Government Information Quarterly 29 (2012) 41–49

Contents lists available at SciVerse ScienceDirect

Government Information Quarterly

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

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

Ardion Beldad [a,*], Thea van der Geest [b], Menno de Jong [a,1], Michaël Steehouder [a]

[a] University of Twente, Faculty of Behavioral Sciences, Department of Technical and Professional Communication, P.O. Box 217, 7500 AE Enschede, The Netherlands
[b] University of Twente, Faculty of Behavioral Sciences, Department of Media, Communication, and Organization, P.O. Box 217, 7500 AE Enschede, The Netherlands

ARTICLE INFO

Available online 12 November 2011

Keywords:
Online trust
e-Government
Information privacy
Personal information
Organizational reputation

ABSTRACT

This article discusses the results of a large-scale Internet survey (with 1156 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 influences 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 increase their trust in government organizations, specifically in terms of how they process and use citizens' personal data.

1. Introduction

Lack of trust both in government organizations and in the Internet has been cited as one of the critical impediments to the widespread acceptance and adoption of e-government (Germanakos, Christodoulou, & Samaras, 2007). Online government transactions are tied to personal information disclosure, which inescapably fuels risk perceptions grounded on the apprehension that personal information disclosed for availing government services online would be abused. Though there is validity in the claim that the appraised advantages of online government services (e.g. round-the-clock access and efficiency) could heighten the acceptability of e-government (AlAwadhi & Morris, 2008), information privacy concerns both sprouting from and fuelling perceptions of risks associated with online personal data disclosure might ebb citizens' intentions and willingness to use e-government services.

Since risks are present in most online transactions and exchanges, the cultivation of trust both in organizations as partners in online exchanges and in the medium used for transactions is compelling. This assertion is anchored on the proposition that trust is necessary only because human actions oftentimes are shrouded in uncertainty (Lewis & Weigert, 1985). 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 do it only with the tax service office.

While creating online trust is deemed problematic (Weckert, 2005), empirical studies on the many factors that positively influence 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 online transactions with them.

Although studies on trust in e-government are increasing in number, investigations into the determinants of trust in e-government are notably few. This study aimed at identifying the determinants of people's trust in government organizations in terms of their processing and usage of citizens' personal data. An online survey with respondents residing in one of the municipalities in the Netherlands was implemented to address the hypotheses of the research.

1.1. Online trust

Availing online government services implies completing electronic registration forms. This subtly forces citizens to disclose their personal information before a particular transaction can proceed and be completed. However, citizens may be getting more conscious about the risks involved in disclosing their personal data online. Personal information shared with an organization digitally could either be exploited by the organization collecting the information or by

* Corresponding author. Fax: +31 53 489 4259.
E-mail addresses: a.beldad@utwente.nl (A. Beldad), t.m.vandergeest@utwente.nl (T. van der Geest), m.d.t.dejong@utwente.nl (M. de Jong), m.f.steehouder@gw.utwente.nl (M. Steehouder).
[1] Fax: +31 53 489 4259.

0740-624X/$ – see front matter © 2011 Published by Elsevier Inc.
doi:10.1016/j.giq.2011.05.003

unauthorized third parties that could access such information using sophisticated technologies. Personal data are susceptible to abuse because they have become tradable commodities.

As accentuated previously, the innateness of risks in online transactions necessitates the cultivation of trust. Internet users chronically perturbed by the risks of transacting online are depriving themselves of the benefits of engaging in computer-mediated exchanges. The implication, therefore, is that users must have enough trust in the other parties involved in online transactions, despite the risks, before they can actually engage in online transactions and relish the conveniences they afford. This assertion is strongly anchored on Luhmann's (1979) view of trust as an effective mechanism in dealing with the complexities inherent in social encounters and exchanges.

Although definitions of trust are far from unanimous, mainstream views of the said concept veer toward the notions of trust either as an expectation regarding the behavior of an interaction partner (Barber, 1983; Koller, 1988; Luhmann, 1979; Rotter, 1967) or as an acceptance of and exposure to vulnerability (Doney, Cannon, & Mullen, 1998; Mayer, Davis, & Schoorman, 1995; Rousseau, Sitkin, Burt, & Camerer, 1998). Trust in an online context is regarded as Internet users' reliance on an organization with regards to that organization's activities in the electronic medium, and in particular, its website (Shankar, Urban, & Sultan, 2002).

