82		
	I am sure that government organizations will treat my personal data confidentially when their websites post privacy statements.				.84		
	It is my belief that government organizations that post privacy statements on their websites can be trusted with my personal data.				.86		
Website security	The websites of government organizations use appropriate technologies to protect users' personal data from unauthorized third party-access.						.74
	The websites of government organizations have the ability to authenticate users for security purposes.						.79
	The websites of government organizations work very well technically						.53
Website quality	Websites of government organizations are easy to navigate.					.87	
	Websites of government organizations contain relevant information, such as information on how I could contact them.					.85	
Trust in government organizations in terms of their processing and usage of citizens' personal data	Trust in the government, in general, in terms of its processing and usage of citizens' personal data.		.94				
	Trust in municipalities in terms of their processing and usage of citizens' personal data.		.95				
	Trust in the tax service office in terms of its processing and usage of citizens' personal data.		.90				

6.5.3 Construct Reliability

Cronbach's alpha scores were also calculated to determine the reliability of the scales. With the exception of 'website security' (respondents with e-government experience), all the constructs included for

the survey instrument for respondents with and without previous online government transaction experience have alpha scores above .70, which indicate adequate reliability (Hinton, 2008). Table 6.4 shows the reliability scores and the mean and standard deviation values of the constructs included in the survey instruments for respondents with and without e-government experience.

Table 6.4. Alpha scores and mean and standard deviation values of the variables of the study

Variables	No. of Items	With e-government experience (N = 959)			Without e-government experience (N = 197)		
		a	*Mean*	*SD*	*a*	*Mean*	*SD*
Quality of previous experience with online government transactions	2	.83	3.82	0.74	-	-	-
Propensity to trust	4	.82	3.67	0.58	.83	3.57	0.59
Government organizational reputation	3	.83	3.27	1.05	.94	2.14	1.58
Confidence in privacy statements	3	.84	3.72	0.84	.87	3.38	1.06
Website security	3	.68	2.75	1.17	.72	2.51	1.24
Website quality	2	.72	3.24	0.92	.81	2.85	1.35
Trust in government organizations in terms of their processing and usage of citizens' personal data	3	.94	7.03	1.57	.95	6.50	1.56

6.5.4 Determinants of trust in government organizations among respondents with e-government experience

Hierarchical regression analysis, which enabled the entrance of the different variables in blocks, was employed to identify the determinants of respondents' trust in government organizations in terms of their processing and usage of citizens' personal data. The entrance of the independent variables in three blocks was in consonance with the three-fold categorization of the hypothesized determinants of online trust, as discussed in Chapter 3.

Internet user-based trust determinants, primarily propensity to trust and level of Internet experience, were entered in the first block resulting in an R^2 value of .02 ($F_{2, 956} = 11.83$, $p < .001$). Organizational reputation and quality of previous online government transaction experience, both organization-based trust determinants, were entered in the second block raising the R^2 value to .19 ($F_{4, 954} = 57.28$, $p < .001$). Website quality, website security, and confidence in privacy statements were entered in the third block with an R^2 value pegged at .33 ($F_{7, 951} = 65.84$, $p < .001$). This signifies that 33 % of the variance of respondents' trust in government organizations in terms of their processing and usage of citizens' personal information is attributable to the seven variables.

Looking at the complete model, it is evident that confidence in privacy statements on government websites (b = .41, $p < .001$), government organizational reputation (b = .22, $p < .001$), and the quality of Internet users' online transaction experience with government organizations (b = .09, $p < .01$) significantly accounted for the variance in trust in government

organizations. Confidence in online privacy statements appears to perform a pivotal role in augmenting respondents' trust in government organizations in terms of their processing and usage of citizens' personal data. This supports the second hypothesis.

When deciding whether or not to trust a government organization, those with e-government experience also assess the reputation of government organizations. High estimation of government organizational reputation evidently results in high levels of trust. Hence, the acceptance of hypothesis 4 is justified. This corroborates results of numerous studies that accentuate the positive impact of organizational reputation in ameliorating people's trust in organizations, whether in online or offline contexts.

Hypothesis 5 is also supported since the quality of one's online government transaction experience is found to contribute to Internet users' trust in government organizations in terms of their processing and usage of citizens' personal information. Table 6.5 shows both the non-standardized and the standardized coefficients of the different variables hypothesized to positively influence users' trust in government organizations in terms of their processing and usage of citizens' personal data.

Table 6.5. Coefficients of the variables hypothesized to influence trust in government organizations in terms of their processing and usage of citizens' personal data among respondents with e-government experience

		B	SE B	β	R^2 (ΔR^2)
Step 1					
	Constant	5.53	.34		
	Propensity to trust	.42	.09	.16 ***	.02 (.02)
	Internet experience (measured in years)	-.00	.01	-.01	***
Step 2					
	Constant	3.27	.37		
	Propensity to trust	.20	.08	.07 *	.19 (.17)
	Internet experience (measured in years)	-.01	.01	-.02	***
	Government organizational reputation	.60	.05	.35 ***	
	Quality of previous online government transaction experience	.28	.07	.13 ***	
Step 3					
	Constant	2.28	.35		
	Propensity to trust	.09	.08	.03	.33 (.14)
	Internet experience (measured in years)	-.01	.01	-.01	***
	Government organizational reputation	.37	.06	.22 ***	
	Quality of previous online government transaction experience	.18	.06	.09 **	
	Website quality	-.12	.06	-.06	
	Website security	.03	.04	.02	
	Confidence in privacy statements	.76	.06	.41 ***	

*** $p < .001$, ** $p < .01$, * $p < .05$

6.5.5 Determinants of trust in government organizations among respondents without e-government experience

To determine the factors that influence trust in government organizations among respondents without e-government experience (N = 197), hierarchical regression analysis was also employed. The procedure of entering the independent variables into three blocks was also used for this analysis. Propensity to trust and level of Internet experience were entered in the first block resulting in an R^2 value of .03 ($F_{2, 194} = 2.72$, *p value not significant*). The entrance of government organizational reputation in the second block spurred a slight increase in the R^2 value of .05 ($F_{3, 193} = 3.07$, $p < .05$). In the third block, website quality, website security, and confidence in privacy statements were entered resulting in an R^2 value of .16 ($F_{6, 190} = 5.88$, $p < .001$). This means that 16 percent of the variance in respondents' trust in government organizations can be explained by the six variables.

In the final model, only confidence in privacy statements (b = .34, *p < .001*) positively influences trust in government organizations among respondents without e-government experience. This precipitates the acceptance of the fifth hypothesis. The relatively small value for the variance in trust in government organizations among those without e-government experience implies two possibilities. First, there are still other factors that could possibly enhance trust in government organizations. Second, trust among those without any e-government experience could not be easily acquired through the usage of trustworthiness cues. It is highly probable that those without e-government experience will need to have an online government transaction experience first before they can actually trust government organizations in terms how they use and process citizens' personal data.

While organizational reputation played a crucial role in improving trust in government organizations among respondents with e-government experience, the aforementioned factor does not have any impact on trust in government organizations among those without e-government experience. One possible explanation is that respondents who have not transacted with government organizations online have a lower estimation of the reputation of government organizations, as indicated by a low mean score of 2.14 (SD = 1.58) – representing 'disagreement' with the items comprising the reputation construct. The fact that website security did not increase the trust of those without e-government experience could be attributed to the possibility that they did not know whether or not government organizations are using security technologies to protect citizens' personal data.

Presented in Table 6.6 are the non-standardized and the standardized coefficients of the different variables hypothesized to positively influence trust in government organizations in terms of their processing and usage of citizens' personal data among respondents without e-government experience.

Table 6.6. Coefficients of the variables hypothesized to influence trust in government organizations in terms of their processing and usage of citizens' personal data among respondents without e-government experience

		B	SE B	β	R^2 (ΔR^2)
Step 1					
	Constant	4.86	.73		
	Propensity to trust	.43	.19	.16 *	.03 (.03)
	Internet experience (measured in years)	.01	.03	.02	
Step 2					
	Constant	4.45	.76		
	Propensity to trust	.44	.19	.17 *	.05 (.02)
	Internet experience (measured in years)	.01	.03	.03	*
	Government organizational reputation	.16	.08	.14	
Step 3					
	Constant	3.61	.75		
	Propensity to trust	.28	.18	.11	.16 (.11)
	Internet experience (measured in years)	-.00	.03	-.01	***
	Government organizational reputation	-.03	.09	-.03	
	Website quality	.08	1.00	.06	
	Website security	.05	1.00	.04	
	Confidence in privacy statements	.50	.11	.34 ***	

*** $p < .001$, ** $p < .01$, * $p < .05$

6.6 Discussion

Several factors have been identified to increase Internet users' trust in online organizations. For instance, studies on trust in online commercial organizations have indicated that cues such as an indication of adequate security, privacy statements on websites, and website quality can positively influence people's assessment of the trustworthiness of organizations, while intangible factors such as organizational reputation and quality of experience with previous online transactions have similar effects. However, as reported in one study (Bart et al., 2005), the effects of different cues are different across site categories and consumers.

Results of this online survey with Dutch respondents – with and without e-government experience – reveal that Internet users' confidence in online privacy statements is a very important determinant of their trust in government organizations in terms of how they use and process citizens' personal data. Among respondents with e-government experience, the quality of their previous online government transactions and the positive reputation of government organizations (in terms of their perceived competence, honesty, and concern) also play pivotal roles in shaping their trust in government organizations.

It is unfortunate, however, that not everybody can claim to rely on their previous online transaction experience for a crucial decision on whether or not to trust a particular government organization in the online environment. Those devoid of experience, therefore, would be pressed to employ other criteria in assessing the trustworthiness of the online

exchange partner. However, people's abilities to make decisions on rational grounds are bounded since they do not always possess complete information about alternatives (Simon, 1955; 1972).

Even if users have access to sets of information relevant for rational decision-making, most will opt for a shorter route to reach a decision even if not rationally founded. As the model of elaboration likelihood advances (Petty & Cacioppio, 1986), a substantial decrease in people's motivation to process complete information and messages heightens the significance of peripheral cues as determinants of persuasion – in this case, the willingness to trust. In the context of online transactions and exchanges, either bounded rationality or decreased motivation to resort to complete processing of information could explain people's dependence on cues such as online privacy statements and a positive organizational reputation.

It may be unsurprising that the quality of a government website did not influence trust in government organizations in terms of how they process and use citizens' personal data. However, only two items were used to measure 'website quality'. This echoes the need to consider other elements that could measure this construct.

The absence of the impact of website security on trust in the aforementioned concern seems discomforting considering that previous studies on the determinants of trust in online transactions, particularly those that are commercial in nature, underscored that the said factor is essential in increasing Internet users' trust in online transactions and in organizations they are transacting with. The absence of effect of security on trust could be attributed to the respondents' low perception of the usage of security mechanisms by government organizations. Most of the respondents did not seem to agree that government organizations employ adequate security measures to ensure the safety of citizens' personal data. However, the evaluation of security measures is targeted towards a more general variable 'trust in government organizations'.

It is very probable that security measures used by different government organizations vary. For instance, one organization may be using a more stringent security mechanism than another organization. While the current research did not look into an estimation of the levels of security deployed by municipalities and the tax service office, future research could consider dwelling on this concern to see if there really are variations in the deployment of security measures among different types of government organizations and to ascertain whether or not such variations would heighten citizens' trust in those organizations.

6.7 Implications and recommendations

The factors that have been found statistically significant in increasing trust in government organizations are elements that any government organization can work on and address to improve and fortify their trustworthiness. Simple cues, if one looks at the results of this study,

could have an enormous impact on organizational efforts to win citizens' trust.

Several studies have already indicated that, although not often read, the availability of privacy statements on websites are effective in quelling Internet users' apprehensions of supplying any information about themselves electronically. This online survey somehow provides enough empirical evidence to assert that confidence in privacy statements on the websites of government organizations is of paramount importance in increasing citizens' trust in government organizations in terms of how they will deal with citizens' personal data.

Nonetheless, available privacy statements would just be irrelevant if finding them is too burdensome. As revealed in a study on the ease of accessing privacy statements on municipal websites (Beldad, De Jong, & Steehouder, 2009), privacy statements on a number of municipal websites were practically difficult to find as they were either not labeled or located in other sections of the websites that were labeled differently.

Government organizations, therefore, should not only strive to include privacy statements on their websites but also increase the ease of finding them whenever available. Furthermore, the posting of online statements should be regarded as an ethical responsibility of informing citizens how their data will be used, processed, and protected. Even if they are not always perused, the few who do due to the perceived risks involved in online information disclosure (Milne & Culnan, 2004), would be expected to clamor for sufficient guarantees that disclosed personal data will not be abused and will only be used for the purposes they were collected for. This only implies that government organizations should employ privacy statements as appropriate media to emphasize transparency in their processing and usage of citizens' personal data.

Banks and other commercial organizations have a lot to lose if they fail to maintain their clients' trust, considering the stiff competition in the market. People would not hesitate to abandon online shops or other commercial institutions that could not be trusted. Messing with people's trust in a competitive market, hence, would be catastrophic for a particular commercial organization, as cited in Chapter 4.

However, government organizations may not have to worry about not earning citizens' trust in electronic government transactions because they have monopoly over government services and products. Nevertheless, despite this monopoly, a particular government organization that channels its services online still faces an unwarranted but real competition. It competes with itself in terms of the mode of its service delivery. Citizens who opt not engage in online transactions with a particular government organization, perhaps for lack of trust in or lack of knowledge of the aforementioned mode of transaction, always have the possibility to engage in the same transaction through the government organization's office.

One can only imagine the significant loss in the investment for the construction and implementation of electronic channels for government service delivery if a substantial number of citizens would just prefer to

transact with organizations offline. It is, therefore, important that citizens do not only appreciate the benefits of electronic government services but also trust government organizations for online transactions.

Cues such as privacy statements may not suffice to persuade most citizens that a particular government organization can be trusted with their personal data. In fact, 'privacy fundamentalists' might just regard conspicuous trustworthiness cues as subtle attempts to manipulate citizens' trust. In this case, government organizations might not succeed in winning citizens' trust with the simple use of trustworthiness cues. Instead, they need to resort to the fortification of their images as trustworthy institutions by not resorting to activities that could be regarded as a betrayal of public trust, such as the accidental, or even intentional, disclosure of citizens' personal data to online and offline channels.

The findings of this study have strong implications not only for policy decisions on e-government management but also for future research. One of the limitations of the current study is its reliance on a sample, though sizeable enough for analysis, comprised of respondents residing in just one municipality. The generalizability of the findings can be limited by this weakness. Therefore, future research should consider using a sample closely representing a national population.

Another thing that merits attention is the inclusion of the items to measure 'website quality'. In this study, the construct was measured in terms of the navigability of government websites and the availability of relevant information on those websites only. However, other indicators should be included to measure 'website quality' such as the use of colors, the types and quality of photographs, and the completeness and correctness of information on websites.

In the survey, trust in government organizations in terms of their processing and usage of citizens' personal information is measured through an appraisal of the trustworthiness of different government organizations (e.g. municipalities, the tax service). Since users' levels of trust in government organizations considerably differ, it can also be expected that the impact of the different trustworthiness cues on trust would vary. Looking into the determinants of trust in a particular government organization, therefore, could be regarded as a logical research pursuit.

6.8 Conclusion

The proliferation of investigations on the determinants of trust in online transactions is symptomatic of the fact that online trust is something that organizations can influence. With risk perceptions potent enough to curtail people's willingness and intentions to engage in computer-mediated transactions, organizations enabling those transactions are eventually confronted with the urgency to establish and maintain their trustworthiness. As a myriad of studies indicate, trust is indispensable in triggering the performance of any human behavior.

Most online transactions, as already noted, primarily necessitate the disclosure of personal information, which is somehow considered risky. Perceptions of the risks involved in online information disclosure need to be countered by the belief that the entity collecting personal data can be trusted. With trust in place, information disclosure could be forthcoming. In the context of e-government, a number of trustworthiness cues, as the current study reveals, are vital in influencing citizens' trust in government organizations in terms of their processing and usage of citizens' personal information. For instance, the impact of available and findable online privacy statements on trust in government organizations, among Internet users with e-government experience and those without, is hardly discountable.

Broadening the scope of research on trust in e-government should be seen in tandem with the pursuit of understanding how trust within the context of online government transactions could be created or developed. Trust in government organizations in an online environment, hence, should be regarded not just as an antecedent of e-government adoption but also as a desirable outcome to be pursued.

7

I trust not therefore it must be risky: Determinants of risk perceptions involved in online disclosures of personal data for e-government transactions

One of the important findings of the study described in Chapter 5 is that Internet users' trust in a government organization (in terms of its processing and usage of citizens' personal data) could reduce perceptions of the risks involved in the disclosure of personal data for e-government services. The conception of trust in that study, however, centered only on the behavior of government organizations toward citizens' personal data. In the study that is described in this chapter, trust is re-conceptualized to target the ability and the willingness of government organizations to safeguard personal data collected from citizens.

Citizens' trust in the organizations' ability and willingness to protect citizens' personal data is hypothesized to be negatively related to perceptions of the risks involved in online personal information disclosure. Risk perceptions are also hypothesized to be positively related to the assessed sensitivity of personal data that will be disclosed. Results of the online survey described in this chapter revealed that Dutch Internet users' lack of trust in a government organization's ability to protect citizens' personal data and users' assessment of the sensitivity of requested personal data could significantly influence users' perceptions of the risks involved in supplying personal data for e-government services.

This chapter is based on a manuscript by Beldad, A., De Jong, M., & Steehouder, M., which is currently under review.

7.1 Introduction

Just as human activities (MacCrimmon & Wehrung, 1986) and exchanges (Molm, Takahashi, & Peterson, 2000) are risky, those pursued in borderless electronic environments are also constantly beleaguered by a host of risks. As people and communities are getting webbed and interactions and transactions digitized, the push to live a second life online is inexorable. We send emails, join networking sites, buy the bestselling books, book our flights, file our taxes, purchase our pills, and pay our bills – all through the almost ubiquitous Internet at the comfort of wherever we are, whenever we like to.

The convenience of doing things online, however, is not costless. Whereas online commercial exchanges rest on monetary payments and personal information disclosures, those that are non-commercial in nature (e.g. signing in for an email address or joining networking sites) primarily compel users to supply pieces of personal information for the completion of an online registration.

Studies in the context of electronic transactions suggest that perceptions of risks, referring to a felt uncertainty regarding possible negative consequences of using a product or a service (Featherman & Wells, 2004) inhibit the formation of a positive attitude towards online economic exchanges (Kim Ferrin, & Rao, 2008). This would eventually result in users' reluctance to adopt or use electronic services (Featherman & Pavlou, 2003; Featherman & Wells, 2004; Liu & Wei, 2003; Ruyter, Wetzels & Kleijnen, 2000) and to share information necessary for an online transaction (McKnight, Choudhoury, & Kacmar, 2002).

Online organizations and companies can counter Internet users' perceptions of the risks involved in online transactions by asserting their trustworthiness (Kim, Ferrin, & Rao, 2008). This corresponds to the supposition that as long as an online organization is assessed to be trustworthy and can be trusted, transactions with the organization would not be perceived as risky.

The heightened popularity of transactions with government organizations through their websites further signifies that citizens are increasingly pushed to share their personal data in the virtual environment. This is logical since an application for a government document, as already underscored, would be impossible to complete without the acquisition of necessary personal information from an applicant. However, online sharing of personal data, even to a government organization, could hardly be considered safe.

As already cited in the previous chapters, personal data, with their relative economic value, can be exploited either by the organization collecting them or by external third parties. Secondary usage of personal data could have adverse consequences for the person to whom the data pertain. Thus, it would be unsurprising that disclosing personal data in the digital environment would be regarded risky. This study investigated the

factors influencing Dutch Internet users' perceptions of the risks involved in an online disclosure of personal data for e-government services. An Internet-based survey was implemented to test the research hypotheses.

7.2 A brief acquaintance with 'risk'

From a general, context-free perspective, risk is defined as the potential for the realization of unwanted, negative consequences of an event (Rowe, 1977). At a general level, risk involves two major components. First, there is the existence of a possible unwanted consequence or loss. Second, there is an uncertainty in the occurrence of that consequence, which can be expressed in the form of a probability of an occurrence (Rowe, 1977). However, MacCrimmon and Wehrung (1986) also argued that risks can be broken down into three components: (1) the magnitude of a loss or an injury; (2) the chance of a loss or an injury; and (3) the exposure to a loss or an injury. The notion of risk signifies a person's exposure to probabilistic outcomes (Williamson, 1993).

In various situations, people may or may not be aware that they are at risk. They may voluntarily assume risks or have risks imposed on them. Risk, therefore, can be categorized as conscious and unconscious, as voluntary and involuntary (Wartofsky, 1986), and, even as calculable and non-calculable (Arnoldi, 2009). Risk is often interchanged with the notion of uncertainty (Denney, 2005; Lupton, 1999), which can be attributed to the premise that uncertain consequences are considered as a component of risk (Litter & Melanthiou, 2006).

However, the distinction between risk and uncertainty is pronounced in a number of studies on risk. While risk refers to the known or knowable probabilities of the outcomes of actions or events, uncertainty can be used to describe situations wherein probabilities of the outcomes of actions or events are inestimable and unknown or, even, not meaningful (Lupton, 1999; Mellor, 2007).

Just as people vary in their propensity to trust (Mayer, Davis, & Schoorman, 1995), risk propensity, defined as a willingness to take risks (Das & Teng, 2004), also differs among individuals (Wang, Kruger, & Wilke, 2009), and so are perceptions of risks (Breakwell, 2007), referring to a subjective belief that there is a probability of suffering a loss in pursuit of a desired outcome (Pavlou & Gefen, 2004). Studies on risks have prominently focused on risk perceptions instead of risk *per se* (Pavlou & Gefen, 2004) since the latter is difficult to measure as an 'objective reality' compared to the former (Pavlou & Gefen, 2004; Warkentin et al., 2002).

7.3 Perceptions of risks online

With exchanges and encounters getting digitized, weighing the blessings of online exchanges and transactions against their potential risks becomes an urgent concern since risks, according to Rousseau et al. (2003),

thrive in computer-mediated interactions. Risks in the virtual environment could either be behavioral or environmental (Pavlou, 2003). Pavlou pointed out that risks are behavioral because of the possibility on the part of online organizations to behave opportunistically by taking advantage of the distant and impersonal nature of online exchanges (e.g. product misrepresentations, personal data leaks, denunciation of product warranties). Environmental risks, he added, exist because of the unpredictable and open nature of the Internet, which is beyond the control of the online organization or the Internet user (e.g. unauthorized third-party access to users' personal data).

It is important to note, however, that perceptions of online risks vary according to the context of the transaction and the organization as the other party in an online transaction. Risk perceptions in e-commerce and e-government, for instance, are significantly different – with users perceiving more risks in the former than in the latter (Belanger & Carter, 2008).

Loss of money and loss of information privacy resulting from data abuse or misuse are two prominent risks that can be expected in e-commerce. In electronic government transactions, the most crucial risk is the possibility of losing one's online information privacy, which could be attributed to the potential misuse of personal data shared to avail a particular government service online. Personal data can be accessed by unauthorized third parties, rented or sold to other organizations, or just used for purposes unknown to the person to whom the data pertain.

7.4 Level of trust and degree of risk perceptions

In interactions that require trust, risk is often viewed in relation with an interaction partner (Koller, 1988), since human relationships are peppered with different levels of risks (Sheppard & Sherman, 1998). Although the presence of trust could reduce risk perceptions in human relationships, some risks can still be perceived even when people trust one another (McKnight, Cummings, & Chervany, 1998). Sources of risks in trusting situations are generally associated with vulnerability and/or uncertainty about an outcome (Doney, Cannon, & Mullen, 1998).

However, the relationship between trust and risk perception, or risks in general, is quite muddled (Lim, 2003; Mayer, Davis, & Schoorman, 1995; McLain & Hackman, 1999), since it is not clear whether risk determines trust, risk is trust, or risk is a consequence of trust (Mayer, Davis, & Schoorman, 1995). Trust is regarded as a 'means of dealing psychologically with risks that would otherwise paralyze actions or lead to feelings of engulfment, dread, or anxiety' (Lupton, 1999). Risk is also seen as a characteristic of trust (Lahno, 2004).

The coupling of trust with risk is rooted on the mainstream conceptualization of trust as an acceptance of and exposure to vulnerability (Doney, Cannon, & Mullen, 1998; Mayer, Davis, & Schoorman, 1995; Rousseau et al., 2003). The apparent lack of clarity in the relationship

between trust and risk, however, eventually leads to different streams of trust-risk relationship conceptualizations.

Trust is viewed as a determinant of the amount of risk one is willing to take (Mayer, Davis, & Schoorman, 1995). This notion received significant support from several empirical studies on trust in online commercial exchanges (Grazioli & Jarvenpaa, 2000; Kim, Ferrin, & Rao, 2008; Kim & Kim, 2005; Pavlou, 2003). One empirical study revealed that the effect of perceived risks on trust is not statistically significant, while another study regarded trust (or the lack thereof) as a significant antecedent of perceived risks – which suggests that the direction of the causal relationship stems from trust to perceived risks and not the other way around (Pavlou, 2003).