Several studies have shown that trust is an important factor influencing the acceptance and the adoption of online government services (Belanger & Carter, 2008; Carter & Belanger, 2005; Colesca & Dobrica, 2008). One should remember, however, that the intention to avail government services online is preceded by the intention to disclose personal information since requests for government products or services could only be processed after the collection of correct and complete information from those initiating the requests. Fig. 1 illustrates the relation between citizens' trust and their intention to share personal information and avail government services online.

1.2. Cues and factors influencing trust in organizations in the online 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 influence online trust. These cues or factors can be categorized into three: Internet user-based (propensity to trust, level of Internet experience), organization-based (organizational reputation, quality of previous online transaction experience), and website-based (perceived website quality, perceived website security, confidence in privacy statements) (Beldad, De Jong, & Steehouder, 2010). 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. Fig. 2 shows the three-fold categorization of the different determinants of trust in organizations in the online environment.

1.2.1. Internet user-based trust determinants

1.2.1.1. Propensity to trust. People significantly vary in their levels of trust (Mayer et al., 1995). Such variations in trust propensity or disposition, referring to 'a tendency to be willing to depend on others' (McKnight, Cummings, & Chervany, 1998, p. 474), are also evident in online economic exchanges. There, some people 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, Iyer, Palvia, & Singh, 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.

1.2.1.2. Level of internet experience. A couple of studies have 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 any time 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, Shankar, Sultan, & Urban, 2005). This is based on the notion of the Internet as an "experience technology," which implies that as people increasingly accumulate online experience the prospect of them developing learned trust in the Internet will also escalate (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

1.2.2. Organization-based trust determinants

1.2.2.1. 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 et al., 1998). Indeed, 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

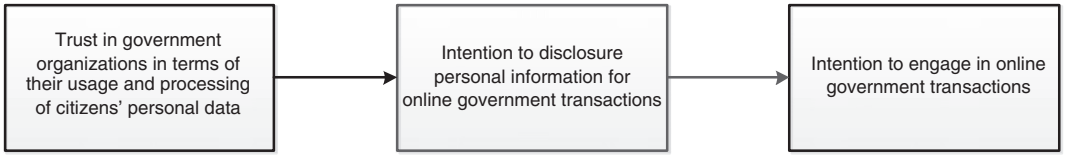

Fig. 1. The relation between citizens' trust in government organization and their intentions to share personal information and to avail government services online.

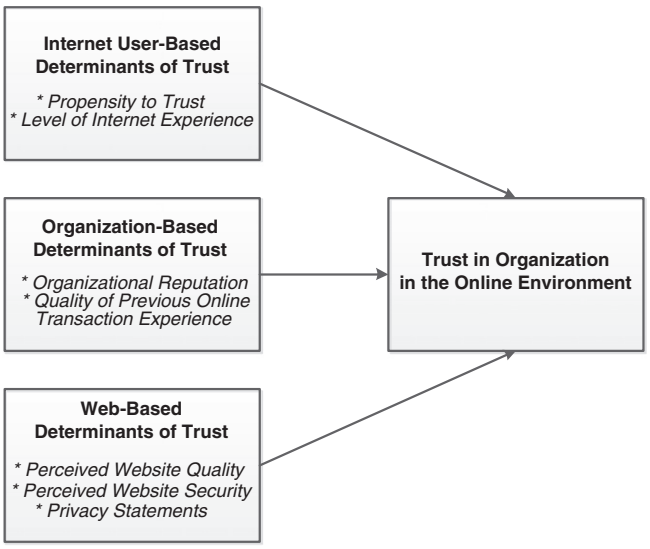

Fig. 2. Three-fold categorization of the determinants of trust in organizations in the online environment.

regarded to act honestly in their daily operations, consider not only their interests but also those of their exchange partners when making decisions, and be competent. These considerations could substantially reinforce their trustworthiness (Keh & Xie, 2009).

Ganesan (1994) underscores that organizational reputation can be assessed in terms of organizational fairness, concern, and honesty — criteria that closely resemble the indicators of trustworthiness (ability, integrity, and benevolence) as identified by several authors (e.g. Barber, 1983; Luhmann, 1979; Mayer et al., 1995; McKnight et al., 1998). 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. As Olivero and Lunt (2004) claim, Internet users will not hesitate to disclose their personal information to well-known online organizations with an image to protect. Assertions on the impact of a positive organizational reputation on online trust formation resulted in the third hypothesis.

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.

1.2.2.2. Quality of previous online transaction experience. Trust viewed as a prediction process, aligned 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 et al., 1998). Sztompka (1999) claims 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, Flavian, & Guinaliu, 2007; Flavian, Guinaliu, & Gurrea, 2006; Pavlou, 2003). These arguments prompted the study's fourth hypothesis.

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

1.2.3. Web-based trust determinants

1.2.3.1. Perceived website quality. Users would be more inclined to trust organizations with websites that are professionally designed. A professionally designed website means 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, Hu, Lee, and Au (2007) argue 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 Internet users' appraisal of the credibility of websites (Fogg et al., 2003). The researchers point out 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.

1.2.3.2. Perceived website security. Security is an important concern not only in online commercial exchanges but also in non-commercial transactions, such as e-government (Blakemore, McDonald, Hall, & Jucuite, 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. According to Koufaris and Hampton-Sosa (2004), the presence of security mechanisms increases users' trust in initial online exchanges.

Security, aside from privacy, is regarded as an important baseline from which Internet users appraise the trustworthiness of an online entity (Urban, Amyx, & Lorenzon, 2009). However, it is argued that security features are deemed 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). The sixth hypothesis is rooted on these assertions.

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.

1.2.3.3. Privacy statements. Perceptions of the risks involved in 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 personal data (Vail, Earp, & Anton, 2008). Internet users who are concerned about their information privacy are expected to consult online privacy statements before opting to disclose personal information (Jensen & Potts, 2004; Pan & Zinkhan, 2006).

Although privacy statements are almost never read or consulted (Arcand, Nantel, Arles-Dufour, & Vincent, 2007; Jensen, Potts, & Jensen, 2005; Meinert, Peterson, Criswell, & Crossland, 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).

Nonetheless, Internet users must have confidence in online privacy statements first before they 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.

2. Methodology

2.1. 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 test the research hypotheses. A link to the Internet-based questionnaire was sent to the 2500 members of the research panel. A total of 1156 completed online questionnaires were returned, resulting in a response rate of 46.42%.

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 1 presents the complete demographic information of the survey participants.

2.2. Survey instrument

Data on respondents' demographic characteristics were collected in the first part of the Internet-based survey. The second part of the survey contained questions pertinent to the variables of the study. Tables 2 and 3 show the items or statements comprising the different constructs. The statements were originally formulated in Dutch. All the items for the other variables (propensity to trust, organizational reputation, quality of previous online transaction experience, perceived website quality, perceived website security, and confidence in privacy statements) were measured on five-point Likert scales, from strongly disagree (1) to strongly agree (5).

For the construct "trust in government organizations," respondents were asked to give a grade to the trustworthiness of government organizations in terms of how they use and process citizens' personal data. The grading system of 1 to 10 used in Dutch schools was used, which prompted the decision to employ a ten-point Likert scale. For this study 10 represents 'very high trust', while 1 'very low trust.' Participants' level of Internet experience was measured in terms of the number of years participants have been using the Internet.

Table 1
Demographic information of survey respondents (N = 1156).

Variable	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

Most of the items were newly formulated for this particular study and were partly based on the responses given during three focus group discussion (FGD) sessions conducted four months prior to the implementation of the survey. 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.

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 previous e-government transactions. 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 various 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 differentiated 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.

3. Results

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

A principal component analysis was performed on the 20 items comprising the online questionnaire for respondents with previous e-government transaction experience. The value of the Kaiser-Meyer Olkin Measure of Sampling Adequacy was pegged at 0.85, which was higher than the recommended value of 0.60 (Kaiser, 1974), while the Bartlett's Test of Sphericity X^2 (231) = 9996.80, $p < 0.001$ 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% of the variance. Shown in Table 2 are the factor loadings after rotation of the items for the questionnaire designed for respondents with e-government experience. Items below 0.40 were intentionally removed from the table.