The presence of trust makes Internet users less sensitive to risk considerations (Grazioli & Jarvenpaa, 2000), which would prompt them to lower their risk perceptions (Kim, Ferrin, & Rao, 2008) and help them overcome such perceptions (Salam, Rao, & Pegels, 2003). A study on trust in e-government reveals that citizens' trust in the government organization reduces their perception of the risks in using electronic government services (Belanger & Carter, 2008).

With the prevalence of technologies that enable unauthorized third party access to personal data stored in organizational electronic databases, Internet users would certainly expect that online organizations have the technical competence to protect whatever data they will collect from their clients. And with the economic value attached to personal data, making them enticing commodities to be profitably traded with other organizations, users would certainly count on the organization's willingness to respect the privacy and confidentiality of personal data it collects, by not using those data for purposes inconsonant with the actual reasons for their collection.

In Chapters 5 and 6, trust was conceptualized to target a government organization's expected behavior, specifically in terms of how it will use and process citizens' personal data. This is a response to the potential risk of having citizens' personal data exploited by government organizations. For instance, government organizations might transmit such data to other government agencies without the knowledge and consent of data owners. However, government organizations are not the only 'threats' to citizens' information privacy. With the right technology and technical expertise, external parties can also gain unlawful access to personal data in government electronic databases. This prompts the need for security.

Security is not something inherent in the Internet. Personal data supplied online could be spared from abuse not because the Internet is naturally safe but because parties that collect those data have done whatever is necessary to safeguard them. Thus, with the duality of the risks in disclosing personal data online, it is not enough that a government organization is willing to respect the confidentiality of citizens' personal data. That same organization must also have the competence to protect such data from external intrusion.

The reconceptualization of trust as a belief in a government organization's willingness and ability to protect citizens' personal data is predicated on the arguments just presented. This also corresponds to the definition of trust as a 'belief that a specific other will be able and willing, in a discretionary situation, to act in the trustor's best interest' (McLain & Hackman, 1999).

If users do not trust that a government organization is able and willing to protect citizens' personal data, an increase in their perceptions of the risks involved in sharing personal data online can be expected. This prompts the study's first two hypotheses:

> *1A. Internet users' trust in a government organization in terms of its **ability** to protect citizens' personal data is negatively related to perceptions of the risks involved in the disclosure of such data for e-government services.*
>
> *1B. Internet users' trust in a government organization in terms of its **willingness** to protect citizens' personal data is negatively related to perceptions of the risks involved in the disclosure of such data for e-government services.*

7.5 Assessment of data sensitivity and risk perceptions

Perceptions of the risks involved in an online disclosure of personal data would not be so high if such data are not appraised as too sensitive and the disclosure of such data will not result in negative consequences for the person to whom the data pertain. However, Internet users are often not in the position to know how their personal data would be used by organizations. Unauthorized collection and secondary usage of Internet users' personal data have been identified as critical factors triggering information privacy concerns (Pan & Zinkhan, 2006).

Internet users have been clamouring for control over any personal information they disclosed online (Earp et al., 2005; Olivero & Lunt, 2004; Phelps, Nowak, & Ferrell, 2000; Sheehan & Hoy, 2000) either as an attempt to protect themselves from information privacy risks or as an assertion of their right of ownership over their information (Olivero & Lunt, 2004). Internet users' concerns regarding the protection of their personal data propel the creation of boundaries around their data (Metzger, 2007). Perceptions of the risks involved in the disclosure of personal data online also influence Internet users' intention to adopt some types of protection strategies and their intention to resort to online privacy-protecting behaviors (Ommen & Leenes, 2008), either by using technology-based protection strategies (Ommen & Leenes, 2008; Paine et al., 2007) or by withholding and falsifying information (Metzger, 2007).

If the data requested by online organizations are assessed to be very sensitive, Internet users' perceptions of the risks involved in sharing personal information online would expectedly increase (Malhotra, Kim, & Agarwal, 2004), which could reduce their inclination to disclose them whenever requested (Castaneda & Montoro, 2007). Several studies have shown that Internet users are reluctant to disclose personally-identifiable information, such as their complete names or contact addresses (Acquisti & Grossklags, 2005; Metzger, 2006; Phelps, Nowak, & Ferrell, 2000), and financial information, such as income and credit card numbers (Metzger, 2006; Phelps, D'Souza, & Nowak, 2001; Phelps, Nowak, & Ferrell, 2000).

Requests for profiling information (e.g. age, weight, political affiliations) raised little concern among users since it could not be connected to their identities (Acquisti & Grossklags, 2005), while financial and personally-identifying information generate the greatest concern (Phelps, Nowak, & Ferrell, 2000). Perceptions of the risks involved in sharing personal data online might increase if data to be disclosed are appraised as too sensitive. The second research hypothesis is founded on the arguments just presented.

> *2. The sensitivity of personal data is positively related to perceptions of the risks involved in the disclosure of such data for e-government services.*

7.6 Internet experience and risk perceptions

Risk taking and perceptions of risks are not always entrenched on rationally-constructed criteria. In online environments, for instance, though the risks of engaging in computer-mediated transactions and exchanges inundate, users may still opt to engage in convenient but possibly risky transactions simply because they are used to doing it. For instance, Internet users with high levels of Internet experience may be inclined to do things online, despite their knowledge of the profusion of risks in computed-mediated transactions.

The relation between Internet users' level of Internet experience and their perceptions of the risks in online transactions is ambiguous. While results of one study indicated that users' experience with the Internet does not lead to low levels of risk perceptions (Corbitt, Thanasankit, & Yi, 2003), it is also suggested that perceptions of the risks, for instance in online commercial exchanges, can be attributed to their levels of Internet experience (Metzger, 2006).

The second assertion implies that people who possess high or low levels of web-proficiency are more likely to have high or low perceptions of the risks in using the web. For this study, it is postulated that a negative relationship exists between level of Internet experience and level of risks perception related to the disclosure of personal data for e-government services. Therefore, the third hypothesis is:

3. *High levels of Internet experience is negatively related to the perceptions of the risks involved in personal information disclosure for e-government services.*

7.7 Methodology

Data used to test the research hypotheses were collected through an Internet-based survey, which was administered for three months. In the first part of the survey, respondents were presented with a scenario of registering a child for an elementary school through a municipality's website. Although an online registration of children for basic schools is not yet implemented in the Netherlands, the scenario was selected as it is possible that such registration would be requiring the most amount of personal data from registrants - not just the usual contact information details, but demographic information as well (e.g. ethnicity, religion). Respondents were requested to complete the survey with the online registration scenario in mind.

The research instrument employed was divided into two. The first part solicited for respondents' demographic information and information on their Internet experience. The second part was designed to measure respondents' degree of trust in the municipality's ability and willingness to protect citizens' personal data, their assessment of the sensitivity of different data that could possibly be requested when registering a child for a basic school through the municipality's website, and their perceptions of the risks involved in an online disclosure of personal data.

Respondents for the survey were invited in two phases. In the first phase, a link to the online survey was sent to employees of two vocational schools in the Dutch region of Twente and to members of three environmental groups based in the province of Overijssel. In the second phase, customized postcards, which explained the nature of the study and included an invitation to participate in the said study, were sent to 900 residents of three towns (Enschede, Hengelo, and Almelo) in the Twente region.

A link to the online survey was also indicated on the postcards. A total of 1,152 invitations were sent out and 223 online filled out questionnaires were returned, resulting in a response rate of 19 percent. Fifteen returned questionnaires were eventually excluded since they were not completed. The remaining 208 questionnaires were used for analysis.

Of the 208 participants who completed the online survey, 109 (52%) were males. Respondents' age ranged from 18 to 82, with a mean of 47.5 (SD = 14.1). The average Internet experience measured in years among research respondents is 10.7 (SD = 4.2), with almost half (N = 88, 43%) of the respondents having Internet experience ranging from 10 to 13 years. Table 7.1 presents the complete demographic information of the survey participants.

Table 7.1. Demographic information of research respondents

Demographic characteristics		Freq.	%
Gender	Male	109	52
	Female	99	48
Age	younger than 30	28	14
	30 and under 50	84	40
	50 and under 65	75	36
	older than 65	21	10
Education	Low	133	64
	High	75	36
Internet experience	less than 2 years	4	2
	2 to 5 years	18	9
	6 to 9 years	47	22
	10 to 13 years	89	43
	14 years or more	50	24

7.8 Results

The 24 items comprising the survey instrument were subjected to principal component analysis using SPSS 16.0. The value of the Kaiser-Meyer Olkin Measure of Sampling Adequacy is pegged at .86, which is higher than the recommended value of .60 (Kaiser, 1974), while the Bartlett's Test of Sphericity X^2 (300) = 3395.32, $p < .001$ reveals that the correlations among the 24 items are sufficiently high for principal component analysis.

The six components also have *eigenvalues* above the Kaiser's criterion of 1 and explained 72 percent of the variance. Values below .40 were suppressed and, therefore, not included in the table. Shown in Table 7.2 are the factor loadings of the 24 items after rotation.

Table 7.2. Factor analysis with VARIMAX rotation of the items included in the online survey instrument.

Constructs	Item	Component					
		1	*2*	*3*	*4*	*5*	*6*
Trust in the municipality (ability to protect citizens' personal data)	The municipality uses appropriate security technologies to protect citizens' personal data.						.60
	The municipality possesses the expertise to ensure that citizens' personal data are safe from external intrusion.						.56
Trust in the municipality (willingness to protect citizens' personal data)	The municipality will not sell citizens' personal data to commercial organizations.		.79				
	The municipality will not share citizens' personal data to civic clubs and NGOs.		.80				
	The municipality will not transmit citizens' personal data to other government agencies.		.73				
	The municipality will not make citizens' personal data publicly accessible.		.79				
	The municipality will destroy citizens' personal data after they have been used.		.78				
Publicly accessible personal information	Name					.77	
	Postal address					.82	
	Telephone number					.76	
Demographic information	Age	.80					
	Ethnicity	.79					
	Gender	.83					
	Civil status	.84					
	Occupation	.73					
	Religion	.60					
Highly confidential personal information	Income			.77			
	E-mail address			.71			
	Health-related information			.81			
	Mobile phone number			.73			
Perceptions of the risks involved in sharing personal information online	I will most likely receive spam mails if I share my email address.				.77		
	The probability that I will receive marketing materials after sharing my personal data to the municipality is high.				.76		
	Third parties might access personal data that I will share to the municipality.				.75		
	Personal data that I will share to the municipality will be used for unknown purposes.				.81		

Attention should be given to the emergence of three components for 'sensitivity of personal data'. Name, postal address, and telephone number gravitate towards component 5, which resulted in their categorization as 'publicly accessible personal information'. Personal data such as gender, age, and religion comprised the category 'demographic information', while income, e-mail address, and health-related information clustered together to form 'highly confidential personal information'.

Results of the principal component analysis precipitated the three-fold differentiation of the second hypothesis:

(a) The sensitivity of publicly accessible contact data (e.g. name, telephone number) is positively related to perceptions of the risks involved in an online disclosure of such data for e-government services;

(b) The sensitivity of demographic data (e.g. age, gender, ethnicity) is positively related to perceptions of the risks involved in an online disclosure of such data for e-government services; and

(c) The sensitivity of highly confidential personal information (e.g. income, email address) is positively related to perceptions of the risks involved in an online disclosure of such data for e-government services.

The loadings validate the premise that different personal data are assessed differently in terms of their sensitivity. The clustering of two pieces of contact information (e-mail address and mobile phone number) with data such as income and health-related information, and not with postal address and telephone address, is a strong indication of how respondents felt about the sensitivity of e-mail addresses and mobile numbers, which are somehow regarded riskier to disclose than telephone numbers and postal addresses. Table 7.3 shows how the sensitivity of the 13 types of personal data were accessed by the research respondents on a five-point Likert scale, with 1 representing 'very sensitive' and 5 for 'not very sensitive'.

A reliability analysis was performed to test the internal consistency of the all the constructs by computing their Cronbach's alpha scores. All the constructs have Cronbach's alpha scores above .70, which indicates acceptable reliability (DeVellis, 2003). Table 7.3 also presents the reliability scores of the different constructs and the mean and standard deviation values for the different items measuring the constructs

Table 7.3. Alpha scores, mean and standard deviation values of the variables of the study (n = 208)

Research constructs with their respective items	Mean	Std. Dev.
Trust in the municipality in terms of its ability to protect citizens' personal data (*a* = .73) *5 – Strongly Agree / 1 – Strongly Disagree*		
The municipality uses appropriate technologies to protect citizens' personal data.	3.15	.69
The municipality possesses the expertise to ensure that citizens' personal data are safe from intrusion.	3.13	.78
Trust in the municipality in terms of its willingness to protect citizens' personal data (*a* = .85) *5 – Strongly Agree / 1 – Strongly Disagree*		
The municipality will not sell citizens' personal data to commercial organizations.	3.76	.83
The municipality will not share citizens' personal data to civic clubs and non-government organizations.	3.59	.89
The municipality will not transmit citizens' personal data to other government agencies.	2.90	1.01
The municipality will not make citizens' personal data publicly accessible.	3.72	.87
The municipality will destroy citizens' personal data after they have been used.	3.02	.93
Sensitivity of personal data : Publicly accessible personal information (*a* = .88) *1 – Very Sensitive / 5 – Not Very Sensitive*		
Name	3.73	1.08
Postal address	3.80	1.01
Telephone number	3.29	1.18
Sensitivity of personal data : Demographic information (*a* = .90) *1 – Very Sensitive / 5 – Not Very Sensitive*		
Age	3.88	.95
Ethnicity	3.45	1.20
Gender	3.99	.80
Civil status	3.88	.88
Occupation	3.60	1.02
Religion	3.11	1.25
Sensitivity of personal data : Highly confidential personal information (*a* = .85) *1 – Very Sensitive / 5 – Not Very Sensitive*		
Income	2.45	1.11
E-mail address	2.88	1.22
Health-related information	2.28	1.11
Mobile phone number	2.63	1.18
Perceptions of the risks involved in sharing personal information online (*a* = .83) *5 – Strongly Agree / 1 – Strongly Disagree*		
I will most likely receive spam mails if I share my email address.	3.01	.98
The probability that I will receive marketing materials after sharing my personal data to the municipality is high.	2.87	1.00
Third parties might access personal data that I will share to the municipality.	2.95	.96
Personal data that I will share to the municipality will be used for unknown purposes.	2.57	.94

Multiple regression analysis was performed to test the research hypotheses. The simultaneous entrance of trust, personal data sensitivity, and Internet experience as predictor variables and of risk perceptions as an outcome variable resulted in an R^2 value of .29, which signifies that 29% of the variance for the perceptions of the risks involved in the disclosure of personal data for e-government services can be explained by the predictor variables mentioned.

Variance, however, is most explained by users' level of trust in the municipality's ability to protect citizens' personal data (b = -.32, p < .001), users' assessment of the sensitivity of highly confidential personal information (b = .19, p < .01), and the assessed sensitivity of publicly accessible contact information (b = .18, p < .05). Table 7.4 shows both the unstandardized and the standardized coefficients of the different variables hypothesized to influence users' level of risk perceptions.

Table 7.4. Coefficients of the variables hypothesized to influence level of risk perceptions

	B	SE B	B
• Constant	3.69	.42	
• Level of trust in the municipality in terms of its ***ability*** to protect citizens' personal data	-.39	.08	.32 ***
• Level of trust in the municipality in terms of its ***willingness*** to protect citizens' personal data	-.12	.07	-.11
• Assessment of data sensitivity – publicly accessible contact data	.14	.06	.18 *
• Assessment of data sensitivity – demographic data	-.03	.08	.00
• Assessment of data sensitivity – highly confidential data	.16	.06	.19 **
• Level of Internet experience	-.01	.01	-.05

*p < .001 ***, p < .01 **, p < .05 **

These results indicate that respondents' level of trust in the ability of the municipality to protect citizens' personal data disclosed online is negatively related to their perceptions of the risks involved in an online disclosure of citizens' personal data. Thus, Hypothesis IA is supported. It is evident that respondents' lack of trust in the municipality's ability or competence to protect citizens' personal data can increase perceptions of the risks involved in an online disclosure of personal data, just as high levels of trust in the municipality's ability to protect citizens' personal data may also result in the reduction of risk perceptions.

Hypotheses 2A and 2C are also statistically supported, indicating that respondents' assessment of the sensitivity of their publicly accessible contact information (name, postal address, telephone number) and highly confidential personal information (income, health-related information, mobile phone number, and e-mail address) can influence risk perceptions. Requests for data deemed sensitive and confidential may spur increased perceptions of the risks involved in sharing personal information online, even to a government organization.

As results of the regression analysis did not indicate that respondents' level of trust in the municipality's willingness to protect citizens' personal data, respondents' assessment of the sensitivity of demographic data, and respondents' levels of Internet experience could statistically influence risk perceptions, Hypotheses 1B, 2B, and 3 have to be rejected.

7.9 Discussion

Apprehensions regarding an online disclosure of personal data for online exchanges are understandable considering the relatively high possibility for online organizations to use their clients' personal data for commercial purposes. In this study, respondents claimed that they trust that the municipality, a non-commercial entity, will protect their personal data by not selling them to commercial organizations and not making them publicly accessible through online or offline channels. They somehow did not agree that their personal data will not be shared to other government agencies or will be destroyed after being used for a particular purpose.

As survey respondents generally appeared to trust the municipality in terms of its willingness to protect citizens' personal data, it could be expected that respondents will have low perceptions of the risks involved in sharing personal information to engage in a hypothetical case of registering a child for a basic school through a municipality's website. The finding that users' lack of trust in the municipality's ability to protect citizens' personal data generates risk perceptions is an indication that whenever users are uncertain about whether or not appropriate technologies are employed to protect their data they will be pushed to believe that disclosing personal data is risky, as data could be vulnerable to third-party abuse.

With the risks of having Internet users' contact information exploited for commercial purposes (disclosing emails may result in annoying spam mails or sharing mobile numbers could lead into disturbing marketing calls), it is not surprising that Internet users would consider contact information such as e-mail addresses and mobile phone numbers as very sensitive data. However, the finding that mobile numbers are assessed as more sensitive than telephone numbers is indicative of how respondents felt about the former. While people's telephone numbers are readily accessible by just consulting a telephone book, mobile phone numbers are somehow private that they can only be known if their owners volunteer to share them.

The results of the research lend credence to the premise that the disclosure of personal data considered highly sensitive is sure to attract risk perceptions ranging from the apprehension that sharing one's e-mail address could trigger an onslaught of spam mails to the fear that personal data disclosed online are easy prey for unauthorized third parties intending to exploit them for reasons unknown. As pieces of demographic information are not estimated to be too sensitive, they could not be expected to augment risk perceptions, unless perhaps somewhat sensitive demographic information such as religion and ethnic background would be tied to the individual and be used for some kind of profiling that might have negative consequences for the person concerned.

Results of various studies on the relation between Internet experience and risk perception yielded incongruent conclusions. While one

study concluded that users' Internet experience does not result in a reduction of risk perceptions, another investigation indicated that more experienced Internet users are most likely to have lowered risk perceptions. Results of this online survey, however, did not confirm either of the two, signifying that respondents' levels of Internet experience do not influence either the lowering of users' risks perceptions or the magnification of such perceptions.

7.10 Implications and recommendations

A significant finding from this study is that lack of trust in a government organization's ability (or in the municipality's ability, as used in the hypothetical situation for the survey) to protect citizens' personal data could increase perceptions of the risks involved in online disclosures of personal data. It is also known that respondents are not even sure whether or not a particular municipality (the one they had in mind while completing the survey) uses appropriate technologies and has the knowledge or expertise to protect citizens' personal data. This could serve as a whistle blow for government organizations to highlight their competence to protect whatever personal data they collect from citizens.

Whenever highly sensitive data are collected, Internet users must also be assured that they will be protected using appropriate technologies and techniques to prevent unauthorized third-party access. As indicated earlier, respondents agreed that the municipality will not share their personal data to commercial organizations, although they did not believe that such data will not be shared to other government agencies.

When government organizations see the need to share citizens' personal data to other government agencies, citizens must be adequately informed of the reasons for the disclosure. By informing citizens that their personal data will be disclosed to other government agencies for legally-accepted purposes, they are significantly provided with the rights of choice and consent, which would eventually provide them with some degree of control over their personal data (Tavani, 2007; Tavani & Moor, 2001).

Respondents also did not also agree that their personal data will be destroyed after they have been used for a designated purpose. This fuels concerns that unnecessary and long-term storage of personal data could be abused either by the collecting agency or by third parties, which may even discourage users from disclosing personal data. Therefore, users should be assured that whatever data they will share online will be removed or destroyed after such data have been used for a particular purpose. Such an assurance could be emphasized either in an online privacy statement or on the page of the government website used as an online form to collect data from citizens.

In one study on the assurances of privacy statements posted on Dutch municipal websites, it is revealed that only 10 percent of the analyzed privacy statements contained any assurance that users' personal

data would be destroyed after usage (Beldad, De Jong, & Steehouder, 2009). This figure is rather dismal considering that Article 10 (1) of the Personal Data Protection Act of the Netherlands states that 'personal data should not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or processed subsequently', except (Article 10:2) when 'data are used for historical, statistical, or scientific purposes'.

Although a number of empirical studies have already investigated the determinants of risk perceptions in online transactions, mostly within the context of electronic commerce, they are somehow constrained by their narrowed view of the factors that contribute to the germination of users' risk perceptions. While trust is found to be negatively related to risk perceptions (Grazioli & Jarvenpaa, 2000; Kim, Ferrin, & Rao, 2008; Kim & Kim, 2005; Pavlou, 2003), other factors that may fuel risk perceptions have not been looked into.

Whereas perceptions of the risks in commercial online transactions are relatively higher than those in non-commercial online transactions, specifically within electronic government, risk perceptions in the latter may significantly impact users' disinclination to avail online services offered by non-commercial institutions such as government organizations. Belanger and Carter's (2008) study on trust and risk situates the former as a determinant of the latter, but their definition of the risk construct fails to distinguish the various types of risks that a user would possibly confront when transacting with a government organization electronically. This study specifically focused on the perceived risks involved in an online disclosure of personal data for a hypothetical transaction with a government organization.

Although a number of possible risks involved in an online disclosure of personal data have already been identified for this study, there is still a need to further explore the risks that people associate with a decision to share personal data to complete a transaction with a government organization. Considering the apparent difference in trusting an organization in terms of its ability and its willingness to protect Internet users' personal data, it should also be worthwhile to see how users' trust in organizational ability or competence to protect Internet users' personal data influences users' level of perceived risks concerning the security of their data and to investigate the impact of users' trust in organizational willingness to protect personal data on users' risk perceptions concerning potential abuse of such data by the organization collecting them.

While trust (specifically in the ability of a government organization to protect citizens' personal data) and the appraised sensitivity of personal data that will be supplied for an e-government service have been found to shape risk perceptions negatively and positively, respectively, other possible factors that could contribute to risk perceptions related to an online sharing of personal data should be explored. Internet user-based variables such as the level of privacy concerns may also play a role in the formation of risk perceptions. For instance, 'privacy fundamentalists' might be more

likely to overestimate the risks involved in sharing personal information in the digital environment than those who are not so concerned about their information privacy.

The study's dependence on Dutch respondents and its relatively small sample size limit the generalizability of the findings. The results may give a sketchy picture of risk perceptions among Dutch Internet users, but these would hardly be illustrative of how citizens from the neighboring countries of the Netherlands, for instance, would perceive the risks in sharing personal information for online transactions with government organizations. Future research could even consider looking into the effects of culture on trust in e-government and the risks involved in sharing personal information online. The issue with the sample size could be addressed by pursuing a similar research with a larger sample.

7.11 Conclusion

As government organizations are increasingly channeling their services through the Internet, efforts of extending a 24-7 online service delivery system is bound either to be enthusiastically accepted or eagerly avoided. With personal data as currencies for most government online transactions, Internet users' concerns regarding the protection, processing, and further usage of their personal data are inestimable. These concerns could eventually morph into risk perceptions, which might lower users' intention to transact with any government organization online – especially when a transaction necessitates the sharing of personal data.

What this study reveals is that although users trust that a government organization will not exploit their personal data for profit, they are uncertain about whether or not a government organization has the ability to protect citizens' personal data, especially those that are considered sensitive and probably risky to disclose. Reducing users' perceptions of the risks in sharing personal data online, therefore, should prompt organizations to fortify their reputation as trustworthy entities armed with the necessary expertise and technology to safeguard their users' personal data, especially those regarded too sensitive, from unwarranted intrusions.

8

When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites

Confidence in privacy statements on government websites, as emphasized in Chapter 5, helps in enhancing Dutch Internet users' trust in government organizations in terms of their usage and processing of citizens' personal data. Online privacy statements, whether or not they are read, are regarded important trustworthiness cues. However, online privacy statements are more than cues. They are the only sources of information for Internet users to be sufficiently informed of organizational usage, processing, and protection of their personal data.

This chapter presents the results of a study that analyzed the contents of privacy statements on Dutch municipal websites. The analysis focused on the guarantees contained in the aforementioned online documents and on their conformity with the important points of the Dutch law on information privacy protection. The availability and the findability of privacy statements on municipal websites were also surveyed.

Three important findings resulted from this study. First, not all municipal websites bother to post privacy statements on their websites. Second, most municipalities do not ensure that their online privacy statements are findable. Third, privacy statements on Dutch municipal websites emphasize diverging assurances and promises – with some privacy policies containing all the important provisions of the WBP, and others offering only general, and sometimes rather vague, guarantees.

This chapter is based on a manuscript by Beldad, A., De Jong, M., & Steehouder, M. (2009), which has been published in Government Information Quarterly, 26(4), 559-566.

8.1 Introduction

Two uncertainties exist in online transactions: the risk of losing one's money during the exchange and the threat of having one's private sphere penetrated. Although the first risk suffices to discourage some clients from engaging in an online exchange, the possibility of having the privacy of their personal data compromised contributes substantially to clients' disinclination to embark on online transactions. (Miyazaki & Fernandez, 2001).

The complexity in the collection and dissemination of data over the internet (Milne, Rohm & Bahl, 2004) spawns a spectrum of privacy concerns that are far from negligible: the bombardment of the clients' mailbox with spam emails, the placement of cookies on the clients' computer to track their internet usage history and preferences, the application of malicious technologies enabling third parties to access clients' personal files, and the inability of clients to control the usage and processing of their personal information disclosed to an online organization (Wang, Lee & Wang, 1998). What is even worse is the possibility of identity theft as a consequence of the mishandling of personal data by whoever is collecting it (Fernback & Papacharissi, 2007).

Efforts to win clients' trust somehow necessary for an engagement in various exchanges with online organizations include the posting of the privacy statements on the organizations' websites (Pan & Zinkhan, 2006). Clients assess the trustworthiness of online organizations based on the presence of privacy protection guarantees (Aiken & Bausch, 2006; Arcand, Nantel, Arles-Dufour & Vincent, 2007; Earp & Baumer, 2003; Liu, Marchewka, Lu & Yu, 2005), even if the privacy statement would not be read thoroughly (Vu, Chambers, Garcia, Creekmur, Sulaitis, Nelson, Pierce & Proctor, 2007) or even consulted (Jensen, Potts & Jensen, 2005; Arcand et al., 2007). However, one criticism regarding an organization's promise to protect the personal information of its clients is that it is purely tactical—fortifying commercial advantage or eluding legal penalties—rather than ethical since pursuing the protection of collected personal data from clients is just the right thing to do (Markel, 2005).

As personal data are becoming valued commodities (Franzak, Pitta & Fritsche, 2001; Olivero & Lunt, 2004; Turner & Dasgupta, 2003), one can never be assured that they will stay untouchable inside a confidentiality chest since they are also susceptible to exploitation for a cornucopia of purposes by those who collect and store them. The notion that data can be effortlessly recycled for unknown purposes, which could jeopardize clients' online privacy rights, only exacerbates clients' reluctance to provide personally-identifiable information, which could spur them to drop their plans of engaging in online exchanges. However, in some cases, the convenience of online transaction trumps privacy concerns, especially when the benefits of an electronic exchange outweigh the value of privacy (Woo, 2006).

For this study, the contents of privacy statements on Dutch municipal websites were analyzed and categorized. The assurances and notifications of those statements were also scrutinized using the provisions of *Wet Bescherming Persoonsgegevens* (WBP) or the Personal Data Protection Act of the Netherlands. This law implements Directives 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data). The study also looked into the ease of finding the privacy statements on the websites of municipalities—considering that not only the availability of a privacy statement but also its findability should be taken into account when appraising an online organization's compliance with OECD's (2002) 'notice principle' of fair information practices.

8.2 Online privacy as a matter of control and restricted access

Although the association of privacy with control is prominent in the writings of both Westin (1967, 2003) and Fried (1984), Moor (1997) argued that control alone does not guarantee the protection of one's online privacy. Personal data, once digitized, slide rapidly through computer systems around the world. His control/restricted access conception of privacy signifies that different people (or organizations) should be given different levels of access to different types of personal information at different times (Moor, 1997). Tavani and Moor (2001) advanced that control of information does not suffice to conceptualize the right to privacy. Instead, the right to privacy is better understood in terms of the theory of restricted access.

Assuming centrality in that theory is the need to create privacy zones to protect people's privacy, especially when they lack control over information about themselves. It is emphasized that in managing one's privacy, one does not need absolute control over information about oneself. Some degree of control can already be achieved through choice, consent, and correction.

Managing one's privacy through choice, as an aspect of limited control, involves prudency in defining the flow of one's personal information and determining the level of access other parties have to that same information; whereas consent, as an element of limited control, implies that people waive their right to privacy and provide others with access to their information. The management of one's privacy is incomplete if the person concerned is not provided with access to his or her data and the opportunity to correct them if necessary (Tavani & Moor, 2001).

8.3 Privacy statements - defensive or protective?

Even if clients do not bother to read or consult online privacy statements (Arcand et al., 2007; Jensen et al., 2005; Vu et al., 2007), online

organizations still resort to the posting of privacy statements on their websites to placate clients who are anxious about providing their personal data for the transaction (Fernback & Papacharissi, 2007). Empirical studies showed that clients use the presence of an online privacy statement as one criterion in assessing the trustworthiness of an online organization (Aiken & Bausch, 2006; Arcand et al., 2007; Earp & Baumer, 2003; Liu et al., 2005). Privacy statements provide clients with the necessary information about the organization's information practices (Milne & Culnan, 2004). By emphasizing the benefits of disclosure, organizations may even use their privacy statements to convince their clients to disclose personal information necessary for the completion of a transaction (LaRose & Rifon, 2006).

However, an analysis of 97 privacy statements revealed that they do not guarantee the protection of personal information, but instead serve as legal safeguards for the company by specifying the usage of collected information. A majority of online organizations used privacy statements to make vague promises of how personally-identifiable information would be protected and to assert their right to collect and trade non-personally-identifiable data. (Papacharissi & Fernback, 2005).

Pollach's (2005) first study, an analysis of communicative strategies in privacy statements, showed that organizations resort to both rational and emotional appeals in the construction of more credible arguments to persuade clients that their personal data would be responsibly handled. The findings of Pollach's (2007) second study suggested that privacy statements are motivated more by efforts to avoid potential lawsuits than by the obligation to uphold the principles of fair information practice.

One study (Earp, Anton, Aiman-Smith & Stufflebeam, 2005) disclosed the apparent conflict between the guarantees of organizational privacy statements and what their clients' expect to be emphasized in those statements. The study found that privacy statements emphasized the security and protection of collected data, procedures of data collection (direct or indirect), and the choice for clients to determine the types of information about them that can be processed and used by the organization. However, clients were most concerned about the transfer of data by the organization (whether the data would be shared, rented, or sold), about the usage of their information by the organization, and about how disclosed data will be stored by the organization. These findings extended full support to the results of another study (Phelps, Nowak & Ferrell, 2000)—that clients would like more information about how organizations use their personal information.

The demand for further information on the usage of collected personal data is an indication that clients do not trust that online organizations will stick to what they are guaranteeing in their privacy statements. This lack of trust springs from clients' belief that online organizations do not share their values about information privacy in the online environment (Hoffman, Novak & Peralta, 1999).

8.4 Legal protection of online privacy in the European Union and in the Netherlands

With the ease in the collection and transmission of data as a result of the advances in technology, the European Union saw the urgency of implementing legislation that would protect European citizens' right to privacy, especially regarding the processing of their personal data. Brey (2007) argued that privacy protection in Western nations subscribes to the principle of informed consent: citizens should be informed about how organizations will store, use, and exchange citizens' personal data; and citizens' consent should be asked whenever their data will be exchanged.

Enacted in 1995 and effective in 1998, Directive 95/46/EC, substantiating the effort to regulate and institutionalize data protection, is founded on the perspective that the government should assume an important role in protecting its constituents from social harm (Strauss & Rogerson, 2002) and is a strong manifestation of the European view that the privacy of personal information is a fundamental human right that merits legal protection (Markel, 2006). Since Directive 95/46/EC is broadly applicable to privacy practices in general, Directive 2002/ 58/EC was adopted in 2002 to extend further protection for internet users (Baumer, Earp & Poindexter, 2004).

Directive 95/46/EC clearly states that EU member states should protect the fundamental rights and freedoms of natural persons (identified or identifiable natural persons), in particular their right to privacy with respect to the processing of their personal data (European Union, 1995 a, b). Bergkamp (2002) argued that, unlike the selective U.S. legislative approach, the European Commission laws impose onerous sets of requirements on all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer.

Elgesem (1999) asserted that two ideals surfaced from Directive 95/46/EC: the ideal of predictability and the ideal of justifiability. The ideal of predictability concerns data subjects' ability to form reasonable expectations on how their personal data will be processed, which is grounded on the Directive's provisions on data quality and security. The ideal of justifiability pertains to questions about the justifications of the different kinds of data processing.

Directive 2002/58/EC furthers the EU's determination to uphold the internet users' right to privacy. An important stipulation in that directive is the provision on the necessity on the part of the organization to inform users' about the usage of cookies and the right of the users to refuse cookies (European Union, 2002).

Cookies pose a potential harm in the sense that collected information from the users' computers through cookies may be used by the organization or company in so many ways that could have unpleasant consequences for the users (Debussere, 2005). Cookies can be used for potentially unethical procedures such as linking online behavior to

personally-identifiable information and reselling this information without the user's consent (Kierkegaard, 2005).

In the Netherlands, Directive 95/46/EC is implemented through the *Wet Bescherming Persoonsgegevens* (Personal Data Protection Act), which was enacted on September 1, 2001. WBP replaced the old *Wet Persoonsregistraties*, which dated from December 28, 1988 (European Commission, 2008). Borking and Raab (2001) presented a summary of significant points concerning the Wet Bescherming Persoonsgegevens (WBP):

1. Reporting the processing—the Data Protection Board or a privacy officer must be informed of the processing of personal data.
2. Transparent processing—the person concerned must be notified of the identity of the data processor and the purpose(s) of the processing.
3. 'As required' processing—the collection of personal data must be founded on specific, explicit, and legitimate purposes and data should not be processed in ways incompatible with the specified purposes.
4. Lawful basis for the data processing—the processing of personal data must be grounded on provisions contained in WBP, such as permission, agreement, legal obligation, and justified interest. Processing of special categories of data, such as racial/ethnic information and health information, have stringent rules.
5. Data quality—the correctness and accuracy of personal data is important. Personal data should be sufficient, to-the-point, and not excessive.
6. Rights of parties involved—parties involved have the right to check and correct their data and they also have the right to raise objections.
7. Data traffic with countries outside the EU—the transfer of personal data to a non-EU country is permitted only if adequate protections are offered in that country.
8. Processing personal data by a processor—a data processor should observe the instructions of the data controller if the processing is outsourced to the processor.
9. Protection against loss and unlawful processing of personal data—lawful data processing requires the use of appropriate security measures to ensure the protection of personal data.

8.5 Research questions

Text and content analyses had been carried out to scrutinize the contents of privacy statements on U.S. based-commercial websites (Earp et al., 2005; ; Fernback & Papacharissi, 2007; Markel, 2005; Papacharissi & Fernback, 2005; Pollach, 2005, 2007; Schwaig, Kane & Storey, 2006). These

analyses aimed at either exposing the flaws in the statements or assessing their compliance or non-compliance to the principles of fair information practice. While it is evident that previous studies have concentrated on the dissection of the privacy statements of commercial websites, the privacy statements of non-commercial organizations—such as those on the websites of government agencies—have been spared from enquiry.

However, the absence of a comprehensive online information privacy protection law in the U.S. makes it impossible to check whether online privacy policies conform to the provisions of a privacy law. The case is different in any EU member state where EU Directives on privacy protection are implemented through the privacy laws in member states. This study aims at dissecting the contents of the privacy policies on municipal websites and at determining whether or not the contents of privacy statements on Dutch municipal websites coincide with the important provisions in the *Wet Bescherming Persoonsgegevens*.

In the United States, for instance, it has been cited that the emphasis of most online privacy statements often clash with what clients expect to read in privacy statements (Earp et al., 2005), which corroborated the claim that online organizations do not share the clients' value about information privacy in the online environment (Hoffman et al., 1999). According to a study by Earp et al. (2005), online privacy statements often underscore the application of security measures and the methods for the collection of data, whereas clients would like to have more information about the further usage and the storage of their personal information.

Schwaig et al. (2006) also cited that organizations focus their efforts on different aspects of fair information practice (notice, access, choice, security, enforcement) and they follow diverging approaches in the selection of the privacy protections they extend to their clients. The differences in the content, structure, and focus of online privacies on commercial websites resulted in an interest to study the content and focus of privacy statements on government websites, which prompted the first research question.

(1) *What are the guarantees contained in the privacy statements on Dutch municipal websites?*

The publication of a privacy statement on the organization's website is already a standard practice and is used either as a trust building mechanism (Araujo, 2005) or as a legal safeguard (Fernback & Papacharissi, 2007). However, the presence of such a statement is not a guarantee that the organization will conform to whatever it says in its privacy statement (Earp et al., 2005; Markel, 2005) or that the privacy statement corresponds to the tenets of fair information practice (Schwaig et al., 2006).

The failure of an online organization to provide its clients with any information about its privacy statements is tantamount to depriving them of the information necessary for them to act autonomously (Markel, 2005) and an indication of that organization's inability to observe 'notice'— the

first principle of fair information practices (Schwaig et al., 2006). When people want to know whether a website has a privacy statement or not, they must first deal with the task of finding it. And this brought us to pose our second question:

> (2) *How easy (or difficult) is it to find the privacy statements on Dutch municipal websites?*

The second question of this study is not centered on the availability of a privacy statement on a government website but on the findability of the aforementioned statement on a website. For this study, the findability of the privacy policy is defined in terms of the ease of locating the statement within the website—whether it is located on the main page or hidden somewhere within the website and whether or not it is labeled.

8.6 Methodology

Privacy statements used for this study were obtained from 100 municipal websites (specifically, the websites of the first 100 municipalities ranked according to their population size). The decision to select the first 100 municipalities, starting from the most populated, was founded on the premise that bigger municipalities (in terms of population size) would be conscientious in providing their users with the option to know how their personal data will be used and protected, although it should not be interpreted that small municipalities are not concerned about the online information privacy of their users.

An initial survey of the contents of privacy statements on 30 Dutch municipal websites (not included in the sample) allowed for the creation of a code book classifying the different assurances and notifications contained in the privacy statements. The code book was then used to survey the contents of the first half of the sample, which, in order to accommodate new items that were not found in the initial survey, also necessitated the constant revision of the code book. The second half of the sample was then analyzed using the revised code book, which was also subjected to a second revision.

The entire sample of 77 privacy statements (out of 100 websites) was then re-analyzed using the expanded code book. Two raters were tasked to code the different parts of the selected privacy policies. The first rater coded the different parts of the entire sample of privacy statements (n=77), while the second rater worked independently with 40 percent of the sample (n=31). Inter-rater agreement was pegged at 84 percent. Disagreements in the analyses were settled through a discussion between the raters.

8.7 Results

8.7.1. What do privacy policies promise?

8.7.1.1 Catching the clients' trust right at the start

In the construction of online privacy statements, organizations seem to be capitalizing on the impact of the 'first paragraph', as rhetorical strategies are prominently employed in the introductory part to temper users' anxiety of having their privacy zones invaded after their decision to share personal data. The majority of the privacy statements of municipal websites (n=53 of 77; 69%) commenced with an assurance that the municipality respects and values the privacy of its users.

This first overarching guarantee is further strengthened by a supporting promise that collected personal information from users will be handled confidentially and with utmost care, with 32 (42%) online privacy statements containing this guarantee. The strategic positioning of the aforementioned broader promises appears to confirm the findings of an experiment (Vu et al., 2007) that readers paid particular attention to the first sentences of a privacy statement, aside from the first few words of each paragraph. Thus, an online organization must, right at the start, capture the trust of clients for the organization's commitment to protect privacy, before clients decide to discontinue reading the rest of the policy. Table 8.1 shows four overarching guarantees that can be found in the privacy statements on municipal websites.

Table 8.1. Overarching guarantees in the privacy policies of municipal and commercial websites.

Statements of guarantees and/or notifications	n=77
Respect for the users' privacy and the confidentiality of their personal information	53 (69%)
Assurance that collected personal information from the users will be handled confidentially and treated with care	32 (42%)
The collection, processing, and usage of personal information are in accordance with existing legislations on information privacy protection	36 (47%)
The organization's procedures for the collection and usage of users' personal data have been reported to a government agency tasked to oversee the processing of data by organizations	3 (4%)

8.7.1.2 Notification of the purposes for personal data collection

Wet Bescherming Persoonsgegevens (WBP) or the Personal Data Protection Act stipulates that the collection of personal data should be performed in accordance with the law and in an appropriate and careful manner (Article 6) and founded on specified, explicit, and legitimate purposes (Article 7). Online organizations, therefore, are expected to spell out their rationales for collecting personal data from their clients.

Fifty privacy statements from municipal websites stated the purposes for the collection of personal information, but only 39 of the 50 (78%) indicated that collected personal data will only be used for the purposes they were collected for. This guarantee is in accordance with Article 9 of the Personal Data Protection Act, which states that personal data should not be further processed in a way incompatible with the purposes for which they have been obtained. Additional points related to the notification of purposes for data collection are shown in Table 8.2.

Table 8.2. Additional assurances and notifications related to the collection of personal data.

Statements of guarantees and/or notifications	50 collected personal information
Only voluntarily disclosed personal information will be processed and used	8 (16%)
Notification of the types of personal information that will be collected from the user	3 (6%)

8.7.1.3 On the collection of data related to website visit

Thirty percent (n = 23 of 77; 30%) of the municipal websites emphasized in their privacy statements that users do not have to supply personal information when visiting the website, therefore implying that clients can visit the website anonymously, for instance to search for information without having to disclose personal data. However, the privilege of an anonymous visit is revoked when users decide to place a request for a document (for instance a driver's license) through the municipal website. Such a request necessitates the disclosure of personally-identifiable information such as the user's complete name, physical address, telephone number, and e-mail address.

Privacy statements on municipal websites (n = 51 of 77; 68%) apportioned a section to articulate their purpose/s for the collection of information concerning users' visit to the website such as the time of visit to the website, the most visited pages, the frequency of visit, and the IP address. Those that register data related to website visit, such as the IP address, emphasized that the collection of such data will only be used for technical supports and statistical purposes and will not be exploited to identify the individual user.

However, one piece of data related to the users' visit to a municipal website is rather controversial. According to the Dutch Data Protection Act Guidelines (2007), an IP address is classified as a piece of personal data since an internet service provider can easily trace this information to the originating person—the internet subscription customer— and it does not matter whether or not the organization collecting the IP address will be using it to identify the user. In fact, one municipal website cited that in certain circumstances, for instance in criminal cases, the service provider

can be requested to reveal relevant information about an IP address, which could eventually link to an individual.

8.7.1.4 On the collection of special personal data

Articles 16 to 24 of the Personal Data Protection Act specify prohibitions on the processing of special personal data such as those that pertain to the users' religion, philosophy, race, political persuasion, health and/or sexual life, as well as data concerning trade union membership, criminal behavior, or unlawful or objectionable conduct. The articles also identify cases for which prohibitions on the collection of special personal data are not applicable.

One municipal website (1%) guaranteed that it will not collect special personal data from its users. The absence of such a guarantee in 99 percent of the analyzed privacy statements could be attributed to the fact that municipal websites only ask for contact information such as the user's name, physical address, telephone number, and e-mail address when the user decides to request a document or apply for a particular service through the municipal website.

8.7.1.5 On personal data processing and usage

A fraction of municipal websites (n = 2 of 77; 3%) explicitly guaranteed that users' consent will be requested whenever their personal information will be processed. In an effort to placate users' concerns over the torrent of spam mails in their mail boxes, one municipal website promised that it will not send spam mails to its users. Such a promise is relevant, especially when municipal websites are requesting their users' e-mail addresses.

8.7.1.6 On the disclosure of personal data to third parties

Article 41 (3) of the Personal Data Protection Act states that responsible parties who are planning to provide personal data to third parties should take appropriate steps to notify users of the option they have to object to the disclosure of their data to third parties. The recognition of personal data as valued commodities (Olivero & Lunt, 2004) and the potential for abuse of disclosed data shape users' concern that whatever data they will disclose to an organization might be traded with other commercial entities or could be used for purposes that could have damaging consequences for them.

Such anxiety could result in their unwillingness to divulge the necessary personal data. To counter such apprehension, municipal websites have resorted to the deployment of two common rhetorical strategies: an assurance that personal data will not be relayed to third parties (n = 8, 10%) and an assurance that they will not be rented or sold (n = 1, 1%).

Only 3 percent (n = 2 of 77) of the municipal websites selected for this study indicated in their privacy statements the conditions for the possibility of disclosing their users' personal information to third parties. The rationale for indicating that there is the possibility of data disclosure to third parties is anchored on the municipality's obligation to supply the police and other government agencies with users' data when necessary.

Table 8.3. Three additional notifications concerning the disclosure of personal data to third parties.

Statements of guarantees and/or notifications	3 disclosed personal information
Notification of the users' right to object to the disclosure of data to third parties	2 (67%)
Notification of the types of thirds parties to whom personal data will be disclosed	1 (33%)

8.7.1.7 Storage and retention of collected personal data

Of the 50 municipal websites that collected personal data from their users, only five (10%) stressed in their privacy statements that collected information will be stored in the organization's database. Article 10 (1) of the Personal Data Protection Act states that personal data should not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or processed subsequently, except (Article 10:2) when data are used for historical, statistical, or scientific purposes.

In accordance with Article 10 (1), 15 (30%) privacy statements emphasized that data will be destroyed after usage. However, this still leaves the fate of the data collected by 30 municipalities unknown since nothing is said about what will happen to them after they have been used for the purpose(s) for which they have been obtained.

8.7.1.8 Users' right of access to their personal data

One of the essential principles of fair information practices is the provision of access that enables users to review, rectify, or remove whatever data they have disclosed to an online organization. This principle is significantly accommodated in Article 36 of the Personal Data Protection Act.

Only two of the 10 (20%) municipal websites that store their users' personal data on a database cited in their privacy statements that users have the right to check and rectify information collected from them. The inclusion of a guarantee that collected data will be destroyed after they have been used for the purpose(s) for which they have been collected might explain why the provision on the right of access is not so popular in most privacy statements.

8.7.1.9 Security of personal data

The Personal Data Protection Act obliges online organizations to implement appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing (Article 13). This study shows that 20 percent (n = 10 of 50) of the municipal websites that collected personal data from their users emphasized in their privacy statements that collected personal data are assured of protection as security technologies, such as the secure socket layer (SSL) protocol, are utilized.

8.7.1.10 Notification of the usage of cookies

According to Article 2 (1), the Personal Data Protection Act applies to fully or partly automated processing of personal data and to the non-automated processing of personal data entered in a file or intended to be entered therein. This corresponds to Article 11 of Directive 95/46/EC, which states that whenever data are not directly obtained from the data subject, the data controller must inform the data subject of the data collection at the time of recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are disclosed.

Kierkegaard (2005) underscored that even if the issue of cookies is not specifically mentioned, almost all aspects and features of the cookie concept can be used to violate the Directive's principles on access restriction and user transparency (European Union, 2002). Directive 2002/58/EC, however, contains a provision that concerns the usage of cookies. According to Article 5(3) of the Directive 2002/ 58/EC:

> *The use of electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with a clear and comprehensive information in accordance with Directive 95/46 EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.*

Two important legal requirements are underscored in this provision: a notification of the purpose of the processing and a notification of the users' right to object to such processing. In the analysis of paragraphs that contain information on the usage of cookies, the two legal requirements noted above correspond to (a) the notification of the purpose(s) of cookies, and (b) the notification of the users' right to refuse the usage of cookies. In accordance with the recommendation of the Article 29 Working Party with regards to the online collection of data, an online privacy statement should include information regarding the automatic data collection procedures, such as the use of cookies (Dutch Data Protection Act Guidelines, 2007).

Twelve out of 77 (16%) municipal websites informed their users that they are using cookies. However, only 67 percent (n = 8) of municipal websites that reported using cookies stated the purposes for using cookies. Only four municipal websites notified their users that they have the possibility to block or refuse the usage of cookies, but only two indicated that the blockage or refusal of cookies may result in the user's inability to use certain sections of the website.

Concerns regarding the perceived potency of the cookie technology to invade privacy and the belief that cookies might harm the user's system (Ha, Al Shaar, Inkpen & Hdeib, 2006) are often confronted with a dosage of rhetoric. For instance, of the 12 privacy statements that stated that cookies are used, seven (58%) provided brief explanations about what cookies are, and three (43%) of which used the adjective 'small' in the definition. According to Pollach (2005), by emphasizing the small size of cookies (e.g. 'cookies are small pieces of information….'), companies and organizations are mitigating their questionable practices by implying that cookies are harmless and no cause for concern.

As the only guarantee in a privacy statement that can be verified by the user of a municipal website, the researchers used the cookie tracking tool of the web browser *Firefox 3* to determine if municipal websites that do not indicate cookie usage in their privacy statements do not really use cookies. Of the 77 visited municipal websites, 75 used cookies, whereas only 12 municipal websites cited in their privacy statements that cookies are being used. One municipal website did not mention using cookies, and it is confirmed using *Firefox 3*, as cookies were not traced.

Most municipal websites used session cookies, while a few used a combination of session cookies and temporary cookies. While the former expires at the end of the session, the latter does not - with the expiration dates set some days after the session. Table 8.4 is allotted for a number of other relevant assurances and notifications related to the usage of cookies.

Table 8.4. Other assurances and notifications related to the usage of cookies.

Statements of guarantees and/or notifications	12 websites used cookies
Data collected through cookies will stay in the users' computer	3 (25%)
Cookies will not track and store personally-identifiable information	6 (50%)
Cookies will not cause harm to the users' computer	1 (8%)
Notification of the types of cookies used	5 (42%)

8.7.1.11 Revisions in the privacy statements

Eleven (14%) municipal websites indicated that they reserve the right to revise their privacy statements, but only six (55%) mentioned that they would post the revised privacy statements. Municipal websites that cited the necessity for revising their privacy statements underscored the

notion that such revision is in line with the need to adapt the policy statements to certain circumstances. One municipal website only advised its users to consult the organizations' privacy statements for updates and changes.

According to Jensen et al. (2005), such advice places the burden of monitoring changes in the privacy statements on the users. This implies that online organizations should take the necessary step in providing their users with the convenience of being informed about revisions in their privacy statements, for instance by citing the latest date of revision of a particular privacy statement on the website.

8.7.1.12 Contact possibilities for inquiries regarding the privacy statements

An important requirement of fair information practices is the provision of contact information to the organization's users that will afford them the appropriate channels necessary for seeking answers to questions regarding the organization's privacy practices, and that will enable them to exercise their rights of choice and access (Strauss & Roberson, 2002). The implication of this provision is the online organization's recognition of the indispensability of transparency in fomenting users' trust. The result of the analysis of privacy statements of municipal websites is not promising—with only 16 percent (n = 12 of 77) of the municipal websites indicating relevant contact information in their privacy statements.

8.7.2 Are privacy statements available and findable?

Only 77 percent (n=77) of the 100 selected Dutch municipal websites contained privacy statements. In terms of the findability of the privacy statements on the websites, only 23 percent (n = 18) of the 77 municipal websites provided a conspicuous link (labeled as 'privacy' and displayed both on the lower section of the homepage and on succeeding pages) to the privacy statements, while 77 percent (n = 59) of the privacy statements can be found in other links within the websites (e.g. proclaimed/disclaimer, colophon, about the site, or contact). The figures indicate high difficulty for finding a privacy statement since users may end up having to click a lot of links before they can actually locate and read the privacy statement of the municipal website, unless they know exactly that the said statement is located, for instance, in the disclaimer.

8.8 Discussion

Privacy statements of municipal websites may lump all possible forms of notifications and assurances in a piece that could be too legalistic for an average reader (Milne & Culnan, 2004). In addition, they could still miss important points that users might expect to read. For instance, over

50% of the 100 municipal websites analyzed for this study contained notifications of the purposes for the collection of both personal data and information related to the users' visits to a municipality's website, but a remarkable percentage of those statements did not mention that users are entitled to have access to personal data they have disclosed to the organization and that necessary security measures are employed to ensure that their confidential data are protected.

Though most municipal websites observed the principle of notice by explaining the purposes for the collection of personal data from their users, their inability to extend a guarantee that allows users to review, rectify, and even remove their data, can result in a significantly incomplete privacy policy. Operators of those municipal websites that do not extend the right of access to their users may contend that since they are not storing collected personal data, as data would be destroyed after they have been used for a designated purpose, there is no justification for enabling users to have access to their personal data stored in the organization's database. However, the provision of the right of access is so fundamental (especially if organizations admit that they store collected data from users) that its non-inclusion in any privacy statement would indicate half-hearted compliance with the principles of fair information practice, and even more importantly with the existing legislation on the protection of information privacy.

The failure on the part of 80 percent of municipal websites to guarantee that necessary security technologies are employed to ensure the protection of collected personal data not only heightens users' apprehension about the possible misuse of their data but also signifies a loose conformity with the legal requirements on the application of security measures. The omission of an assurance of security in a privacy statement may stir users to think that their personal data are susceptible to third-party abuse, and this could discourage them from supplying the necessary personal data to complete a transaction online.

Even if municipal websites are indeed employing the required technology to ensure the security of personal data, from a communication perspective, such practices should at least be indicated in the privacy statement to assure users that personal data they will disclose for the completion of an online government transaction are secured and protected from unwarranted abuse. While most municipal websites indicated that they collect personal data, only a few mentioned that collected data will be stored in a database and will be destroyed after usage. Even if users are informed of the purposes for the collection of their personal data, there would still be questions on what will happen to the data after usage. Therefore, an assurance that data will be destroyed or deleted after they had been used for a particular purpose may help in dispelling users' fear about the fate of their personal data.

What is evident is that despite the many assurances and guarantees contained in the privacy statements of municipal websites, there are points that are highlighted in some statements but not included in others. When privacy statements do not include a particular guarantee or notice, two

interpretations are possible. It could be that they find saying something about what they are not doing irrelevant, or that they just opt not to say something about what they are actually doing. The second statement is more likely in the case of cookie usage. While almost all municipal websites that have privacy statements (n = 77) used cookies, only a quarter cited in their policy statements that cookies are being used.

While some privacy statements are considerably long to the point of including all possible guarantees that are in accordance with the Personal Data Protection Act of the Netherlands, other privacy statements are relatively short, with only one or two sentences. Such differences in length and structure could be attributed to the increasing application of the multilayered format, which Article 29 of Directive 95/46/EC recommends (Article 29 Data Protection Working Party, 2004).

The multilayered format has three structures: layer 1 (short notice) contains minimal information, primarily the identity of the data controller and the purpose(s) of the processing; layer 2 (condensed notice) presents the following information: the name of the company, the purpose of the data processing, the recipients of the data, the choices available for the users with regards to responding to questions and the consequences of such choices, the possibility of transfer to third parties, and the users' right of access; and layer 3 (full notice) should include all national legal requirements and specificities (Article 29 Data Protection Working Party, 2004).

Privacy statements of municipal websites also heavily rely on the use of rhetorical devices or 'overarching assurances' at the beginning of almost all privacy statements as an attempt to catch the users' trust even before the decision is made to continue or discontinue the reading of the entire privacy policy. Some examples of such 'overarching assurances' include the following: the organization respects the privacy of its users; collected data from users will be handled confidentially and treated with utmost care. The strategic placement of those broad assurances appears to confirm the result of an experiment that clients tend to read the first few sentences in the privacy statement (Vu et al., 2007), while leaving the remaining parts of the policy uninspected.

The selection of the first hundred municipal websites in the Netherlands, ranked according to the population size of the municipalities, was rooted on the premise that big municipalities will be conscientious in notifying their users about how their information privacy will be protected. However, as shown previously, privacy statements were still missing in the websites of 23 percent of municipalities selected for this study. Further, even though the majority of the municipal websites had privacy statements, a great number of those statements were difficult to find. Thus, users who are curious about the guarantees of a municipality's privacy statement will have to do some kind of a treasure hunt. An available privacy statement is bordering on insignificance if finding it demands herculean efforts from users.

8.9 Conclusion

Differences in the contents of privacy statements suggest differences in organizational practices that are adopted to ensure that the privacy of clients' data is maintained. These differences in contents also reflect differences in interpretations, on the part of organizations, of what users are expecting to read in privacy statements. This premise could be a starting point for exploring what users are really expecting to read in privacy policies of municipal websites and for determining which assurances and notifications are most important for them. While it is evident that the structure, content, and focus of the privacy policies on Dutch municipal websites vary significantly, the privacy statements should be constructed in a way that their contents and foci are aligned with the provisions contained in the existing laws on privacy protection.

As the present study also reveals that municipalities do not pay sufficient attention to the significance of making privacy statements findable on their websites, it would also be interesting to look into the impact of highly findable privacy statements on the formation of trust among Internet users. The finding is also surprising because it would be expected that government agencies should lead in the practice of posting privacy statements on their websites and in making them findable—not only for the sake of acquiring their users' trust, but also as a response to an ethical obligation of informing users about how their personal data will be handled.

While empirical studies on trust in online commercial exchanges are abundant, investigations on trust in e-government transactions are still sparse. An area that should be further explored is the relationship between (a) trust in a government organization and the decision to disclose personal data through its online channel as a prerequisite for an online transaction, (b) trust in the government organization's willingness and ability to protect its clients' personal data and the client's intention to read the privacy statement on the institution's website before the decision to disclose personal data, and (c) the contents of the privacy statement on a government organization's website and the decision to disclose personal data.

9

Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites

While several studies have shown that online privacy statements are hardly consulted or read, reading privacy statement is regarded as one of the strategies in dealing with online information privacy concerns. The study discussed in this chapter investigated the factors influencing Dutch Internet users' intention to read privacy statements on government websites. The study also focused on the pattern of privacy statement readership of Dutch Internet users and on the effect of available and findable online privacy statements on Internet users' trust in government organizations.

Results of the online survey revealed that although not all users consult a privacy statement on a municipal website before opting to disclose personal data, the availability and the ease of finding a privacy statement on a municipal website strongly contribute to users' belief that a municipality can be trusted with their personal data whenever they are shared for a particular online transaction. This study also shows that users' perceptions of the risks involved in the online disclosure of their personal data influence their intention to read online privacy statements on municipal websites. Older users are also more likely to consult privacy statements than their younger counterparts, while those with lower levels of education and Internet experience express a higher tendency to read such online documents than those with higher levels of education and Internet experience.

This chapter is based on a manuscript by Beldad, A., De Jong, M., & Steehouder, M. (2010), which has been published in Government Information Quarterly, 27(3), 238-24.

9.1 Introduction

Privacy statements or policies are documents posted on organizational websites that describe how organizations collect, use, and disclose their clients' data (Vail, Earp, & Anton, 2008). Although they are seldom perused, their presence on websites alone can persuade users that the organization can be trusted and that sharing data with that organization online is risk-free. Therefore, it is not surprising that organizations, both commercial and non-commercial in nature, are increasingly pushed to post privacy statements on their websites in an effort to quell internet users' information privacy concerns in the digital environment.

However, privacy statements should be more than just trustworthiness cues. Often they are the only means for internet users to know how organizations will process and use their personal data (Vail et al., 2008). Privacy statements should instead be regarded as crucial sources of information for users who are concerned about their online information privacy, which could be significantly impacted by the perceived risks of divulging personal data through the internet. Failure on the part of online organizations to post privacy statements on their websites can easily be regarded as an attempt to deprive internet users of the information necessary for them to decide whether or not requested personal data for a particular transaction will be shared online (Markel, 2005).

The Wet Bescherming Persoonsgegevens (WBP) or the Personal Data Protection Act of the Netherlands stipulates that the collection of personal data should be performed in accordance with the law and in an appropriate and careful manner (Article 6), and that it should be founded on specified, explicit, and legitimate purposes (Article 7). These provisions provide the foundation for the expectation that organizations, commercial or non-commercial in nature, should articulate their rationale for the online collection of personal data from users.

This rationale and the other assurances related to organizational usage and protection of personal data collected online are expected to be contained in a clickable document referred to as a privacy statement. However, in a study of privacy statements on Dutch municipal websites, there were still websites that do not contain privacy statements or any type of document that explains how personal data will be used, processed, and protected (Beldad, De Jong, & Steehouder, 2009).

Although internet users may perceive more risks in online commercial exchanges than in online government transactions (Belanger & Carter, 2008), the risks of having one's personal data misused and abused after being disclosed online for a particular government transaction is not negligible. While empirical studies on the readership of online privacy statements in the context of online commercial exchanges are copious, similar studies within the context of e-government transactions have not been pursued yet.

Previous studies on the online privacy statement readership of users had also been done mostly with American respondents. Differences between the online privacy statement readership behaviors of users from the United States and Netherlands would surely vary. However, this study did not address the aforementioned concern.

The study aimed at determining the patterns of online privacy statement readership of users in the Netherlands when transacting with government organizations, specifically with municipalities, through their websites. Factors that influenced users' intention to read privacy statements posted on municipal websites were also identified.

9.2 The importance of an online privacy statement

Online privacy statements can be regarded both as crucial sources of information and significant trustworthiness cues that any organization can use to subtly persuade its clients to supply personal data necessary for a specific online transaction or exchange. Studies have shown that even if online privacy statements are not read or consulted (Arcand et al., 2007; Jensen et al., 2005; Meinert et al., 2004; Vu, Chambers, et al., 2007; Vu, Garcia, et al., 2007), their mere presence would be enough to win users' conviction that an online organization can be trusted (Meinert et al., 2004; Pan & Zinkhan, 2006). Studies have also demonstrated that privacy statements are instrumental to the collection of accurate information from users (Xie, Teo, &Wan, 2006) and vital for establishing the credibility of websites (Sheehan, 2005).

Nevertheless, it is also noted that users are not only concerned about the presence or absence of privacy statements on websites, but are also interested in the contents of those statements (Ackmerman, Cranor, & Reagle, 1999). Whenever users are uncertain about how online organizations will deal with their personal data, privacy statements are often the only sources of information for them to be adequately informed of organizational practices involving their data (Vail et al., 2008), just as privacy statements can also serve as bases for users to decide whether or not they will disclose requested personal data (Jensen & Potts, 2004). Reading online privacy statements is regarded as one of the many online privacy protection behaviors internet users resort to (Milne, Rohm, & Bahl, 2004) and is seen as part of an overall strategy of managing perceived risks involved in online disclosures of personal data (Milne & Culnan, 2004).

9.3 Why do some read and others not?

The decision to read an online privacy statement is precipitated by a certain need. Often users who invest time to consult the said online privacy statements are those who are likely to engage in transactions that propel them to supply personal data (Meinert et al., 2006). Due to the perceived risks involved in online disclosures of personal data, which can

be attributed to users' lack of information about data handling practices of online organizations (Reagle & Cranor, 1997) and to users' inability to control other people's access to their personal data (Hoffman, Novak, & Peralta, 1999), they may eventually opt to read online privacy statements as one of the ways to address their privacy concerns (Milne & Culnan, 2004).

However, as noted earlier, most users do not bother to read or scan privacy statements before sharing their personal data for a specific online transaction. For one, many users do not know what a privacy statement is, nor do they understand its significance. This lack of understanding can lead them to overlook it despite its presence on a website (Lichenstein, Swatman, & Babu, 2003).

The legalistic nature (Bolchini et al., 2004; Milne & Culnan, 2004; Pan & Zinkhan, 2006) and the length of privacy statements (Bolchini et al., 2004; Milne & Culnan, 2004; Vu, Chambers, et al., 2007), making them incomprehensible and difficult to read (Milne & Culnan, 2004), are also cited as primary reasons for users' reluctance to read the aforementioned online documents. Users also do not bother to read privacy statements on organizational websites when they have prior positive experience with the organizations behind the sites (Milne & Culnan, 2004) and when they trust those organizations (Vu, Chambers, et al., 2007).

9.4 Do users' demographics matter?

In a number of studies, female internet users are found to be more concerned about their online privacy than their male counterparts (Cho, Rivera-Sanchez, & Lim, 2009; O'Neil, 2001; Sheehan, 1999; Youn & Hall, 2008); women also perceived more risks related to the disclosure of their personal data than men (Youn & Hall, 2008). As the level of risk perceptions increase, the tendency to seek information in an attempt to reduce these perceptions is also expected to intensify. Indeed, as shown in one study, women are more inclined to read online privacy statements than men (Milne & Culnan, 2004).

The impact of users' age on their privacy concerns was addressed in a study by Paine et al. (2007). The study showed that users over the age of 45 tend to be either not at all concerned about privacy or highly concerned about it. Since privacy appears to be more important for older Internet users than for younger users (Cho et al., 2009; Paine et al., 2007), one can expect that the former would be more predisposed to read privacy statements than the latter. Milne and Culnan (2004) also found out that users' age is positively related to their intention to read online privacy statements.

Concerns about online privacy are also found to be higher among users who had achieved higher levels of education than those with lower levels of education (Cho et al., 2009; Sheehan, 2002). However, it is surprising that education is negatively related to intention to read privacy statements (Milne & Culnan, 2004), suggesting that those with lower levels

of education are more inclined to peruse the aforementioned documents than people who are highly educated.

People with more internet experience have low privacy concerns (Bellman, et al., 2004; Cho et al., 2009), although another study reveals that privacy is an important concern for users with longer internet experience than those with lower levels of internet experience (Miyazaki & Fernandez, 2001). Nevertheless, if we subscribe to the finding that greater online experience results in decreased privacy concerns, it should be logical to hypothesize that those with low levels of internet experience, as they would be expected to have more privacy concerns, would be more inclined to seek information by consulting online privacy statements than those with higher levels of internet experience.

9.5 Research objectives and hypotheses

This study primarily aimed at knowing whether or not Internet users read privacy statements on municipal websites whenever they intend to supply their personal data to take advantage of the services their municipalities provide online, such as scheduling an appointment for the renewal of a passport or filing income tax returns. For this study, however, survey participants were provided with a different transaction scenario.

The study also looked into users' perceptions of the role of available and easily accessible online privacy statements in fostering the perceived trustworthiness of a municipality as recipients of users' data. Furthermore, the study aimed at determining the factors that influence users' intention to read privacy statements on municipal websites. To address the third objective, the following hypotheses were formulated:

1. Female internet users would be more inclined to read online privacy statements than their male counterparts.
2. Older internet users would be more inclined to read online privacy statements than younger internet users.
3. Internet users with lower levels of education would be more inclined to read online privacy statements than those with higher levels of education.
4. Internet users with lower levels of internet experience, measured in years, would be more inclined to read online privacy statements than those with higher levels of internet experience.
5. Users' perceptions of the risks involved in online disclosures of their personal data determine their intention to read privacy statements posted on municipal websites.
6. Users' lack of trust in their municipalities determines their intention to read privacy statements posted on the municipal websites.
7. Users' positive expectations of the content and the structure of a privacy statement determine their intention to read privacy statements posted on municipal websites.

The selection of these factors as determinants of users' intention to read an online privacy statement was based on previous studies on privacy statement readership behaviors of online users in the context of commercial transactions, considering the unavailability of similar studies within the framework of electronic government transactions.

9.6 Methodology

9.6.1 The respondents

Survey respondents were presented with the scenario of registering a child for an elementary school through their municipalities' websites. While an online registration of children for primary schools is not yet implemented in most parts of the Netherlands, the scenario was selected as it could be requesting a substantial amount of personal data from registrants, ranging from basic contact details to demographic and more sensitive information such as users' religion, ethnicity, and income. Throughout the survey, respondents were reminded to answer the questions with the said scenario in mind.

A link to the online survey was sent to employees of two vocational schools and to members of environmental groups based in one of the provinces of the Netherlands. Customized postcards explaining the purpose of the survey and containing the link to the online survey were also sent to 900 residents of three Dutch cities. A total of 1,152 invitations were sent out, generating 223 respondents, resulting in a response rate of 19 percent. Fifteen questionnaires were eventually excluded from analysis as they were not completed.

Fifty-two percent (n = 109) of those who completed the survey were males. Respondents' age ranged from 18 to 82, with a mean of 47.5 (SD=14.1). In terms of Internet experience (measured in years), almost half (n = 88, 43%) of the respondents indicated that they have been using the internet for 10 to 13 years already, with an average Internet experience of 10.7 years (SD = 4.2).

Considering the complicated system of ranking the levels of education in the Netherlands, the researchers decided to group respondents according to their educational attainment into two— those who have higher education (completed university and/or college education) and those who have lower education (did not complete university and/or college education, or only completed vocational education and high school education). For this study, 64 percent of respondents have lower levels of education, while the remaining 36 percent are highly educated. Table 9.1 shows the complete demographic information about the survey respondents.

Table 9.1. Demographic information of research respondents

Demographic characteristics		Freq.	%
Gender	Male	109	52
	Female	99	48
Age	under 30	26	13
	30 and under 50	86	41
	50 and under 65	75	36
	65 and under 75	14	7
	75 and over	7	3
Education	Low	133	64
	High	75	36
Internet experience	less than 2 years	1	1
	2 to 5 years	21	10
	6 to 9 years	48	23
	10 to 13 years	88	42
	14 years or more	50	24

9.6.2 The survey instrument

The research instrument used was divided into two, with the first part soliciting for respondents' demographic information and details regarding their Internet experience. The second part contained questions on users' perceptions of the risks involved in online disclosures of their personal data for e-government transactions, their levels of trust in their municipalities, their positive expectations of the content and the structure of a privacy statement, and their intention to read privacy statements posted on municipal websites.

The construct 'perceptions of the risks involved in online disclosures of personal data' was measured with statements that focused on the probability of information abuse either by organizations collecting the data or by external third parties. Statements that indicated Internet users' beliefs in the municipalities' possession of the necessary technology and expertise to protect citizens' personal data and confidence in the municipalities' willingness to safeguard the aforementioned data by not sharing them to third parties were used to measure 'level of trust in municipalities'. The construct 'expectations of the content and structure of a privacy statement' was measured in terms of whether or not privacy statements are easy to read, short, and do not contain technical and legal jargons.

9.7 Results

Cronbach's alpha scores for the constructs included in this study were calculated to determine their internal consistency. Reliability scores of all constructs, except for "positive expectations from the structure and the content of the online privacy statement" (a = 0.69), were all above 0.80, indicating highly acceptable reliability (DeVellis, 2003). Table 9.2 presents

the results of the reliability analysis and the mean and the standard deviation values of the constructs for this study.

Table 9.2. Alpha scores and mean and standard deviation values of the variables of the study (n = 208)

Construct	Scale	No. of Items	α	Mean (SD)
Perceptions of risks involved in online disclosures of personal data	5 (most likely) - 1 (not most likely)	3	.82	2.94 (0.84)
Level of trust in a government agency	5 (strongly agree) - 1 (strongly disagree)	8	.88	3.45 (0.69)
Positive expectations from the structure and the content of an online privacy statement on a municipal website	5 (strongly agree) - 1 (strongly disagree)	3	.69	3.08 (0.74)
Intention to read online privacy statements on a municipal website	5 (strongly agree) - 1 (strongly disagree)	3	.83	3.31 (0.93)

Frequencies and percentages were determined and calculated, respectively, to show the patterns of online privacy statement readership of users when transacting with a government agency online. Table 9.3 shows that over half of the total respondents (64%) indicated that they would read an online privacy statement before they would disclose their personal data when registering a child for a basic school through their municipal websites.

The majority of those who participated in the study (69%) agreed that the need to know how their data would be used and protected is a primary motivation for reading an online privacy statement. Only a minority of those surveyed (31%) stated that they would read a privacy statement on a municipal website even if they do not intend to share any personal data.

Table 9.3. Frequency counts and percentage of the items in 'intention to read online privacy statements'

Statement	Level	Freq.	%
I will read an online privacy statement on a municipal website before disclosing my personal data.	strongly agree agree neither agree nor disagree disagree strongly disagree	32 101 32 35 8	15 49 15 17 4
Even if I will not disclose personal data, I will still read the privacy statement on the municipal website.	strongly agree agree neither agree nor disagree disagree strongly disagree	11 54 41 72 30	5 26 20 35 14
I will read the privacy statement on the municipal website to know how my data will be used and protected.	strongly agree agree neither agree nor disagree disagree strongly disagree	34 111 28 28 7	16 53 14 14 3

The same procedure used to analyze the data in Table 9.3 was used to analyze the data in Table 9.4. Do respondents think that the availability

and the ease of finding an online privacy statement impact their appraisal of the trustworthiness of a municipality and their willingness to supply personal data whenever requested? The majority of the respondents (38%), though barely comprising half of the total number of those who took part in this study, agreed that the presence of a privacy statement on a municipal website reflects the trustworthiness of the municipality in terms of how it handles and processes users' personal data.

More than 50 percent of the respondents also agreed that the accessibility or the ease of finding a privacy statement on a municipal website is a sign that the municipality can be trusted with their personal data. Over half of the total number of respondents in this study indicated that a privacy statement on a municipal website would suffice to increase their willingness to share personal data.

Table 9.4. Frequency counts and percentage of the items in 'presence and accessibility of an online privacy statement and trustworthiness of the municipality'

Statement	Level	Freq.	%
The presence of a privacy statement on a municipal website indicates that the agency can be trusted with my personal data.	strongly agree	12	6
	agree	67	32
	neither agree nor disagree	71	34
	disagree	42	20
	strongly disagree	16	8
The ease of finding the privacy statement on a municipal website indicates that the agency can be trusted with my personal data.	strongly agree	11	5
	agree	100	48
	neither agree nor disagree	42	20
	disagree	39	19
	strongly disagree	16	8
The presence of a privacy statement on a municipal website increases my willingness to disclose personal data for a transaction with the agency with my personal data.	strongly agree	12	6
	agree	103	50
	neither agree nor disagree	39	19
	disagree	37	18
	strongly disagree	17	8

Hierarchical multiple regression analysis was performed to examine the relationship between the various predictor variables and users' intention to read privacy statements on municipal websites. The statistical technique enabled the researcher to decide on the ordering of the list of this study's predictors, which is achieved by putting the predictors or groups of predictors into blocks of variables (Howitt & Cramer, 2005).

Demographic variables (gender, age, education) were entered in the first block resulting in an explained variance of 11% ($F_{3, 204} = 8.13$; $p < 0.001$). After users' level of internet experience was entered in the second block, the explained variance rose to 14% ($F_{1, 203} = 7.12$; $p < 0.01$). Users' perceptions of the risks involved in online disclosures of their personal data, their levels of trust in their municipalities, and their positive expectations of the structure and the content of an online privacy statement were entered in the third block. This led to an explained variance of 21 percent ($F_{6, 197} = 3.20$; $p < 0.01$) for users' intention to read online privacy statements.

What is evident here is that although demographic variables accounted for 11% of the variance in users' intention to read a privacy statement on a municipal website, adding predictors such as perceptions of the risks involved in online disclosures of personal data and expectations of the structure and the content of a privacy statement, would significantly increase the variance for users' intention to read. In the complete model, users' age ($b = 0.31$, $p < .001$), their levels of education ($b = -0.14$, $p < .05$), their levels of internet experience ($b = -0.17$, $p < .05$), and their perceptions of the risks involved in online disclosures of their personal data ($b = 0.27$, $p < .001$) accounted for the calculated variance.

Older respondents are more likely to read online privacy statements compared to younger respondents. This lends credence to the result of an earlier study that age is positively related to the likelihood of or intention to read privacy statements on organizational websites (Milne & Culnan, 2004). Therefore, Hypothesis 2 is accepted. Online privacy statements may not often be read, but results of this study also show that users who perceived risks involved in online disclosures of their personal data were also more likely to read privacy statements on municipal websites. This supports Hypothesis 5.

The negative relationship between respondents' levels of education and their intention to peruse online privacy statements is also statistically supported, validating the hypothesis that respondents with lower levels of education are more likely to read online privacy statements than those with higher levels of education (Hypothesis 3) and further supporting results of previous studies on the relation between users' education and their readership of privacy statements (Milne & Culnan, 2004).

Analysis also revealed that respondents' level of internet experience is negatively related to their intention to read the aforementioned online document. This signifies that respondents with lower levels of internet experience would be more inclined to read privacy statements on municipal websites compared to those with higher levels of Internet experience, leading to the acceptance of Hypothesis 4. The absence of statistical significance for users' gender, their degree of trust in their municipalities, and their expectations from the structure and the content of online privacy statements as determinants of their intention to read privacy statements prompted the rejection of Hypotheses 1, 6, and 7.

Table 9.5 shows both the nonstandardized and the standardized coefficients of the different variables hypothesized to influence users' intention to read or consult online privacy statements on municipal websites.

Table 9.5. Coefficients of the variables hypothesized to influence users' intention to read online privacy statements

	B	SE B	β	R^2 (ΔR^2)
Step 1				.11 (.11)
• constant	3.02	.41		
• gender	.07	.13	.04	
• age	.02	.00	.29 *	
• education	-.14	.05	-.19 **	
Step 2				.14 (.03)
• constant	3.41	.43		
• gender	.00	.13	.00	
• age	.02	.00	.30 *	
• education	-.11	.05	-.16 ***	
• internet experience (in years)	-.04	.02	-.18 **	
Step 3				.21 (.07)
• constant	2.39	.72		
• gender	-.02	.13	-.01	
• age	.02	.00	.31 *	
• education	-.10	.05	-.14 ***	
• internet experience (in years)	-.04	.02	-.17 ***	
• perceptions of risks	.30	.08	.27 *	
• lack of trust in the government agency	.13	.09	.10	
• positive expectations from an online privacy statement	-.07	.08	-.06	

** $p < .001$, ** $p < .01$, *** $p < .05$*

9.8 Discussion and research implications

Although this survey reveals that not all respondents read online privacy statements, confirming results of previous studies (Arcand et al., 2007; Jensen et al., 2005; Meinert et al., 2004), it is worth noting that respondents consider the availability and the accessibility or findability of a privacy statement as indicators of a municipality's trustworthiness in terms of how it uses and processes users' personal data. The presence and the ease of finding an online privacy statement are sufficient to prompt most respondents to disclose requested personal data. This signifies that available and easily accessible privacy statements are potent trustworthiness cues, as also revealed by the study discussed in Chapter 5, which could moderate users' perceptions of the risks involved in the sharing of their personal data online.

A recent study on privacy statements on Dutch municipal websites reveals that of the 100 sites used for analysis, about 23 percent do not post any form of privacy statement or policy (Beldad, De Jong, & Steehouder, 2009). That same study also reported that only 23 percent of the analyzed websites provided a conspicuous link to a privacy statement, with the remaining 77 percent having privacy statements located in other parts of the websites (e.g. proclaimer/disclaimer, about the site, contact), denoting very low accessibility or findability levels.

Results pointing to the importance of available and accessible privacy statements as paramount online trust builders should already serve as an important recommendation for municipalities, in particular, and for

other government organizations, in general, to make privacy statements available on their websites and to improve their accessibility or findability if ever they are present on those sites. Ensuring that privacy statements are available on websites should not only be seen as an exercise of compliance with existing laws on personal data protection but should also be regarded as an ethical act of adequately informing users how their personal data will be used, processed, and protected.

However, it is also important for Internet users to consider that an available and findable privacy statement on a municipal website is not a sufficient guarantee that a particular municipality can be trusted with just any type of personal data that they would decide to disclose. Since this study did not focus on the impact of the contents of online privacy statements on users' trust in municipalities that collect their personal data it is hard to argue with any conviction that the contents of privacy statements would have a significant impact on users' concerns related to their personal data.

Considering the universal nature of online privacy concerns as they confront internet users regardless of their culture and geographic location (Cho et al., 2009; Raiha & Ovaska, 2009; Zhang, Chen, & Wen, 2002), the finding that available and easily accessible or findable privacy statements will increase users' trust in disclosing personal data for electronic government transactions may be valid not only in the Netherlands but also in countries where e-government services are constantly pushed for widespread citizen acceptance. However, increased acceptance and usage of electronic government services in any country depend not only on the perceived benefits that can be derived from the aforementioned type of service provision (Al Awadhi & Morris, 2009), but also on users' level of trust in this new system of service delivery (Belanger & Carter, 2008; Carter & Belanger, 2004).

Privacy issues, alongside security concerns, contribute to users' reluctance in trusting and using electronic government services (Al Awadhi & Morris, 2009). This leads to the premise that the mere presence of a privacy statement on a government website may help lower users' privacy concerns, which in turn may increase their trust in e-government services and their intention to use those services. Data analysis further reveals that a positive relation exists between users' age and their intention to read online privacy statements, and a negative relation exists between their levels of education and Internet experience and reading intentions.

Older users are more likely to read privacy statements on municipal websites compared to their younger counterparts, further supporting findings from an earlier study (Milne & Culnan, 2004). Highly educated users and those with higher levels of Internet experience have lower inclinations to peruse the aforementioned online documents. Users' gender, however, has no bearing on their willingness to read a privacy statement, despite results of earlier studies that women are more concerned about their privacy than men are (O'Neil, 2001; Sheehan, 1999; Youn & Hall, 2008).

While users' lack of trust does not propel them to read privacy statements, their perceptions of the risks involved in online disclosures of their personal data do. This supports the assertion that users read privacy statements as one way of dealing with online privacy risks (Milne & Culnan, 2004), which, in turn, further substantiates the hypothesis that uncertainties related to how organizations handle users' data push them to search for information to be adequately informed of organizational procedures related to data processing and handling. Increasing the accessibility of online privacy statements is also very crucial for government agencies with online services that cater to older citizens since it is known that they are most likely to consult such documents whenever they are requested to supply their personal data to complete a transaction.

However, this recommendation should also extend to other online organizations that target older users as clients. Even if it is revealed that most users do not read privacy statements, the few who do as a result of perceived risk might always check for a privacy statement whenever they intend to use the online services of their municipalities. If they discover that a privacy statement is missing, information-conscious users might be pressed to suppose that a particular municipality is not concerned about their needs for information related to organizational processing and usage of their data, which could further spur them to believe that the municipality could not be trusted with their personal data.

One may argue that the presence of trust could dispel perceptions of risks involved in data sharing. Within the context of the study, however, users may trust that their municipalities will not abuse, exploit, or misappropriate their data for purposes that could result in adverse consequences for them, but they may not be convinced that their personal data will be spared from unwarranted external intrusions.

Users may be associating risks related to online disclosures of their personal data with the probability of having their data abused, not by the municipality *per se* but by third parties with the technologies that provide them with unauthorized access to users' data. It can be surmised, therefore, that when users consult privacy statements on municipal websites, or on websites of other types of government agencies, because of perceived risks, they may be doing so to be sufficiently informed of the ways their data will be protected by a collecting government agency.

Since a number of investigations have also indicated that users refuse to read online privacy statements due to their legalistic nature and lengthy content, it can be hypothesized that when they have positive expectations regarding the structure and content of privacy statements, the likelihood that they will read such statements will increase. However, as revealed in this study, such expectations do not impact reading intentions, which could imply that regardless of the content and the structure of privacy statements, users will still read online privacy statements if they perceive greater risks in the online sharing of their personal data. Nevertheless, this assertion calls for further investigation to see whether or not users' positive expectations regarding the length, content, and structure

of privacy statements would really influence their intentions to consult online privacy statements regardless of their assessments of the risks involved in sharing personal data online.

9.9 Conclusion

The finding that perceptions of risks involved in online disclosures of personal data contribute to users' intention to read online privacy statements may be an indication that when users consult privacy statements they expect to read specific guarantees. For instance, they may expect to find information highlighting that municipalities, in particular, and government agencies, in general, will do whatever is necessary to protect users' personal data from unauthorized external intrusions. However, this is just one premise that requires further investigation, and signifies that future studies on the readership of online privacy statements, particularly within the context of e-government transactions, may have to focus on what users expect to read from such online documents.

Though the current study has attempted to test the impact of a number of factors on privacy statement reading intentions, other factors that could influence reading intentions but are not identified in this research should certainly be considered in future investigations. The sample size in this study constrains the generalizability of the findings, although the inclusion of respondents from all demographic clusters (according to age, gender, and level of education) indicates that the sample is not biased towards a particular group, which enabled the researchers to test the effect of respondents' demographic characteristics on their intention to read online privacy statements.

While countries within the European Union, including the Netherlands, have implemented laws to ensure the protection of citizens' personal data and information, many countries, including the United States, do not have comprehensive online privacy protection laws (Baumer, Earp, & Poindexter, 2004; O'Connor, 2008; Strauss & Rogerson, 2002). Bellman et al. (2004) cite that the existence of a legal protection of personal data substantially influences people's level of concern regarding online privacy.

From this statement, it can be hypothesized that users from countries without any personal data protection law would perceive more risks related to the disclosure of their personal data online and would be, therefore, more inclined to consult a privacy statement on any website before they would share their personal data for an online transaction than users from countries with existing personal data protection laws. Thus, a comparison in the online privacy statement readership behaviors of users from countries with and without personal data protection laws would be another matter to look into for future studies.

The domain of privacy studies in the context of e-government is still unripe and appears to call for further investigation. The widespread deployment of internet technology to extend a 24/7 government service

delivery entails accelerated disclosures of personal data on the part of users for the initiation and completion of various government transactions. Increased online disclosures of personal data in an environment saturated with possibilities for data abuse and illegal data usage will undoubtedly inflame risk perceptions, nudging users to resort to a host of privacy protection behaviors. With risk perceptions related to the online sharing of data comes the need for information on how data will be utilized. And this information can only be obtained from online privacy statements, assuming that a government agency bothers to post a comprehensive privacy statement on its website.

As people regardless of cultural differences (Cho et al., 2009; Raiha & Ovaska, 2009; Zhang et al., 2002) are confronted with privacy concerns, especially in their interactions with online entities that are both commercial and non-commercial in nature (Belanger & Carter, 2008), the role of privacy statements on websites should be more than an organizational attempt to comply with existing national laws on personal data protection but should be regarded as an ethical exercise of showing concern for users' needs for online information privacy. Just as Internet users from the Netherlands believe that an available and findable privacy statement on a government website is an indication of a government agency's trustworthiness in terms how it will use and process citizens' personal data, it is not implausible to insinuate that users from other countries would share a similar view. This assertion, therefore, calls for further investigation.

Regardless of whether or not online privacy statements are read, they assume important roles both for government agencies offering an online service and users. Attachment of importance to such online documents also suggests that, though oft ignored by users, they can be deserving of research interests.

10

General discussion of results, theoretical and practical implications, future research directions, and conclusion

Entrance to the wonderful world of the Internet does not always require us to identify who or what we are. Nonetheless, the possibility of having all our moves tracked by those miniscule and invisible 'hideous cookies' should not be discounted. While Ali Baba gained access to a cave where the bounty lies with 'open sesame', access to a gamut of online services is predicated on the disclosure of personal information. As emphasized in Chapters 2 and 5, sharing personal information online is far from safe. Perceptions of the risks trailing online personal information sharing spur the need for trust in the virtual environment.

This dissertation is entrenched in two central themes: the need for trust in e-government and the irrefutable reality of information privacy concerns prompted by online personal information disclosure for e-government services. In this chapter, the general findings of the different studies pursued along the two themes mentioned and the theoretical and practical implications of the results are discussed. Recommendations for future research are also presented.

10. 1 General Discussion

Five questions directed this research project. The first two questions were pursued to identify the determinants of a behavioral intention to disclose personal data for e-government services and of trust in government organizations within the framework of online transactions. The third question aimed at ascertaining the effect of trust or the lack thereof on risk perceptions related to the online disclosure of personal data for e-government services.

The importance of an online privacy statement in increasing Internet users' trust in government organizations in terms of their usage and processing of citizens' personal data prompted the two-fold question on the contents of privacy contents on government websites and on the conformity of those contents to the stipulations of the Dutch law on personal data protection. The fifth question addressed the determinants of Internet users' intention to read online privacy statements on government websites.

10.1.1. Factors influencing Dutch citizens' willingness to disclose personal data for online government transactions

Online transactions with government organizations, such as scheduling an appointment for a passport application or filing an income tax return, are intertwined with personal data sharing. However, the commoditization of personal data inflates their susceptibility to exploitation either by organizations that collect them or by external third parties for purposes unknown. Secondary usage of citizens' personal data could unerringly shape information privacy concerns, which in turn would fuel perceptions that disclosing personal data online is risky. Several authors (Germanakos, Christodoulou, & Samaras, 2007; Jaeger, 2003; Layne & Lee, 2001) argue that citizens' information privacy concerns are critical impediments for the realization and adoption of e-government services.

Using different theoretical perspectives, it is known that different factors can influence people's willingness and disinclination to disclose personal data for online government transactions. In Chapter 2, it is underscored that trust in the organization that collects personal data and low perceptions of the risks involved in online information sharing prompt information disclosure intentions. Without trust and with high risk perceptions, Internet users would be reluctant to supply their personal data for an e-government service, which would result in the failure of an online transaction. In this dissertation, citizens' willingness to disclose personal data is regarded as a measure of the adoption of e-government services among Dutch citizens.

From an exchange perspective, the behavioral intention to disclose personal information online can be triggered by a belief that disclosure may

result in the acquisition of 'something' valuable in return. This is to say that Internet users would be very inclined to share personal data if the value of the expected benefits of online information disclosure outweighs its estimated cost. The fact that personal data have become tradable and profitable commodities in a competitive market implies that Internet users are starting to regard information disclosure as some kind of an exchange. Internet users would not hesitate to fill out online forms if doing so would instigate the procurement of both tangible (e.g. gift checks) and intangible (e.g. convenience of doing things online) benefits.

A large-scale Internet-based survey with 2,202 Internet users in the Netherlands was implemented. Respondents were segregated according to whether or not they have experienced availing government services online. This was based on the premise that the impact of trust, risk perceptions, and expected benefits on the behavioral intention to share personal data for e-government services would vary considerably among Internet users with e-government experience and those without. As discussed in Chapter 5, Internet users' trust in government organizations, specifically in terms of their processing and usage of citizens' personal data, is a very important factor influencing the behavioral intention to disclose personal data for online government transactions.

The study also reveals that personal information sharing for e-government services can also be expected if citizens believe that the risks involved in the disclosure act are minimal or almost non-existent. It is also known that a negative relation between trust and risks perceptions exists. When Internet users trust government organizations (in terms of their processing and usage of citizens' personal data) their perceptions of the risks of disclosing personal information would be less. The relationship between trust and risk perception, as established in another empirical study, however, will be discussed thoroughly in the later part of this chapter.

In consonance with the postulations of the exchange theory, results of the large-scale online survey further indicate that expected benefits that can be derived from an online government service also prompt the disclosure of personal information for a particular e-government service. For instance, Internet users, with and without any e-government experience, would not hesitate to supply personal information for an online government service when availing that service would save them time and energy.

Beliefs in the adequacy of legal protection for online transactions can also increase Internet users' inclination to share personal data for e-government services. These beliefs are also found to improve users' trust in government organizations in terms of their processing and usage of citizens' personal data. The association is clear. Internet users' trust is somehow anchored on the existence of laws that would ensure the safety of their transactions online and the personal data that they will disclose for those transactions. Therefore, laws protecting online transactions and personal data supplied for online transactions can be regarded as safety

nets that could somehow taper risk perceptions and boost Internet users' confidence.

10.1.2. Determinants of trust in government organizations within the frame of online government transactions

Trust is indubitably essential in increasing Internet users' intention to disclose personal data for e-government services, as evidenced by the previously described large-scale Internet-based survey. In fact, a sizable number of empirical studies affirmed that trust is pivotal in influencing Internet users' decision to engage in online commercial exchanges (Buttner & Goritz, 2008; Everard & Galleta, 2005; Gefen, 2000; Keh & Xie, 2009; Kim, Ferrin, & Rao, 2008; McKnight, Choudhoury, & Kacmar, 2002) and non-commercial transactions, such as those done with government organizations (Belanger & Carter, 2008; Carter & Belanger, 2005; Colesca & Dobrica, 2008). Trust also steers Internet users to share their personal information for computer-mediated transactions (Malhotra, Kim, & Agarwal, 2004; McKnight, Choudhoury, & Kacmar, 2002; Schoenbachler & Gordon, 2002; Dinev & Hart, 2006; Zimmer et al., 2010).

The thing is that trust does not emerge from nothingness. For instance, in the physical world, it is argued that people base their trust in other parties or entities on three criteria: reputation, performance, and appearance (Sztompka, 1999). This contention still makes sense when applied in an online environment. The distance, intangibility, and impersonality of online exchanges and interactions would surely propel Internet users to look for cues that would signal the trustworthiness of the other party in the exchange. A comprehensive review of literature, in Chapter 3, underscored that the development of online trust can be attributed to several cues (organization-based cues such as reputation and website-based cues like privacy statements and security features) and factors (mostly Internet user-based such as trust propensity and Internet experience).

However, as Bart et al. (2005) noted, the effects of different cues on online trust vary across website categories and Internet users. For instance, third party guarantees may be effective in endorsing the privacy and security policies and practices of commercial organizations (Cheung & Lee, 2006), but these factors would hardly influence citizens' trust in government organizations, especially if the practice of having external agencies monitor government organizations' usage, processing, and protection of citizens' personal data is not common.

Results of three focus group discussions, as elaborated in Chapter 4, indicated that Dutch Internet users consider three criteria in appraising the trustworthiness of an organization as the other party in an online transaction: website quality, indication of security technology usage, and the presence of a privacy statement on a website. However, the items identified are mostly website-based trust cues. To systematically identify the real determinants of trust in government organizations, specifically in

terms of their usage and processing of citizens' personal data, another large-scale online survey was implemented with 1,156 Dutch Internet users. Respondents were again segregated into two: those with e-government experience and those without.

Trust in government organizations, in terms of their usage and processing of citizens' personal data, is strongly influenced by Internet users' (with and without e-government experience) confidence in privacy statements on government websites. This seems logical since citizens' trust in this context specifically targets government organizations' expected behavior towards citizens' personal data. Several studies have shown that even if online privacy statements are not read or consulted, their mere presence on websites would already increase Internet users trust in organizations as recipients of personal data.

In this study, however, it is assumed that the availability of privacy statements does not suffice in influencing Internet users' trust. Internet users must also have confidence in available privacy statements as effective guarantees for the ethical behaviors of organizations. This confidence in the aforementioned online document would then translate into Internet users' trust in government organizations in terms of their processing and usage of citizens' personal data.

Among Dutch Internet users who have transacted with government organizations online, a positive government organizational reputation and a positive online government transaction experience also could increase their trust in government organizations in terms of their processing and usage of citizens' personal data. With the risk of having personal data in government electronic databases illegally accessed by external third parties, it would be expected that Internet users will look for an indication that a government organization employs appropriate security technologies to ensure the protection of collected data from citizens. However, it is surprising that an indication of security technology usage does not influence trust in government organizations. A possible explanation for this finding is that survey respondents did not believe that government organizations are using security mechanisms to protect citizens' personal data from unauthorized third-party access.

10.1.3 The relationship between Internet users' trust in government organizations and their perceptions of the risks involved in sharing personal data for electronic government services

Risks necessitate trust (Koller, 1988; Lewis & Weigert, 1985), since the latter would be irrelevant if actions can be pursued with certainty (Lewis & Weigert, 1985). Nevertheless, as shown in several studies, trust in another party can lower perceptions of the risks involved transacting with that party, just as lack of trust could inflate risk perceptions. It was previously indicated in Chapter 5 that Internet users' trust in government

organizations could reduce their perceptions of the risks involved in sharing personal data for e-government services.

In a small-scale online survey with 208 respondents, it was hypothesized that perceptions of the risks involved in online information disclosure are determined by a number of factors such as Internet users' lack of trust in government organizations' ability and their willingness to protect citizens' personal data, their estimation of the sensitivity of personal data that they will share online, and their levels of experience with the Internet. Data analysis revealed that Internet users' lack of trust in a government organizations' ability to protect citizens' personal data contributes to perceptions of the risks involved in online information disclosure. This signifies that whenever Internet users are uncertain about whether or not appropriate technologies are employed to protect their personal data they will be stirred to believe that data disclosed for e-government services would be vulnerable to third-party abuse.

Results of the aforesaid study also indicated that Internet users would perceive more risks in disclosing personal data regarded highly sensitive, such as their publicly accessible contact information (postal address, telephone number) and information considered too confidential to be shared with just anybody (income, health-related information, and even, e-mail address and mobile phone number). However, risks perceptions, as this study also shows, are not influenced by Internet users' lack of trust in a government organization's willingness to protect citizens' personal data. This could be attributed to the fact that survey participants expressed trust in a government organization's willingness to protect citizens' personal data.

10.1.4 Contents of privacy statements on government websites and the conformity of the contents to the provisions of the law on personal data protection

The European Union's Directive 95/46 is a clear expression of the need for an institutionalized protection of personal data. As a member of the European Union, the Netherlands implements the directive through the *Wet Bescherming Persoonsgegevens* (WBP) or Personal Data Protection Act. One of the central themes in the law just cited is transparency on the part of organizations in the processing of their 'clients' personal data (Borking & Raab, 2001). This need for transparency substantiates the indispensability of online privacy statements since they are critical sources of information on how organizations will use, process, and protect personal data they will be collecting.

Analysis reveals that the contents of a number of privacy statements do not conform to the stipulations of the law on personal data protection. For instance, while WBP underscores that personal collection should be founded on specified, explicit, and legitimate purposes (Article 7), signifying that organizations should articulate their rationale for the

collection of personal data from their clients, less than 75 percent of the analyzed privacy statements stated their purposes for data collection. The Dutch Personal Data Protection Act also prescribes that data should be destroyed after they have been used for the purposes they were collected for (Article 10, Section 1). However, only 30 percent of the privacy statements stated that collected personal data from citizens will be destroyed after they have been used.

What is clear from the content analysis is that privacy statements on municipal websites, despite their many assurances and promises, still missed to contain important points that are required by the personal data protection law and points that any Internet user might expect to read. Whereas most privacy statements contained notifications of the purposes for data collection, many did not mention, for instance, that Internet users have the right to access their personal data in case they find it necessary to rectify, modify, or remove those data. Thus, it is evident that while some privacy statements on Dutch municipal websites were constructed to meet most of the requirements of the Dutch Personal Data Protection Act, others only offered general and, oftentimes, vague guarantees.

Two interpretations are possible for the failure of government organizations to include a particular guarantee or promise in their online privacy statements. First, it could be that organizations found it irrelevant to say something about what they do not do. Second, they probably just opted not to say something about what they are actually doing. For instance, most privacy statements did not indicate that cookies are used in municipal websites. However, it was discovered, through a cookie tracking technology, that almost all municipal websites included in the study actually utilized cookies.

Websites of the 100 biggest Dutch municipalities, in terms of population, were selected for this study. It was initially assumed that the contents of 100 online privacy statements would be analyzed. However, only 77 privacy statements were subjected to analysis considering that 33 municipal websites did not have privacy statements. This strongly suggests that a significant number of municipalities do not see the significance of privacy statements and do not regard the posting of privacy statements on their websites as an ethical obligation of sufficiently informing their 'clients' how their personal data will be used and processed.

10.1.5 Factors influencing citizens' intention to read privacy statements on government websites

Empirical studies accentuating the low readership of online privacy statements teem. Reading privacy statement obviates the speedy performance of an act in the online environment. Privacy statements are often not perused because doing so would cost time or they simply are too complicated to be understood with their legal and technical jargons. Nonetheless, Milne and Culnan (2004) accentuated that reading online

privacy statements is one of the strategies Internet users employ to manage the perceived risks involved in disclosing personal data online.

In Chapter 2, it was cited that Internet users' trust in organizations in terms of their usage and processing of clients' personal data would positively reduce their intention to read privacy statements on organizational websites. As the theory of uncertainty reduction postulates, uncertainties regarding organizational usage and processing of Internet users' personal data would spark increased motivation on the part of Internet users to seek information on how their personal data will be used and protected by consulting online privacy statements.

A small-scale Internet-based survey was conducted to identity the factors that would influence Dutch Internet users' intention to read online privacy statements on government websites. Perceptions of the risks involved in disclosing personal data online emerged as an important determinant of online privacy statement reading intention.

The study also probed into the impact of Internet users' characteristics (e.g. gender, age, Internet experience) on their willingness to consult privacy statements on government websites. The effects of age, Internet experience, and level of education on privacy statement reading intention are apparent. Older Internet users are more inclined to read online privacy statements than younger Internet users, while those with low levels of education and Internet experience indicated a higher disposition to peruse the aforementioned online document than those with high levels of education and Internet experience.

10.2 Implications of the results

10.2.1. Theoretical implications

While existing studies on trust in e-government have focused on two trust targets, namely government organizations and the technology used for an online transaction (Belanger & Carter, 2008; Carter & Belnager, 2005; Teo, Srivastava, & Jiang), trust in this dissertation is operationalized in terms of Internet users' appraisal of the ability and the willingness of government organizations to protect citizens' personal data. This conceptualization is aligned with the view of trust as an expectation of the behavior of the other party in a trusting situation (Barber, 1983; Koller, 1988; Luhmann, 1979; Rotter, 1967) and a belief in the trustee's willingness and ability to act in the trustor's best interest (McLain & Hackman, 1999).

Perceptions of the risks involved in any form of online transactions would expectedly necessitate trust in the Internet technology, which is perceived in terms of the availability of safeguards, structures, or systems to ensure the safety of transactions or exchanges in the virtual environment. However, such safeguards and structures do not spring just out of nowhere. They are implemented, deployed, and maintained. Some hands are responsible for their existence. Therefore, people and entities behind a

technology or those using it should be trusted and not the technology itself (Friedman, Kahn, & Howe, 2000).

The safety of disclosed personal data from unauthorized and unwarranted third-party access depends not on the speculated innate security of the Internet technology but rather on the ability or competence of organizations to protect whatever data have been collected from their 'clients', specifically through the usage of security mechanisms such as encryption technologies. This justifies the emphasis on the notion of trust in government organizations in an online setting as partly predicated on their ability and competence.

Nonetheless, the risks involved in online personal data disclosure can also be attributed to the organization collecting the data. For instance, personal data shared to online commercial organizations might be relayed to other parties for marketing purposes without the knowledge and consent of individuals to whom the data pertain. Government organizations in the Netherlands may not be in the habit of sharing citizens' personal information to commercial and marketing organizations but they will certainly relay citizens' personal information to other government agencies when legally obliged. In fact, a number of analyzed privacy statements on municipal websites emphasized this point.

A significant contribution of this dissertation to online trust research is its focus not only on trust in the context of electronic government but also on the determinants of trust in the aforementioned system or mode of service delivery, considering that empirical studies on the second area are remarkably few when compared to those pursued within the frame of online commercial exchanges. The impact of trust, alongside other factors such as risk perceptions and expected benefits, on Dutch citizens' behavioral intention to disclose personal data for e-government services has also been explored in this dissertation.

Furthermore, information privacy concerns and behaviors in the context of e-government remain underexplored. The application of a comprehensive model to understand citizens' willingness to disclose personal data for government services could be regarded as another significant contribution of this dissertation, specifically to information privacy research within the context of e-government.

10.2.2 Practical implications

Trust, as already noted, is of paramount importance for the augmentation of citizens' willingness to engage in online government transactions via their predilection to share personal information online, just as trust proves compelling in reducing risk perceptions. Therefore, it is imperative for any government organization that channels its services online to win its' 'clients' trust' through the fortification of its image as a trustworthy entity.

10.2.2.1 Make things secure and make it known

Confronted with information privacy risks, Internet users would be pressed to look for an indication that security mechanisms are employed to protect personal information transmitted online. The finding that Internet users' beliefs in organizational usage of security do not increase trust in e-government is considerably surprising. A possible explanation is that research respondents do not believe that government organizations are using security technologies to ensure the safety of online transactions, in general, and of personal information, in particular.

It is shown in Chapter 7 that Internet users' lack of trust in a government organization's ability to protect citizens' personal data significantly influences their perceptions of the risks involved in disclosing personal data online. This clearly indicates that when Internet users do not trust that government organizations employ necessary and appropriate technologies to protect personal data they will share online their perceptions of the risks involved in disclosing personal data online will increase. This only means that government organizations should emphasize their usage of security mechanisms as one strategy to reduce citizens' perceptions of the risks involved in the disclosure of personal information for e-government services.

10.2.2.2 Privacy statements nurture trust

Confidence in online privacy statements, as discussed in Chapter 6, positively influences citizens' trust in government organizations in terms of how they will deal with citizens' personal data. Nonetheless, available privacy statements would just be irrelevant if finding them is cumbersome. An inspection of the *findability* and availability of privacy statements on municipal websites indicated that a great number of those privacy statements are practically difficult to find as they are either not labeled or located in other sections of the websites that are labeled differently.

The importance of findable and available privacy statements on government websites is indisputable. As underscored in Chapter 8, the availability and the accessibility or *findability* of privacy statements are regarded as indicators of government organizations' trustworthiness in terms of how they will use and process citizens' personal data. The presence and the ease of finding an online privacy statement might suffice to prompt most respondents to disclose personal data for e-government services. This signifies that available and easily accessible privacy statements are potent trustworthiness cues, which could moderate or reduce users' perceptions of the risks involved in sharing personal data online.

Government organizations, therefore, should not only strive to include privacy statements on their websites but also increase the ease of finding them whenever available. The posting of online statements should even be regarded as an ethical responsibility of informing citizens how their

data will be used, processed, and protected. Even if online privacy statements are not always perused, the few who do due to the perceived risks involved in online information disclosure would be expected to clamor for the availability of guarantees emphasizing that disclosed personal data will not be abused and will only be used for the purposes they were collected for. Therefore, government organizations should employ privacy statements as appropriate media to emphasize transparency in their processing and usage of citizens' personal data.

10.2.2.3 Reputation matters

Organizational reputation increases Internet users' trust in government organizations in terms of how they process and use citizens' personal data, as accentuated in Chapter 6. Banks and other commercial organizations have a lot to lose if they fail to maintain their clients' trust, considering the stiff competition in the market. People would not hesitate to abandon online shops or other commercial institutions that could not be trusted. Hence, messing with people's trust in a competitive market could be disastrous for a particular commercial organization.

Government organizations, however, may not really bother about not earning citizens' trust in electronic government transactions for two reasons. First, they have monopoly over the services and products they offer to citizens. Second, citizens will have, in one way or another, to avail a particular government service either through a government organization's electronic channel or through its physical outlet. With monopoly comes a nonchalant attitude, on the part of government organizations, toward the necessity of constantly maintaining a trustworthy image.

Nevertheless, despite the discernable monopoly of government organizations over a range of products and services, a particular government organization that offers its services online still faces the unwarranted but real competition. It competes with itself in terms of the mode of its service delivery. Citizens who opt not engage in online transactions with a particular government organization, perhaps for lack of trust in or lack of knowledge of the aforementioned mode of transaction, always have the possibility to engage in the same transaction through the government organization's offline channel. One can only imagine the significant loss in the investment for the construction and implementation of electronic channels for government service delivery if a substantial number of citizens would just prefer to transact with organizations offline.

Cues such as privacy statements may not suffice to persuade most citizens that a particular government organization can be trusted with their personal data. In fact, 'privacy fundamentalists' might just regard conspicuous trustworthiness cues as subtle attempts to manipulate citizens' trust. In this case, government organizations might not succeed in winning citizens' trust with the simple use of trustworthiness cues. Instead, they need to resort to the fortification of their images as trustworthy institutions by not resorting to activities that could be regarded as a betrayal of public

trust, such as the accidental, or even intentional, disclosure of citizens' personal data to online and offline channels.

10.2.2.4 Satisfaction begets trust

Although a positive online transaction experience does not directly translate into citizens' willingness to disclose personal information, as noted in Chapter 5, its effects are noteworthy since it does not only enhance citizens' trust in government organizations and reduces risk perceptions, but also amplifies the appraisal of the benefits of e-government services. Since high levels of trust, low risk perceptions, and high estimations of e-government benefits could result in a heightened intention to disclose information online, it could, therefore, be surmised that a positive online transaction experience indirectly increases intentions to engage in online government transactions, preceded by a willingness to divulge personal data. Government organizations, therefore, must ensure that citizens who opt to avail government services online are highly satisfied with their transactions.

People who are highly positive about their previous online government transactions are also inclined to be trusting of government organizations, as revealed by the analysis of the survey data. What this result reverberates is the exigency for government organizations to constantly guarantee citizens with a satisfying and fulfilling online transaction experience. Government organization can certainly satisfy citizens who transact online in so many ways. For instance, citizens should have the possibility to track the progress of their online requests and applications, since it was raised during the focus group sessions that transacting with a government organization online makes it impossible for citizens to know whether or not their transactions will be processed correctly and promptly.

10.3 Future research directions

10.3.1. Explore not only perceived risks but also actual risks

Disclosures of personal data to avail electronic government services are peppered with risks. First, there is the risk that government organizations will transmit citizens' personal data to other government agencies or to commercial organizations without the knowledge and consent of those to whom the data pertain. Second, there is the risk that personal data stored in electronic government databases could be illegally accessed by external parties for unknown purposes. Risk perceptions instead of actual risks are highlighted in this study since 'capturing' the former as an objective reality is regarded difficult (Pavlou, 2003; Warkentin et al., 2002).

The possible risks related to an online sharing of personal data for e-government services are based on perceptions of the risks involved in supplying personal information for online commercial exchanges. Focus group sessions (Chapter 4) partly unveiled the risks involved in sharing personal data for e-government services as perceived by participants. Nevertheless, it is possible that participants have limited knowledge of the risks involved in disclosing personal data for e-government services.

There is no denying that risk perceptions could already curtail personal information disclosure behaviors (Malthotra, Kim, & Agarwal, 2004; Norberg, Horne, & Norberg, 2007; Treiblmaier & Chong, 2007). However, the need to understand the actual risks in online personal information disclosure, if they do exist, is also an urgent concern. Understanding actual risks involved in sharing personal information for e-government services may significantly contribute to an understanding of the reality of online personal information disclosure risks.

10.3.2 Revisit the notion of online information privacy

The definition of information privacy in this study is primarily theoretical and founded on the perspectives of a couple of experts. The concept of online information privacy might have changed significantly within the past few years considering how Internet users have increasingly asserted their presence in the virtual environment. One should consider the phenomenal popularity of online social networking, which primarily prompts Internet users to share something about themselves before online identities can be created. The risks in such a disclosure are indubitably analogous to those that can be expected in sharing personal information for e-government services. Nonetheless, a remarkable amount of personal information is constantly transmitted online for the sake of being present virtually.

Changing attitudes towards personal information in the online environment are expected to fuel information privacy concerns, which may compel an eventual revision in the definition of online information privacy. Thus, it should be a legitimate agendum to explore Internet users' perspective on online information privacy to be informed whether or not such a perspective would still coincide with the established perspective on the aforementioned type of privacy.

10.3.3 Investigate the effects of the contents and the structures of privacy statements on information disclosure intentions and risk perceptions

In consonance with several investigations, one of the studies presented in this dissertation (Chapter 6) indicates that Internet users' confidence in privacy statements posted on government websites could positively affect users' trust in government organizations in terms of their processing and usage of citizens' personal data. While the contents of

privacy statements on government websites had already been analyzed (Chapter 8), the impact of those contents on citizens' trust in government organizations and risk perceptions related to online disclosures of personal information for e-government services has not been explored.

It is true that most Internet users seldom consult privacy statements before opting to share personal information for an online transaction. Nonetheless, information privacy conscious users, though presumably few, may always peruse the abovementioned documents whenever pressed to complete an electronic form at the start of a computer-mediated exchange. Privacy statements on government websites differ considerably in terms of their contents and their structures, as highlighted in Chapter 8.

A study by Earp et al. (2005) accentuates that a tension exists between what organizations emphasized on their online privacy statements and what Internet users expect to read from those online documents. For instance, organizations stressed the explicit and hidden processes about data collection, while Internet users are more concerned about information related to the possible transmission of their information to third parties (Earp et al., 2005). Such tension may instigate Internet users to believe that organizations collecting their personal data put organizational interests above their clients'.

While most privacy statements on government websites emphasized that citizens' personal information will be respected and treated confidentially, only a few contained any notification that citizens have the right to object to the disclosure of their personal information to third parties. The inclusion and the exclusion of certain guarantees from online privacy statements may have serious consequences for citizens' inclination to share personal information for e-government services. Future research could, therefore, explore the impact of privacy statements containing different guarantees on Internet users' trust in government organizations, on their perceptions of the risks involved in sharing personal information for e-government services, and on their willingness to disclose personal information correctly and completely.

10.3.4 Examine the impact of website design characteristics on trust in e-government services

Privacy statements on websites are potent trustworthiness cues, just as indications of security usage enhance Internet users' trust in organizations as partners in online transactions. Since Internet users are deprived of the opportunity to interact with a flesh-and-blood government agent during an online government transaction, the website deployed for the transaction immediately becomes the visible transaction partner. In one of the large-scale surveys conducted (Chapter 6), website quality, as a trust determinant, was measured in terms of website navigability and the availability of relevant information on a government website.

Despite the absence of effect of website quality on trust in government organizations (specifically in terms of their processing and usage of citizens' personal data), it is firmly postulated that the aforementioned 'variable' as a potential trustworthiness cue merits reconsideration. The effects of the other aspects of website quality (e.g. layout, colors, font types, and photographs), aside from website navigability and information quality, on trust in government organizations within the context of online transactions certainly deserve further investigation.

10.3.5 Compare trust and risk perceptions in government transactions and those done with commercial organizations

A small-scale survey conducted before every focus group discussion (FGD) session (Chapter 4) revealed that online banking is trusted more than transactions with government organizations, which are in turn regarded as more trustworthy than online exchanges with commercial organizations (e.g. web shops). Although strong conclusions could not be readily derived from such a survey with only a handful of respondents, the initial findings could be taken as a springboard for a possible large-scale study on trust in different online transactions. A comparison of risk perceptions and privacy concerns in different online transactions could be another agendum worthy of research pursuit. This would address the inquiry on whether or not perceptions of information privacy risks are higher in online commercial transactions than those with government organizations.

10.3.6 Explore the impact of the nature and the structure of government organizations on citizens' trust and perceptions of the risks involved in online transactions with those government organizations

Results of the small-scale survey conducted before the FGD sessions also indicated that participants' trust in online transactions with the tax service office is slightly higher than their trust in online transactions with municipalities. While the aforementioned results are far from being conclusive, they somehow give a hint at the high probability of citizens trusting different types of government organizations in varying degrees. This assertion substantiates the recommendation that the nature and the structure of government organizations be explored as possible factors impacting variations in citizens' trust in online transactions with different government organizations.

Some online transactions with particular government organizations could be requesting for more sensitive personal data than other online government transactions. For instance, filing an annual tax return online prompts citizens to share sensitive information (e.g. income), which may

not be asked when they would be requesting for an appointment for a passport application through a municipality's website. Since different types of online transactions with different government organizations necessitate the disclosure of different types of personal data, citizens' perceptions of the risks involved in sharing personal data for online transactions with different government organizations could also be investigated.

10.3.7 Understand the impact of culture on trust and information privacy concerns within the context of e-government

Although results of the different studies might somehow reflect trust issues and information privacy concerns within the context of e-government among Dutch Internet users, the research findings would hardly be valid beyond the borders of the Netherlands. Individuals delineated by cultural differences and those coming from different societies will vary in their overall level of trust and in the ways trust is formed (Doney, Cannon, & Mullen, 1998), just as expressions of privacy significantly vary across cultures (Westin, 2003). For instance, trust propensity has been found higher among individuals from individualist cultures than those from collectivist cultures (Huff & Kelley, 2003; 2005).

It has also been advanced that people's privacy concerns are strongly associated with the cultural values of their countries (Milberg, Smith, & Burke, 2000). Citizens from countries without privacy protection laws are said to have more information privacy concerns than those from countries with similar laws (Bellman, Johnson, & Kobrin, 2004). Nevertheless, information privacy concerns could also vary among citizens from different countries with privacy protection laws.

For instance, the Eurobarometer survey (Gallup Organization, 2008) indicated that Germans (64.6%) are very much concerned about organizational protection of their personal data compared to Dutch (7.7%). Although Germany and the Netherlands both have privacy protection laws, variations in information concerns of the citizens of the two countries could be attributed to differences in national or cultural values. It is, therefore, recommended that the impact of cultural differences and values on trust and information privacy, specifically within the context of e-government, be explored.

10.4 Conclusion

The success of e-government certainly depends on numerous factors. While citizens' realization of the benefits of being able to access government services online contributes to the wide acceptance of e-government, perceptions of the risks in transacting with government organizations electronically could also reduce citizens' e-government usage intention.

Since availing government services online is tightly linked with personal information disclosure, one can only expect that information privacy-conscious citizens would evade online government transactions. It is, therefore, crucial that citizens' trust in government organizations that channel their services online is firmly established. Specifically, government organizations should be regarded as trustworthy recipients of citizens' personal data.

Citizens would not hesitate to share their personal data for an online government transaction when the government organization collecting the data can be trusted. Trust in a government organization does not only increase citizens' information disclosure intention but also lowers citizens' perceptions of the risks involved in personal information sharing.

Winning citizens' trust in a particular government organization, nonetheless, is an arduous hurdle. While government organizations should persistently and consistently strive to maintain their trustworthiness, the burden of building a trustworthy image could be eased by relying on certain cues. For instance, privacy statements on a government website and a positive government organizational reputation could help foster trust in a government organization. A satisfying online transaction experience with a government organization also inflates citizens' trust.

Citizens must always be assured that whatever personal data they will share for an e-government service would be treated with utmost respect and safeguarded. At the same time, government organizations should constantly strive to uphold their reputation as trustworthy recipients of citizens' personal data. In the end, the right to information privacy, though not absolute, still merits protection.

References

Ackerman, M.S., Cranor, LF., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. Proceedings of the 1st ACM conference on Electronic commerce, *Denver*, CO. Retrieved from http://portal.acm.org/citation.cfm?id=336995.

Acquisti, A. & Grossklags, J. (2004). Privacy attitudes and privacy behavior: losses, gains, and hyperbolic discounting. In J. Camp & S. Lewis (Eds.), *Economics of Information Security (pp. 165-178).* Boston: Kluwer Academic Publishers.

Acquisti, A. & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy,* 3(1), 26-33.

Aiken, K. D., & Bousch, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context specific nature of internet signals. *Journal of the Academy of Marketing Science*, 34, 308–323.

AlAwadhi, S. & Morris, A. (2008). The use of the UTAUT model in the adoption of e-government services in Kuwait. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. Retrieved from http://www.computer.org/portal/web/csdl/doi/10. 1109/ HICSS.2008.452.

AlAwadhi, S. & Morris, A. (2009). Factors influencing the adoption of e-government services. *Journal of Software*, 4(6), 584-590.

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.

Andersen, K.V. & Henriksen, H.Z. (2006). E-government maturity models: Extension of the Layne and Lee model. *Government Information Quarterly*, 23, 236-248.

Anderson, J.C. & Gerbing, D.W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103(3), 411-423.

Anderson, M. (1971). Family structure in the 19th century Lancashire. Cambridge, UK: Cambridge University Press.

Andrade, E.B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of policy, reward, and company reputation. *Advances in Consumer Research*, 29, 350-353.

Araujo, I. (2005). Privacy mechanisms supporting the building of trust in e-commerce. In *Proceedings of the 21st International Conference on Data Engineering, Tokyo, Japan*. Retrieved from http://www.computer.org/portal/web/csdl/doi/10.1109/ICDE.2005. 263.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a Web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review,* 31(5), 661-681.

Arnoldi, J. (2009). *Risk: An introduction*. Cambridge, UK: Polity Press.

Article 29 Data Protection Working Party (2004). *WP 100 - opinion on more harmonized information provisions*. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

Ashworth, L. & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics,* 67, 107-123.

Atkin, C. (1973). Instrumental utilities and information seeking. In P. Clarke (Ed.), *New models for mass communication research* (pp. 205-239). Beverly Hills, CA: Sage Publications, Inc.

Bachmann, R. (1998). Conclusion: Trust – conceptual aspects of a complex phenomenon. In C. Lane & R. Bachmann (Eds.), *Trust within and between organizations* (pp. 298–322). Oxford, UK: Oxford University Press.

Barber, B. (1983). *The logic and limits of trust*. New Brunswick, NJ: Rutgers University Press.

Barrett, P. (2007). Structural equation modeling: Adjudging model fit. *Personality and Individual Differences*, 42, 815–824.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, 69, 133–152.

Bauer, R.A. (1960). Consumer behavior as risk taking. In D.F. Cox (Ed.), *Risk taking and information handling in consumer behavior* (pp. 389-398). Cambridge, MA: Harvard University Press.

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security*, 23, 400−412.

Belanger, F. & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information* Systems, 17, 165–176.

Belanger, B., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems,* 11, 245–270.

Beldad, A., De Jong, M., & Steehouder, M. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites. *Government Information Quarterly*, 26(4), 559–566.

Beldad, A., De Jong, M., & Steehouder, M. (2010). Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. *Government Information Quarterly*, 27(3), 238-244.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International differences in information privacy concerns: a global survey of consumers. *The Information Society,* 20, 313-324.

Berendt, B., Gunther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM,* 48, 101-106.

Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, reciprocity, and social history. *Games and Economic Behavior*, 10, 122–142.

Berger, C.R. (1986). Uncertain outcome values in predicted relationships: Uncertainty reduction theory then and now. *Human Communication Research,* 13(1),34-38.

Berger, C.R. & Calabrese, R.J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research,* 1, 99-112.

Bergkamp, L. (2002). The privacy fallacy: Adverse effects of Europe's data-protection policy in an information-driven economy. *Computer Law & Security Report*, 18(1), 31−47.

Blakemore, M., McDonald, N., Hall, N., & Jucuite, R. (2010). Delivering citizen-centric public services through technology-facilitated change. In P.G. Nixon, V.N. Koutrakou, & R. Rawal (eds.), *Understanding e-government in Europe* (pp. 19-37). Oxon, UK: Routledge.

Blau, P.M. (1964). *Exchange and power in social life*. New York, NY: John Wiley & Sons, Inc.

Blunch, N.J. (2008). *Introduction to structural equation modeling using SPSS and AMOS*. Thousand Oaks, CA: Sage Publications, Inc.

Bolchini, D., He, Q., Anton, A. I., & Stufflebeam, W. (2004). 'I need it now': Improving website usability by contextualizing privacy policies. In N. Koch, P. Fraternali, & M. Wirsing (Eds.), *ICWE 2004, LCNS 3140* (pp. 31−44). Heidelberg, DE: Springer- Verlag.

Borking, J.J. & Raab, C.D. (2001). Laws, PETs, and other technologies for privacy protection. *Journal of Information, Law, and Technology*, 1. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking.

Boyd, J. (2003). The rhetorical construction of trust online. *Communication Theory*, 13(4), 392–410.

Brashers, D.E. (2001). Communication and uncertainty management. *Journal of Communication,* 51(3), 477-497.

Breakwell, G.M. (2007). *The psychology of risk*. Cambridge, UK: Cambridge University Press.

Brey, P. (2007). Ethical aspects of information security and privacy. In M. Petrovic & W. Jonker (Eds.), *Security, privacy, and trust in modern data management* (pp. 21-36). Berlin-Heidelberg, DE: Springer-Verlag.

Briggs, P., Simpson, B., & De Angeli, A. (2004). Personalisation and trust: A reciprocal relationship? In C. M. Karat, J. O. Blom, & J. Karat (Eds.), *Designing personalized user experiences in e-commerce* (pp. 39–55). Netherlands: Kluwer.

Buskens, V. (1998). The social structure of trust. *Social Networks*, 20, 265–289.

Buttner, O.B. & Goritz, A.S. (2008). Perceived trustworthiness of online shops. *Journal of Consumer Behavior*, 7, 35-50.

Byrne, B.M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. New York, NY: Routledge.

Capgemeni, Rand Europe, IDC, Sogeti, & Dti (2009). *8th e-government benchmark measurement*. EU: European Commission, Directorate General for Information Society and Media.

Carter, L. & Belanger, F. (2004). Citizen adoption of electronic government initiatives. In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*. Retrieved from http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2004.1265306.

Carter, L. & Belanger, F. (2004). The influence of perceived characteristics of innovating on e-government adoption. *Electronic Journal of e-Government*, 2(1), 11-20. Retrieved from http://www.ejeg.com/volume2/issue1.

Carter, L. & Belanger, F. (2005). The utilization of e-government services: citizen trust, innovation, and acceptance factors. *Information Systems Journal*, 15, 5-25.

Casalo, L. V., Flavian, C., & Guinaliu, M. (2007). The influence of satisfaction, perceived reputation and trust on a consumer's commitment to a website. *Journal of Marketing Communications*, 13(1), 1–17.

Castaneda, J.A. & Montoro, F.J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research,* 7, 117-141.

Chadwick-Jones, J. K. (1976). *Social exchange theory: Its structure and influence in social psychology*. London, UK: Academic Press, Inc.

Chau, P. Y. K., Hu, P. J. H., Lee, B. L. P., & Au, A. K. K. (2007). Examining customers' trust in online vendors and their dropout decisions: An empirical study. *Electronic Commerce Research and Applications*, 6, 171–182.

Chellapa, R.K. & Sin, R.G. (2005). Personalization versus privacy: An empirical examination of the online consumers' dilemma. *Information Technology and Management,* 6, 181-202.

Chen, C. (2006). Identifying significant factors influencing consumer trust in an online travel site. *Information Technology and Tourism*, 8, 197–214.

Chen, R. & He, F. (2003). Examination of brand knowledge, perceived risk and consumers' intention to adopt an online retailer. *Total Quality Management & Business Excellence*, 14(6), 677-693.

Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in ecommerce. *Information Technology and Management*, 4, 303–318.

Cheung, M. K., & Lee, M. K. O. (2006). Understanding consumer trust in Internet shopping: A multidisciplinary approach. *Journal of the American Society for Information Science and Technology*, 57(4), 479–492.

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society,* 11(3), 395−416.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior,* 12(3), 341-345.

Clark, R. (1997). Introduction to dataveillance and information privacy, and definition of terms. Retrieved from http://www.rogerclarke.com/DV/Intro.html.

Coleman, J. S. (1990). *Foundations of social theory*. Cambridge, MA: Harvard University Press.

Colesca, S.E. (2009). Increasing e-trust: A solution to minimize risk in e-government adoption. *Journal of Applied Quantitative Methods*, 4(1), 31-44.

Colesca, S.E. & Dobrica, L. (2008). Adoption and use of e-government services: The case of Romania. *Journal of Applied Research and Technology*, 6(3), 204-216.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, 2, 203–215.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). Online trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58, 737–758.

Cullen, R. (2008). Citizens' concerns about the privacy of personal information held by government: A comparative study, Japan and New Zealand. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, *Waikoloa, HI*. doi: 10.1109/HICSS.2008.91

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

Currall, S. C., & Judge, T. A. (1995). Measuring trust between organizational boundary role persons. *Organizational Behavior and Human Decision Processes*, 64(2), 151–170.

Cyr, D., Hassanein, K., Head, M., & Ivanov, A. (2007). The role of social presence in establishing loyalty in e-service environments. *Interacting with Computers*, 19, 43–56.

Das, T. K., & Teng, B. S. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology*, 19(1), 85–116.

Dashti, A., Benbasat, I., & Burton-Jnes, A. (2009). Developing trust reciprocity in electronic government: The role of felt trust. In *Proceedings of the European and Mediterranean Conference on Information Systems*, Izmir, Turkey. Retrieved from http://www.iseing.org/emcis/CDROM%20Proceedings%20Refereed%20Papers/Proceedings/Presenting%20Papers/C16/C16.pdf.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

Debussere, F. (2005). The EU e-privacy directive: A monstrous attempt to starve the cookie monster? *International Journal of Law and Information Technology*, 13(1), 70−97.

DeCew, J.W. (1997). *In pursuit of privacy – law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Denney, D. (2005). *Risk and society*. Thousand Oaks, CA: Sage Publications.

DeVellis, F.F. (2003). *Scale development: Theory and applications* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Diffie, W. & Landau, S. (1998). *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: The MIT Press.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of Marketing*, 61, 35–51.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review*, 23(3), 601–620.

Dutch Data Protection Authority (2007). Dutch DPA guidelines – Publication of personal data on the Internet. Retrieved from http://www.dutchdpa.nl/downloads_overig/en_20071108_ richtsnoeren_internet.pdf?refer=true&them=purple.

Dutton, W.H. (2010). The fifth estate: Democratic social accountability through the emerging network of networks. In P.G. Nixon, V.N. Koutrakou, & R. Rawal (eds.), *Understanding e-government in Europe* (pp. 3-18). Oxon, UK: Routledge.

Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W.H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-236.

Earp, J.B. & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM,* 46(4), 81-83.

Elgesem, D. (1999). The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. *Ethics and Information Technology*, 1, 283−293.

Emerson, R.M. (1987). Toward a theory of value in social exchange. In K.S. Cook (Ed.), *Social exchange theory* (pp. 11-46). Newbury Park, CA: Sage Publications, Inc.

European Commission (2008). Eleventh Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries. Retrieved from http://ec.europa.eu/justice_home/fsj/ privacy/ docs/wpdocs/2008/11th_annual_report_en.pdf.

European Union (1995a). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/ docs/95-46-ce/dir1995-46_part1_en.pdf.

European Union (1995b). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/ docs/95-46-ce/dir1995-46_part2_en.pdf.

European Union (2002). Directive 2002/58 EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Retrieved from http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_ 20120020731en00370047.pdf.

Everard, A. & Galleta, D.R. (2005). How presentation flaws affect perceived site quality, trust, and intention purchase from an online store. *Journal of Management Information Systems*, 22(3), 55-95.

Fairweather, N.B. & Rogerson, S. (2006). Towards morally defensible e-government interactions with citizens. *Information, Communication, & Ethics in Society*, 4, 173-180.

Featherman, M. & Pavlou, P.A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59, 451-474.

Featherman, M.S. & Wells, J.D. (2004). The intangibility of E-services: effects on artificiality, perceived risk, and adoption. In *Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii*. Retrieved fromhttp://www.computer.org/portal/web/csdl/doi?doc=doi/10.1109/HICSS.2004.1265424.

Fernback, J., & Papacharissi, Z. (2007). Online privacy as legal safeguard: The relationship among consumer, online portal, and privacy policies. *New Media and Society*, 9(5), 715–734.

Flavian, C., Guinaliu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction, and consumer trust on website loyalty. *Information & Management*, 43, 1–14.

Fogg, B.J., Soohoo, C., Danielson, D.R., Marable, L., Stanford, J., and Tauber, E.R. (2003). How Do Users Evaluate the Credibility of Websites? A Study with over 2,500 Participants. In *Proceedings of the 2003 Conference on Designing for User Experiences; San Francisco, California*. Retrieved from http://portal.acm.org/citation.cfm?id=997097.

Franzak, F., Pitta, D., & Fritsche, S. (2001). Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing,* 18(7), 631-641.

Fried, C. 1984. Privacy: A moral analysis. In F.D. Schoeman (Ed.), *Philosophical dimensions of privacy: An Anthology* (pp. 203-222). Cambridge, UK: Cambridge University Press.

Friedman, B., Kahn, P.H., & Howe, D.C. (2000). Trust online. *Communications of the ACM*, 43(12), 34-40.

Gallup Organization (2008). Data protection in the European Union: Citizens' perceptions. Analytical report *(A survey requested by Directorate-General Justice, Freedom, & Security)*. Retrieved from http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing*, 58, 1-19.

Gefen, D. (2000). E-commerce: The roles of familiarity and trust. *Omega*, 28, 725–737.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services. *Omega*, 32, 407–424.

Gefen, D., Warkentin, M., Pavlou, P.A., & Rose, G.M. (2002). E-government adoption. *AMCIS 2002 Proceedings. Paper 8*3. Retrieved from http://aisel.aisnet.org/amcis2002/83.

Germanakos, P., Christodoulou, El. & Samaras, G. (2007). A European perspective of e-government presence – Where do we stand? The EU-10 case. In M.A. Wimmer, H.J. Scholl, & A. Gronlund (Eds.), *EGOV 2007, LNCS 4656* (pp. 436-447). Berlin-Heidelberg: Springer-Verlag.

Gilbert, D., Balestrini, P., & Littleboy, D. (2004). Barriers and benefits in the adoption of e-government. *The International Journal of Public Sector Management*, 17(4), 286-301.

Goffman, I. (1959). *The presentation of self in everyday life*. London, UK: The Penguin Press.

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. *Journal of Business Ethics*, 39, 43–50.

Grazioli, S. & Jarvenpaa, S.L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, 30(4), 395-410.

Ha, V., Al Shaar, F., Inkpen, K., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. In *Conference on Human Factors in Computing Systems, Montreal, Canada*. Retrieved from http://portal.acm.org/citation.cfm?id=1125615.

Haas, D. F., & Deseran, F. A. (1981). Trust and symbolic exchange. *Social Psychology Quarterly*, 44(1), 3–13.

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

Hardin, R. (1991). Trusting persons, trusting institutions. In R. J. Zeckhauser (Ed.), *Strategy and choice* (pp. 185–209). Cambridge, MA: The MIT Press.

Hassanein, K., & Head, M. (2004). Instilling social presence through the web interface. In *Proceedings of the third annual workshop on HCI research in MIS, Washington, DC*. Retrieved from http://sighci.org/Research/ICIS2004/SIGHCI_2004_Proceedings_paper_9.pdf.

Heath, R.L. & Bryant, J. (2000). *Human communication theory and research* (2nd edition). Mahwah, NJ: Lawrence Erlbaum Associates.

Henderson, S.C. & Snyder, C.A. (1999). Personal information privacy: Implications for MIS managers. *Information and Management,* 36, 213-220.

Herbig, P., Milewicz, J. & Golden, J. (1994). A model of reputation building and destruction. *Journal of Business Research,* 31, 23-31.

Herrero Crespo, A., Rodriguez del Bosque, I., Garcia de los Salmones Sanchez, M.M. (2003). The influence of perceived risk on Internet shopping behavior: A multidimensional perspective. *Journal of Risk Research*, 12(2), 259-277.

Hinton, P.R. (2008). *Statistics explained* (2nd ed.). East Sussex, UK: Routledge.

Hoffman, D. L., Novak, T. P., & Peralta, M.A. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80–85.

Hoffman, D.L., Novak, T.P., & Peralta, M.A. (1999). Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web. *The Information Society,* 15, 129-139.

Homans, G. (1958). Social behavior as exchange. *The American Journal of Sociology,* 63(6), 597-606.

Homans, G. (1961). *Social behavior: Its elementary forms*. London, UK: Routledge & Kegan Paul Ltd.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception, and trust as determinants of adoption of e-government services in the Netherlands. *Computers in Human Behavior*, 23, 1838–1852.

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review*, 20(2), 379–403.

Howitt, D. & Cramer, D. (2005). *Introduction to SPSS in psychology* (3rd ed). Essex, England: Pearson Education Limited.

Hoyle, R.H. & Panter, A.T. (1995). Writing about structural equation models. In R.H. Hoyle (Ed.), *Structural equation modeling: concepts, issues, and applications* (pp. 158-176). Thousand Oaks, CA: Sage Publications.

Hu, L. & Bentler, P.M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 6(1), 1-55.

Huff, L. & Kelley, L. (2003). Levels of organizational trust in individualist versus collectivist societies: A seven-nation study. *Organization Science*, 14(1), 81-90.

Huff, L. & Kelley, L. (2005). Is collectivism a liability? The impact of culture on organizational trust and customer orientation: A seven-nation study. *Journal of Business Research*, 58, 96-102.

Hung, S.Y., Chang, C.M., & Yu, T.J. (2006). Determinants of user acceptance of the e-government services: The case of online tax filing and payment system. *Government Information Quarterly*, 23, 97-122.

Jaeger, P.T. (2003). The endless wire: E-government as global phenomenon. *Government Information Quarterly*, 20, 323-331.

James, H. S. (2002). The trust paradox: A survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, 47, 291–307.

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). Retrieved from http://jcmc.indiana.edu/vol5/ issue2/ jarvenpaa.html.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management*, 1, 45–71.

Jensen, C. & Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI*

conference on Human factors in computing systems, *Vienna, Austria*. Retrieved http://portal.acm.org/citation.cfm?id=985752.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies,* 63, 203-227.

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *The Academy of Management Review*, 23(3), 531–546.

Jorgensen, D.J. & Cable, S. (2002). Facing the challenges of e-government: A case study of the city of Corpus Christi, Texas. *SAM Advanced Management Journal*, 67(3), 15-21.

Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43, 618–644.

Kaiser, H.F. (1974). An index of factorial simplicity. *Psychometrika,* 39(1), 31-36.

Karvonen, K. (2000). The beauty of simplicity. In *Proceedings on the 2000 Conference on Universal Usability, Arlington, VA*. Retrieved from http://portal.acm.org/citation.cfm?id=355460.355478.

Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological consideration in the study of trust and suspicion. *Journal of Conflict Resolution*, 14(3), 357–366.

Keh, H.T. & Xie, Y. (2009). Corporate reputation and behavioral intentions: The roles of trust, identification, and commitment. *Industrial Marketing Management*, 39, 732-742.

Kierkegaard, S. M. (2005). How the cookies (almost crumbled): Privacy & lobbyism. *Computer Law & Security Report*, 21, 310−322.

Kim, D.J., Ferrin, D.L. & Rao, H.R. (2003). A study of the effect of consumer trust on consumer expectations and satisfaction: The Korean experience. In *Proceedings of the 5th International Conference on Electronic Commerce, Pittsburg, PA*. Retrieved from http://portal.acm.org/citation.cfm?id=948005.948046.

Kim, D., Ferrin, D., & Rao, R. (2003). An investigation of consumer online trust and purchase-repurchase intentions. In *Proceeding of the International Conference on Information Systems*. Retrieved from http://aisel.aisnet.org/icis2003/30.

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, 544–564.

Kim, D. J., Song, Y. I., Braynoy, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: A conceptual framework and content analyses of academia/practitioner perspectives. *Decision Support Systems*, 40, 143–165.

Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces: Trustworthiness of cyber-banking system interfaces. *Interacting with Computers*, 10, 1–29.

Kim, Y.H. & Kim, D.J. (2005). A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI*. Retrieved from http://www.computer.org/portal/web/csdl/abs/proceedings/hicss/2005/2268/07/22680170cabs.htm

Kimery, K. M., & McCord, M. (2002). Third party assurances: The road to trust in online retailing. In *Proceedings of the 35th Hawaii international conference on system sciences, Hawaii*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=994158&tag=1.

Kipnis, D. (1996). Trust and technology. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 39–50). Thousand Oaks, CA: Sage Publications Inc.

Kline, R.B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York, NY: The Guilford Press.

Kobsa, A. (2007). Privacy-enhanced personalization. *Communications of the ACM,* 50(8), 24-33.

Koehn, D. (2003). The nature of and conditions for online trust. *Journal of Business Ethics*, 43, 3–19.

Koller, M. (1988). Risk as a determinant of trust. *Basic and Applied Social Psychology*, 9(4), 265–276.

Koufaris, M. & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management,* 41, 377-397.

Kuan, H. H., & Bock, G. W. (2007). Trust transference in brick and click retailers: An investigation of the before-online-visit phase. *Information & Management*, 44, 175–187.

Kumar, V., Mukerji, B., Butt, I., & Persaud, A. (2007). Factors for successful e-government adoption: A conceptual framework. *The Electronic Journal of e-Government*, 5(1), 63-76. Retrieved from http://www.ejeg.com/volume5/issue1.

Lahno, B. (2004). The three aspects of interpersonal trust. *Analyse & Kritik*, 26, 30-47.

Lane, C. (1998). Introduction: Theories and issues in the study of trust. In C. Lane & R. Bachmann (Eds.), *Trust within and between organizations* (pp. 31–63). Oxford: Oxford University Press.

LaRose, R., & Rifon, N.J. (2006). Your privacy is assured—of being disturbed: Websites with or without privacy seals. *New Media & Society*, 8(6), 1009−1029.

LaRose, R. & Rifon, N.J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs,* 41(1), 127-149.

Lau, T.Y., Aboulhoson, M., Lin, C., & Atkin, D.J. (2008). Adoption of e-government in three Latin American countries: Argentina, Brazil, and Mexico. *Telecommunications Policy*, 32, 88-100.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, 6, 323–331.

Laufer, R.S. & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33(3), 22-42.

Lee, H.Y., Ahn, H., & Han, I. (2006). Analysis of trust in the e-commerce adoption. In *Proceedings of the 39th Hawaii International Conference on System Sciences*. Retrieved from http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2006.61.

Lee, M. K. O., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce*, 6(1), 75–91.

Lenk, K. & Traunmueller, R. (2007). Broadening the concept of electronic government. In J.E.J. Prins (Ed.), *Designing E-Government* (pp. 9-18). Alphen aan den Rijn, NL: Kluwer Law International.

Lewicki, R., & Bunker, B. (1996). Developing and maintaining trust in work relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in Organizations: Frontiers of Theory and Research* (pp. 114–139). Thousand Oaks, CA: Sage Publications, Inc.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, 63(4), 967–985.

Liao, C., Palvia, P., & Lin, H. N. (2006). The roles of habit and website quality in ecommerce. *International Journal of Information Management*, 26, 469–483.

Lichenstein, S., Swatman, P., & Babu, K. (2003). Adding value to online privacy for consumers: remedying deficiencies in online privacy policies with an holistic approach. In *Proceedings of the 36th International Conference on System Science, Victoria, Australia*. doi: 10.1109/HICSS.2003.1174470.

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications*, 2(3), 216-228.

Litter, D. & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking. *Journal of Retailing and Consumer Services,* 13, 431–443.

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

Liu, X. & Wei, K.K. (2003). An empirical study of product differences in consumers' E-commerce adoption behavior. *Electronic Commerce Research and Application*, 2, 229-239.

Lohse, G. L., & Spiller, P. (1998). Electronic shopping. *Communications of the ACM*, 41(7), 81–87.

Luhmann, N. (1979). *Trust and power*. Chichester: John Wiley.

Lupton, D. (1999). *Risk*. London, UK: Routledge.

Lwin, M.O. & Williams, J.D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters,* 14(4), 257-272.

MacCrimmon, K.R. & Wehrung, D.A. (1986). *Taking risks: The management of*

uncertainty. New York, NY: The Free Press.
Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
Marcella, A. J. (1999). *Establishing trust in vertical markets*. Altamonte Springs, FL: The Institute of Internal Auditors.
Marchionni, G. (1995) *Information seeking in electronic environments*. Melbourne, AUS: Cambridge University Press.
Markel, M. (2005). The rhetoric of misdirection in corporate privacy-policy statements. *Technical Communication Quarterly*, 14(2), 197−214.
Markel, M. (2006). Safe harbor and privacy protection: A looming issue for IT professionals. *IEEE Transactions of Professional Communication*, 49(1), 1−11.
Markland, D. (2007). The golden rule is that there are no golden rules: A commentary on Paul Barrett's recommendations for reporting model fit in structural equation modeling. *Personality and Individual Differences*, 42, 851–858.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organization trust. *Academy of Management Review*, 20(3), 709–734.
McLain, D.L. & Hackman, K. (1999). Trust, risk, and decision-making in organizational change. Public Administration Quarterly, 23(2), 152.176.
McDonagh, M. (2002). E-government in Australia: The challenge to privacy of personal information. *International Journal of Law and Information Technology*, 10(3), 327-343.
McKnight, D. H., & Chervany, N. L. (2002). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), 35–59.
McKnight, D.H., Choudhoury, H. & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems,* 11, 297-323.
McKnight, D.H., Cummings, L. & Chervany, N.L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review,* 23(3), 473-490.
Meinert, D.B., Peterson, D.K., Criswell, J.R., & Crossland, M.D. (2004). Would regulation of website privacy policy statements increase consumer trust? *Informing Science Journal* ,9, 123-142.
Meinert, D.B., Peterson, D.K., Criswell, J.R., & Crossland, M.D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations*, 4(1), 1−17.
Mellor, D.H. (2007). Acting under uncertainty. In T. Lewens (Ed.), *Risk: Philosophical perspectives* (pp.113-130). Oxford, UK: Routledge.
Meztger, M.J. (2004). Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* 9(4). Retrieved from http://jcmc.indiana.edu/vol9/issue4/metzger. html.
Metzger, M.J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, 33(3), 155–179.

Metzger, M.J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication,* 12, 335-361.

Milberg, S.J., Smith, H.J., & Burke, S.J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, 11(1), 35-57.

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.

Milne, G.R., Rohm, A.J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs,* 38(2), 217-232.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35(1), 27−43.

Miyazaki, A.D. & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *The Journal of Consumer Affairs,* 36(1), 28-49.

Mollering, G. (2006). Trust, institutions, agency: Towards a neoinstitutional theory of trust. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (pp. 355–376). Cheltenham: Edward Elgar.

Molm, L. D., Takahashi, N., & Peterson, G. (2000). Risk and trust in social exchange. An experimental test of a classical proposition. *American Journal of Sociology*, 105(5), 1396–1427.

Moor, J.H. (1991). The ethics of privacy protection. *Library Trends,* 39(1-2),69-82.

Moor, J.H. (1997). Towards a theory of privacy in the information age. *Computers and Society,* 27(3), 27-32.

Muir, A. & Oppenheim, C. (2002). National information policy developments worldwide I: Electronic government. *Journal of Information Science*, 28 (3), 173-186.

Mullen, H. & Horner, D.S. (2004). Ethical problems for e-government: an evaluative framework. *Electronic Journal of e-Government*, 2(3), 187-196. Retrieved from http://www.ejeg.com/volume2/issue3.

Myerscough, S., Lowe, B., & Alpert, F. (2006). Willingness to provide information online: The role of perceived risk, privacy statements, and brand strength. *Journal of Website Promotion*, 2(1/2), 115-140.

Nehf, J.P. (2007). Shopping for privacy on the Internet. *The Journal of Consumer Affairs,* 41(2), 351-365.

Newell, P.B. (1995). Perspectives on privacy. *Journal of Environmental Psychology,* 15, 87-104.

Norberg, P.A. & Dholakia, R.R. (2004). Customization, information provision and choice: What are we willing to give up for personal service? *Telematics and Informatics,* 21, 143-155.

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

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy,* 17(5-6), 559-596.

O'Connor, P. (2008). An international comparison of approaches to online privacy protection: Implications for the hotel sector. *Journal of Services Research*, 6, 7−26.

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, 243-262.

Ommen, I. & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, & J. Borking (Eds.), *Policies and research in identity management* (pp. 121-138). Boston, MA: Springer.

O'Neil, D. (2001). Analysis of internet users' level of online privacy concerns. *Social Science Computer Review*, 19(1), 17−31.

Organization for Economic Cooperation and Development. (2002). *OECD guidelines on the protection of privacy and transborder flows of personal data*. Paris, FR: OECD.

Paine, C., Reips, UD., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies,* 65, 526-536.

Pan, Y. & Zinkhan, G.M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing,* 82(4), 331-338.

Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media*, 49 (3), 259−281.

Pavlou, P. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 17(3), 101–134.

Pavlou, P.A. & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37-59.

Pedersen, D.M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology,* 17, 147-156.

Petronio, S. (2007). Translational research endeavors and the practices of communication privacy management. *Journal of Applied Communication Research,* 35(3), 218-222.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York, NY: Springer-Verlag.

Phelps, J.E., D'Souza, G.D., & Nowak, G.J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.

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.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power, and informed consent. *Journal of Business Ethics*, 62, 221−235.

Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM,* 50(9), 103−108.

Posner, R.A. (1984). An economic theory of privacy. In F.D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 333-345). Cambridge, UK: Cambridge University Press.

Raiha, K. J., & Ovaska, S. (2009). Faces of privacy: Effect of culture and context. In T. Gross (Ed.), *INTERACT 2009, Part 1, LNCS 5726* (pp. 700−703). Berlin, DE: Springer.

Ranganathan, C., Goode, V., & Ramaprasad, A. (2003). Managing the transition to bricks and clicks. *Communications of the ACM*, 46(12), 308–316.

Reagle, J. & Cranor, L.F. (1997). The platform for privacy preferences. *Communications of the ACM,* 42(2), 48-55.

Regan, P. (2008). Privacy in an electronic government context. In H. Chen, L. Brandt, V. Gregg, R. Traunmueller, S. Dawes, E. Hovy, A. Macintosh, & C.A. Larson (Eds.), *Digital government: E-government research, case studies, and implementation* (pp. 127-139). New York, NY: Springer.

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation systems. *Communications of the ACM*, 43(12), 45–48.

Rezgui, A., Bouguettaya, A., & Eltoweissy, M.Y. (2003). Privacy on the web: Facts, challenges, and solutions. *IEEE Security and Privacy,* 1(6), 40-49.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *Journal of Strategic Information Systems*, 11, 271–295.

Riegelsberger, J., & Sasse, M. A. (2002). Face it – Photos don't make a web site trustworthy. In *Conference on Human Factors in Computing Systems*, *Minneapolis, MN*. Retrieved from http://portal.acm.org/citation.cfm?id=506575

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2003). Shiny happy people building trust? Photos on e-commerce websites and consumer trust. In *Conference on Human Factors in Computing Systems*, *Ft. Lauderdale, FL.* Retrieved from http://portal.acm.org/citation.cfm?id=642611.642634.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology,* 91, 93-114.

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.T. Cacioppo & R.E. Petty (Eds.), *Social psychophysiology* (pp. 153-174). Park Avenue South, NY: The Guilford Press.

Rose, W.R. & Grant, G.G. (2010). Critical issues pertaining to the planning and implementation of e-government initiatives. *Government Information Quarterly*, 27, 26-33.

Rothstein, B. & Eek, D. (2009). Political corruption and social trust: An experimental approach. *Rationality and Society*, 21(1), 81-112.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35(4), 651–665.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist*, 26, 443–452.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1), 1–7.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404.

Rowe, W.D. (1977). *The anatomy of risk*. New York, NY: John Wiley & Sons.

Ruyter, K., Wetzels, M., & Kleijnen, M. (2000). Customer adoption of e-service: An experimental study. *International Journal of Service Industry Management*, 12(2), 184-207.

Salam, A. F., Iyer, L., Palvia, P., & Singh, R. (2005). Trust in e-commerce. *Communications of the ACM*, 48(2), 73–77.

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.

Schaupp, L.C. & Carter, L. (2010). The impact of trust, risk, and optimism bias on e-file adoption. *Information Systems Frontier*, 12(3), 299-309.

Schimke, D., Stoeger, H., & Ziegler, A. (2007). The relationship between social presence and group identification within online communities and its impact on the success of online communities. In D. Schuler (Ed.), *Online communities and social concept, HCII2007, LNCS 4564* (pp. 160–168). Heidelberg: Springer-Verlag.

Schoenbachler, D.D. & Gordon, G.L. (2002). Trust and customer willingness to provide information in a database-driven relationship marketing. *Journal of Interactive Marketing,* 16(3), 2-16.

Schreiber, J.B., Stage, F.K., King, J., Nora, A., & Barlow, E.A. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research*, 99(6), 323-337.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management*, 43, 805−820.

Schwester, R.W. (2009). Examining the barriers to e-government adoption. *Electronic Journal of e-Government*, 7(1), 113-122. Retrieved from http://www.ejeg.com/volume7/issue1.

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *Journal of Strategic Information Systems*, 11, 325–344.

Sharma, S.K. & Gupta, J.N.D. (2003). Building blocks of an e-government – A framework. *Journal of Electronic Commerce in Organizations*, 1(4), 34-48.

Sheehan, K.B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4), 24-38.

Sheehan, K.B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society,* 18, 21-32.

Sheehan, K. B. (2005). In poor health: An assessment of privacy policies at direct-to-consumer websites. *American Marketing Association*, 24(2), 273−283.

Sheehan, K.B. & Hoy, M.G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising,* 28(3), 37-51.

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

Sheppard, B. H., & Sherman, D. M. (1998). The grammars of trust: A model and general implications. *The Academy of Management Review*, 23(3), 422–427.

Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. London, UK: John Wiley & Sons.

Sillence, E., Briggs, P., Fishwick, L., & Harris, P. (2004). Trust and mistrust of online health sites. In *Proceedings of the SIGCHI conference on Human factors in computing systems, Vienna, Austria*. Retrieved from http://portal.acm.org/citation.cfm?id=985776.

Sillence, E., Briggs, P., Harris, P., & Fishwick, L. (2007). Health websites that people can trust – The case of hypertension. *Interacting with Computers*, 19, 32–42.

Simon, H.A. (1955). A behavioural model of rational choice. *The Quarterly Journal of Economics,* 69(1), 99-118.

Simon, H.A. (1972). *Models of bounded rationality: Behavioural economics and business organization* (Vol. 2). Cambridge, MA: The MIT Press.

Smeltzer, L. (1997). The meaning and origin of trust in buyer–seller relationships. *International Journal of Purchasing and Materials Management*, 33(1), 40–48.

Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review,* 154(3), 477-560.

Son, J.Y. & Kim, S.S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly,* 32(3), 503-529.

Srinivasan, S. S., Anderson, R., & Ponnavolu, K. (2002). Customer loyalty in ecommerce: An exploration of its antecedents and consequences. *Journal of Retailing*, 78, 41–50.

Srivastava, S.C. & Teo, T.S.H. (2009). Citizen trust development for e-government adoption and usage: Insights from young adults in Singapore. *Communications of the Association for Information Systems*, 25(31), 360-378.

Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn (Eds.), *Socio-technical and human cognition elements of information systems* (pp. 79-103). London, UK: Idea Group.

Steinbrueck, U., Schaumburg, H., Duda, S., & Krueger, T. (2002). A picture says more than a thousand words – Photographs as trust builders in e-commerce websites. In *CHI '02 extended abstracts on Human factors in computing systems, Minneapolis, MN*. Retrieved from http://portal.acm.org/citation.cfm?id=506443.506578.

Strandburg, K.J. (2006). Social norms, self control, and privacy in the online world. In K.J. Strandburg & D.S. Raicu (Eds.), *Privacy and technologies of*

identity: a cross-disciplinary conversation (pp. 31-53). New York, NY: Springer Science.

Strater, K. & Richter, H. (2007). Examining privacy and disclosure in a social networking community. *ACM International Conference Proceeding Series – Proceedings of the 3rd Symposium on Usable Privacy and Security,* 229, 157-158.

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, 19, 173−192.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge, UK: Cambridge University Press.

Tamara, D. & Hart, P. (2006). An extended privacy calculus model for e-commerce transaction. *Information Systems Research*, 17(1), 61-80.

Tan, C., Benbasat, I., & Cenfetelli, R. T. (2008). Building citizen trust towards e-government services: Do high quality websites matter? In *Proceedings of the 41st Hawaii international conference on system sciences, Waikoloa, HI*. doi: 10.1109/HICSS.2008.80.

Tavani, H.T. (2007). Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22.

Tavani, H.T. (2008). Informational privacy: concepts, theories, and controversies. In K.E. Himma & H.T. Tavani (Eds.), *The handbook of information and computer ethics* (pp. 131-164). Hoboken, NJ: Wiley-Interscience.

Tavani, H.T. & Moor, J.H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. In R.A. Spinello & H.T. Tavani (Eds.), *Readings in cyberethics* (pp. 378-391). Sudbury, MA: Jones and Bartlett Publishers.

Teo, T. S. H., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore, and China. *Omega*, 35, 22–38.

Teo, T.S.H., Srivastava, S.C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems*, 25(3), 99-131.

Theunissen, C. (2007). Contextual issues surrounding portable and interactive technologies within the contemporary and future environment of e-government and informatisation. In J.E.J. Prins (Ed.), *Broadening the concept of electronic government* (pp. 47-67). Alphen aan den Rijn, NL: Kluwer Law International.

Toms, E. G., & Taves, A. R. (2004). Measuring user perceptions of Web site reputation. *Information Processing and Management*, 40, 291–317.

Treiblmaier, H. & Chong, S. (2007). Antecedents of the intention to disclose personal information on the Internet: a review and model extension. In *Proceedings of the Sixth Annual Workshop on HCI Research in MIS, Montreal, Canada*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1002&context=sighci2007.

Tu, C. H. (2002a). The measurement of social presence in an online learning environment. *International Journal of E-Learning*, 1(2), 34–45.

Tu, C. H. (2002b). The relationship between social presence and online privacy. *Internet and Higher Educatio*n, 5, 293–318.

Tu, C. H., & McIsaac, M. (2002). The relationship of social presence and interaction in online classes. *The American Journal of Distance Education*, 16(3), 131–150.

Tullberg, J. (2008). Trust – The importance of trustfulness versus trustworthiness. *The Journal of Socio-Economics*, 37, 2059–2071.

Turner, E.C. & Dasgupta, D. (2003). Privacy on the Web: An examination of user concerns, technology and implications for business organizations and individuals. *Information Systems Management,* 20(1), 8-18.

Tyler, T. R., & Kramer, R. M. (1996). Wither trust? In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 1–15). Thousand Oaks, CA: Sage Publications Inc.

Urban, G., Amyx, C., & Lorenzon, A. (2009). Online trust: State of the art, new frontiers, and research potential. *Journal of Interactive Marketing,* 23, 179-190.

Vail, M.W., Earp, J.B., & Anton, A.I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management,* 55(3), 442-453.

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, 41–48.

Van Dijk, J. (2006). The network society (2nd ed.). London, UK: Sage Publications.

Volkman, R. (2003). Privacy as life, liberty, property. *Ethics and Information Technology,* 5, 199-210.

Vu, K.P., Chambers, V., Garcia, F., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R., & Proctor, R. (2007). How users read and comprehend privacy policies. In M.J. Smith & G. Salvendy (Eds.), *Human interface, Part II* (pp. 802-811). Berlin-Heidelberg: Springer-Verlag.

Vu, K.P.L., Garcia, F.P., Nelson, D., Sulaitis, J., Creekmur, B., Chambers, V., & Proctor, R. (2007). Examining user privacy practices while shopping online: what are users looking for? In M. J. Smith, & G. Salvendy (Eds.), *Human Interface, Part II, HCII 2007* (pp. 792−801). Berlin-Heidelberg: Springer-Verlag.

Walczuch, R., & Lundgren, H. (2004). Psychological antecedents of institution-based consumer trust in e-retailing. *Information & Management*, 42, 159–177.

Wang, H., Lee, M. K. O., & Wang, C. (1999). Consumer privacy concerns about internet marketing. *Communications of the ACM,* 41(3), 63–70.

Wang, X.T., Kruger, D.J., & Wilke, A. (2009). Life history variables and risk-taking propensity. *Evolution and Human Behavior*, 30, 77–84

Warkentin, M., Gefen, D., Pavlou, P.A., & Rose, G.M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets*, 12(3), 157-162.

Warren, S.D. & Brandeis, L.D (1898). The right to privacy. *Harvard Law Review,* 4(5). Retrived from http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Wartofsky, M.W. (1986). Risk, relativism, and rationality. In V.T. Covello, J. Menkes, & J. Mumpower (Eds.), *Risk evaluation and management* (pp. 131-153). New York, NY: Plenum Press.

Weber, J. M., Malhotra, D., & Murnighan, J. K. (2005). Normal acts of irrational trust: Motivated attributions and the trust development process. *Research in Organizational Behavior*, 26, 75–101.

Weckert, J. (2005). Trust in cyberspace. In R.J. Cavalier (Ed.), *The Impact of the Internet on our lives (*pp. 95-117). Albany, NY: State University of New York Press.

Welch, E. W. & Hinnant, C. C. (2002). Internet use, transparency, and interactivity effects on trust in government. In *Proceedings of the 36th Hawaii international conference on system sciences*. doi: 10.1109/HICSS.2003.1174323.

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

Westin, A.F. (1991). *Harris-Equifax consumer privacy survey*. Atlanta, GA: Equifax, Inc.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues,* 59(2), 431−453.

Wheaton, B., Muthen, B., Alwin, D.F., Summers, G.F. (1977). Assessing reliability and stability in panel models. *Sociological Methodology*, 8, 84-136.

Williams, M.D. (2008). E-government adoption in Europe at regional level. Transforming Government: *People, Process, and Policy*, 2(1), 47-59.

Williamson, O.E. (1993). Calculativeness, trust, and economic organization. *Journal of Law and Economics*, 36(1), 453-486.

Worchel, P. (1979). Trust and distrust. In W. G. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 174–187). Belmont, CA: Wadsworth.

Wyld, D.C. (2004). The 3 Ps: The essential elements of a definition of e-government. *Journal of E-Government*, 1(1), 17-22.

Woo, J. (2006). The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media and Society*, 8(6), 949−967.

Xie, E., Teo, HH, & Wan, W. (2006). Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters,* 17, 61-74.

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

Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, 16(2), 47–63.

Youn, S., & Hall, J. (2008). Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior*, 11(6), 763−765.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly*, 17(2), 229–239.

Zhang, Y., Chen, J. Q., & Wen, K. W. (2002). Characteristics of internet users and their privacy concerns. *Journal of Internet Commerce*, 1(2), 1−16.

Zimmer, J.C., Arsal, R.E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management,* 47(2), 115-123.

Zimmer, J.C., Arsal, R.E., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems*, 48, 395–406.

Samenvatting

Evenals de meeste commerciële instellingen zoals banken en winkels, proberen ook overheidsinstellingen hun transacties met burgers online af te wikkelen. Daarbij valt te denken aan online aanvragen van informatie (bestemmingsplannen), persoonlijke documenten (paspoorten) en diensten (uitkeringen). Zulke online transacties met de overheid hebben ongetwijfeld voordelen. Ze kunnen bijvoorbeeld uitgevoerd worden op elk tijdstip en van huis uit. Ze zijn echter alleen mogelijk als de overheid beschikt over de voor de transactie relevante volledige en correcte persoonsgegevens van de aanvrager. Online transacties kunnen alleen plaatsvinden als die persoonlijke gegevens door burgers worden verstrekt.

Aangezien persoonsgegevens waardevolle informatie zijn, is misbruik ervan zeer goed mogelijk. Persoonsgegevens kunnen worden gedeeld met andere partijen of ze kunnen met behulp van geavanceerde technieken illegaal worden ingezien door derden. Het is niet zo verrassend dat het verstrekken van persoonsgegevens wordt gezien als een risico, vooral door degenen die zich zorgen maken over inbreuk op hun privacy. Alom wordt erkend dat risico's en risicoperceptie vertrouwen noodzakelijk maken. Vertrouwen in online transacties en online informatieprivacy zijn de twee centrale thema's die in de verschillende studies van deze dissertatie worden onderzocht.

In hoofdstuk 1 worden de centrale thema's van de dissertatie verkend. Het begrip e-government wordt nader uitgewerkt en de invloed van informatieprivacy en online vertrouwen op de acceptatie van e-government wordt onder de loep genomen. In het eerste hoofdstuk wordt beargumenteerd dat de intentie om e-government te accepteren gelijkgesteld kan worden met de bereidheid van de burger om met de overheidsinstelling online zaken te doen. Aangezien bij vrijwel alle online transacties met de overheid van de burger gevraagd wordt persoonlijke gegevens te verstrekken, kan de intentie om deze te verstrekken ook worden gezien als een uiting van bereidheid van de burger online transacties met de overheid aan te willen gaan. In dit hoofdstuk worden ten slotte de belangrijkste onderzoeksvragen geïntroduceerd, die in de verschillende onderzoeken van deze dissertatie gesteld worden.

Hoofdstuk 2 geeft een in de vorm van een literatuurstudie theoretische verdieping van het concept *informatieprivacy*. Het hoofdstuk begint met een vergelijking van verschillende privacyconcepten uit de literatuur. Het grootste deel van het hoofdstuk bespreekt de verschillende vormen van gedrag ten aanzien van de informatieprivacy, zoals het zoeken naar informatie alvorens een besluit te nemen om al dan niet persoonsgegevens te verstrekken. Verschillende theorieën op het gebied van communicatie, sociale psychologie en sociologie worden gebruikt om dit gedrag ten aanzien van informatieprivacy te verklaren. Zo laat bijvoorbeeld de Social Exchange Theory zien dat mensen bereid zijn persoonlijke gegevens te verstrekken in het kader van een online transactie

als het voordeel van deze transactie opweegt tegen de kosten (of beter gezegd het risico) van het verstrekken van deze gegevens.

In hoofdstuk 3 wordt, eveneens aan de hand van een literatuurstudie, het begrip *vertrouwen* theoretisch verdiept. Benadrukt wordt dat vertrouwen een belangrijke factor is die het menselijke gedrag beïnvloedt, bij het verstrekken van persoonlijke gegevens in een digitale omgeving. Aan de hand van studies, naar de determinanten van vertrouwen in (meestal commerciële) online transacties, beschrijft hoofdstuk 3 de verschillende factoren die het vertrouwen van burgers in online transacties met de overheid kunnen beïnvloeden. Deze factoren worden ondergebracht in de volgende categorieën: factoren die gerelateerd zijn aan de internetgebruikers zelf (neiging om te vertrouwen, internetervaring), factoren gerelateerd aan de inhoud van de website (privacyverklaringen, veiligheidssymbolen), en factoren gerelateerd aan de organisatie (reputatie).

Hoofdstuk 4 doet verslag van gesprekken met drie focusgroepen met in totaal 23 internetgebruikers uit drie Twentse steden. Aan de deelnemers werd gevraagd naar hun ervaringen met en hun zorgen over het gebruik van online diensten van de overheid. De belangrijke theoretische noties uit hoofdstuk 2 en 3 werden gebruikt om de structuur van de gesprekken tijdens deze focusgroepsessies te sturen. Terwijl deelnemers beaamden dat online transacties met de overheid voordeel oplevert, waren ze ook bezorgd over de zekerheid en het slagen van online transacties. Ook waren ze bezorgd over de veiligheid van persoonsgegevens die ze moesten verstrekken. De deelnemers gaven ook aan dat ze verschillende strategieën gebruikten om zich te verzekeren van voldoende online informatieprivacy en verschillende onderdelen van de websites bestudeerden om de betrouwbaarheid van instellingen achter de websites te controleren.

In hoofdstuk 5 wordt verslag gedaan van een online enquête onder 2202 Nederlandse internetgebruikers. Doel van dit onderzoek was te bepalen welke factoren van invloed zijn op de bereidheid om persoonlijke gegevens aan de overheid te verstrekken in het kader van een online transactie. De resultaten laten zien dat met name vertrouwen in de betreffende overheidsinstelling een beslissende factor is, zowel bij mensen met eerdere ervaring met e-government als bij mensen zonder eerdere ervaring. Daarnaast is de bereidheid groter naarmate het risico lager wordt ingeschat, de verwachte voordelen van de transactie hoger worden ingeschat en men meer vertrouwen heeft in de effectiviteit van wettelijke beschermingsmaatregelen. De resultaten laten ook een negatief verband zien tussen vertrouwen en risicoperceptie: vertrouwen van de burger in de overheidsinstelling leidt tot een lagere inschatting van de risico's die het verstrekken van gegevens met zich meebrengt.

Hoofdstuk 6 beschrijft een tweede online enquête onder 1156 Nederlandse internet gebruikers. Hierbij is nader onderzocht welke factoren de risicoperceptie van gegevensverstrekking ten behoeve van online transacties beïnvloeden. De resultaten van deze enquête laten zien

dat het vertrouwen in online privacyverklaringen een positieve invloed heeft op het vertrouwen in de betreffende overheidsinstellingen zelf. Dat geldt zowel voor burgers zonder als met ervaring met overheidstransacties. Onder burgers met ervaring blijkt een positieve ervaring en een positieve reputatie van de overheidsinstelling hun vertrouwen in overheidsinstellingen te doen toenemen.

In hoofdstuk 7 wordt een derde online onderzoek (met 208 internetgebruikers) gerapporteerd, waarin de factoren zijn onderzocht die van invloed zijn op de risicoperceptie bij het online verstrekken van persoonsgegevens. Aan de hand van een fictieve case (het aanmelden van kinderen voor de basisschool via een gemeentelijke website) werd nagegaan welke gegevens als meer of minder gevoelig beschouwd werden, en in hoeverre de gevoeligheid van gevraagde gegevens van invloed was op de risicoperceptie. De resultaten lieten zien dat de risicoperceptie sterk gerelateerd was aan de gevoeligheid van de gegevens en de mate van vertrouwen dat de overheidsinstelling bereid en in staat is de gegevens te beschermen.

Omdat onder meer het onderzoek uit hoofdstuk 6 liet zien dat privacyverklaringen invloed hebben op het vertrouwen van Nederlandse internetgebruikers in overheidsinstellingen, wordt in hoofdstuk 8 een inhoudsanalyse gerapporteerd van privacyverklaringen op 100 gemeentelijke websites Dit onderzoek levert drie belangrijke resultaten op: ten eerste spannen niet alle gemeenten zich in, een privacy verklaring op hun website te plaatsen, ten tweede zijn de verklaringen bij de meeste gemeenten moeilijk te vinden en ten derde doen gemeentelijke websites verschillende beloften: sommige doen recht aan alle alle onderdelen van de Wet Bescherming Persoonsgegevens, terwijl andere slechts algemene en soms vage garanties geven.

Ook hoofdstuk 9 heeft betrekking op privacyverklaringen op overheidswebsites. Hier staat de vraag centraal in hoeverre die gelezen worden voordat burgers besluiten gegevens te verstrekken, en of hun aanwezigheid en vindbaarheid invloed heeft op het vertrouwen van internetgebruikers in de betreffende overheidsinstelling. De data voor dit onderzoek zijn afkomstig uit dezelfde enquête als die uit hoofdstuk 7. De resultaten laten zien dat de aanwezigheid en de vindbaarheid van een privacyverklaring op de website bijdraagt tot een grotere bereidheid tot het verstrekken van persoonsgegevens aan een gemeente, ook als de pricacyverklaring feitelijk niet gelezen wordt. Deze studie laat ook zien dat als gebruikers het riskant vinden, persoonsgegevens aan gemeentelijke websites te verstrekken, hun neiging om de privacy verklaring te lezen toeneemt. Ouderen, lager opgeleiden en mensen met relatief weinig internetervaring rapporteren een relatief hoge neiging om de privacyverklaring te lezen.

Acknowledgment

The road was rough and the ride was grueling, nonetheless the destination has been reached. This has never been a one-man adventure. Names of the many who have contributed to this academic pursuit unquestionably merit recognition and deserve my sincerest thanks.

It all started with Prof. Dr. Michaël Steehouder, my first *promotor*. It was just four years ago when I inquired about his willingness to supervise a PhD project on something that I could barely elaborate way back then. Michaël supervised me when I was writing my master's thesis and the working relationship was intellectually stimulating. The idea, therefore, of Michaël supervising my PhD project was and still is splendid. He was on an educational leave when he, figuratively speaking, opened the seemingly tightly fastened gates to possibilities in the academic/research community. The thought of pursuing a PhD, though exciting, was irrefutably daunting. This dissertation would have not been possible without the assiduous supervision of Michaël, who seems adept in boosting another person's self-confidence in a time when others will do anything to shatter it.

The adventure got off to a promising start with Prof. Dr. Menno de Jong agreeing to be my daily supervisor. Completing this dissertation with Menno as my second *promotor* is just marvelous. While the track that led to this dissertation was oftentimes rugged, Menno always had his door open for a regular talk on how to ease the burden of gathering and analyzing data and on things that go beyond the scope of the PhD project. A crowded calendar of daily activities did not prevent him from listening to my acutely trivial apprehensions. As setbacks and intricacies were inevitably ingrained in the project, Menno had his way of ensuring that those unwarranted elements would not crush the zeal that fuelled me to proceed with what I was and should be doing. In fact, completing this dissertation would have been unthinkable without Menno's unwavering guidance.

For somebody with a restrained network to potential sources of data, completing a survey, no matter how small in scope, for instance, would have been unimaginable. Hans Kits generously helped in collecting the data for the small-scale survey. His communal connections guaranteed that I would have an adequate sample, though not necessarily sizeable, to provide the data for one study. The problem of translating some of the research instruments from English to Dutch was also addressed with his help. His support has been remarkable.

Designing an online survey, the first one conducted during the first phase of this PhD project, would have been tremendously arduous without the help of Johan Jonker. Johan spent significant amount of time providing me with a 'crash course' on Dreamweaver, InDesign, and Photoshop. Johan was also very kind to assist in collecting some data for the small-scale survey. It is always a pleasure to visit his office and just talk about a variety of things ranging from photography to holiday trips.

Johan and Marc Draijer, a good colleague within the group 'communication skills', also deserve my sincerest thanks for their willingness to stand as my *paranimfen* (I could not think of an English equivalent for the word) during the defense of this dissertation.

Furthermore, I am grateful to the five members of the graduation committee who invested immeasurable amount of time and effort in reading this dissertation: Prof. Dr. Jan van Dijk, Prof. Dr. Ronald Leenes, Prof. Dr. Cees Midden, Prof. Dr. Philip Brey, and Prof. Dr. Leo Lentz.

Along the way, I was also involved in an external research project on Citizens' Trust in Dutch e-Government and DigiD, which was subsidized by *Alliantie Vitaal Bestuur*. For this particular project, I had the chance to work with Thea van der Geest, who also contributed substantially to this PhD project. It was certainly a good learning experience to work with somebody who immerses herself in understanding the nature of and the dynamics involved in the interaction between citizens and the government in the online environment.

I am also taking this opportunity to thank a number of people who had been, in different ways, significantly instrumental in the completion of the aforementioned research project: Mildo van Staden and Tanja Timmerman of the Ministry of the Interior and Kingdom Relations of the Netherlands; Xander Linde and Odette Vlek of Ruigrok NetPanel; Ineke Willighagen of the Gemeente Zwolle.

Since this PhD project was implemented within the Department of Technical and Professional Communication (under the leadership of Michael, and then Menno), my colleagues in TPC certainly deserve my thanks, too. Thanks to Emmy Cheret for the assistance during the hectic period when I was completing the final version of the dissertation. Marita Wesselink was also very helpful when I was confronted with the complication of working with a couple of design software.

A number of marvelous individuals also merit my acknowledgment: Emiel Reimerink, Jan and Riet de Bruin, Adel Agina, and the late Lize Kits. Furthermore, members of ROC van Twente, Nivon, and Stichting Natuur- en Milieuraad had been generous with their time by participating in the small-scale online survey.

I owe a great deal to Reinhard Walterbach for the encouragement even before I thought of pursuing this project. *Vielen Dank!*

In memory of my father and mother.

Ad Majorem Dei Gloriam

About the author

Ardion Beldad currently lectures at the University of Twente, the Netherlands. He previously worked for a research project on trust in Dutch e-government and DigiD (an electronic authentication system Dutch citizens use to access the many services offered by most Dutch government organizations in the online environment).

Beldad received his Bachelor of Science in Development Communication, specializing in Development Journalism, from Xavier University, the Philippines, in 1998. He also pursued graduate studies in sociology in the same university. Prior to his decision to leave for the Netherlands, he taught courses in mass communication and sociology in a Catholic college in the Philippines.

In 2006, he obtained his Master of Science in Communication Studies (*cum laude*) from the University of Twente, with a thesis on misunderstanding and non-understanding in the usage of English as a common language in helpdesk encounters involving non-native speakers. Two years later, he started a PhD project on trust and information privacy concerns in Dutch e-government, which culminated to this dissertation.