3.2. 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 performed on the 18 items comprising the online questionnaire for respondents without e-government transaction experience. The value of Kaiser-Meyer Olkin Measure of Sampling Adequacy was 0.80. Correlations among the 18 items were also high for principal component analysis as

Table 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 experience with online government transactions	My online transactions with government organizations have always been good.						0.86	
	I have no negative experiences in transacting online with government organizations.						0.90	
Propensity to trust	I trust people in general.		0.83					
	I tend to count upon other people.		0.73					
	I generally have faith in humanity.		0.83					
	I feel that other people have generally good intentions.		0.83					
Government organizational reputation	Government organizations have the reputation of being competent in carrying out online transactions with citizens.				0.77			
	Government organizations have the reputation of being honest in carrying out online transactions with citizens.				0.85			
	Government organizations have the reputation of taking the interests of the citizens into consideration during online transactions.				0.79			
Confidence in privacy statements on government websites	Government organizations will not abuse my personal data when their websites have privacy statements.			0.78				
	Government organizations will treat my personal data confidentially when their websites post privacy statements.			0.82				
	Government organizations that post privacy statements on their websites can be trusted with my personal data.			0.81				
Website security	The websites of government organizations use appropriate technologies to protect users' personal data from unauthorized third-party access.					0.74		
	The websites of government organizations have the ability to authenticate users for security purposes.					0.74		
	The websites of government organizations work very well technically					0.74		
Website quality	Websites of government organizations are easy to navigate.							0.85
	Websites of government organizations contain relevant information, such as information on how I could contact them.							0.83
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.	0.89						
	Trust in municipalities in terms of their processing and usage of citizens' personal data.	0.90						
	Trust in the tax service office in terms of its processing and usage of citizens' personal data.	0.89						

shown by the Bartlett's Test of Sphericity X^2 (190) = 2505.91, $p<0.001$. The six components also had *eigenvalues* above the Kaiser's criterion of 1 and explained for 76.09% of the variance. Presented in Table 3 are the factor loadings after rotation of the items for the questionnaire designed for respondents without e-government experience. Items below 0.40 were also intentionally removed from the table.

Table 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.			0.83			
	I tend to count upon other people.			0.71			
	I generally have faith in humanity.			0.86			
	I feel that other people have generally good intentions.			0.83			
Government organizational reputation	Government organizations have the reputation of being competent in carrying out online transactions with citizens.	0.91					
	Government organizations have the reputation of being honest in carrying out online transactions with citizens.	0.91					
	Government organizations have the reputation of taking the interests of the citizens into consideration during online transactions.	0.88					
Confidence in privacy statements on government websites	Government organizations will not abuse my personal data when their websites have privacy statements.				0.82		
	Government organizations will treat my personal data confidentially when their websites post privacy statements.				0.84		
	Government organizations that post privacy statements on their websites can be trusted with my personal data.				0.86		
Website security	The websites of government organizations use appropriate technologies to protect users' personal data from unauthorized third party-access.						0.74
	The websites of government organizations have the ability to authenticate users for security purposes.						0.79
	The websites of government organizations work very well technically						0.53
Website quality	Websites of government organizations are easy to navigate.					0.87	
	Websites of government organizations contain relevant information, such as information on how I could contact them.					0.85	
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.		0.94				
	Trust in municipalities in terms of their processing and usage of citizens' personal data.		0.95				
	Trust in the tax service office in terms of its processing and usage of citizens' personal data.		0.90				

Table 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)		
		Cronbach's α	Mean	Std. deviation	Cronbach's α	Mean	Std. deviation
Quality of previous experience with online government transactions	2	0.83	3.82	0.74	–	–	–
Propensity to trust	4	0.82	3.67	0.58	0.83	3.57	0.59
Government organizational reputation	3	0.83	3.27	1.05	0.94	2.14	1.58
Confidence in privacy statements	3	0.84	3.72	0.84	0.87	3.38	1.06
Website security	3	0.68	2.75	1.17	0.72	2.51	1.24
Website quality	2	0.72	3.24	0.92	0.81	2.85	1.35
Trust in government organizations in terms of their processing and usage of citizens' personal data	3	0.94	7.03	1.57	0.95	6.50	1.56

3.3. Construct reliability

Cronbach's alpha scores were also calculated to determine the reliability of the constructs. With the exception of 'website security' (included in the questionnaire for respondents with e-government experience), all the constructs included for the survey instrument for respondents with and without previous e-government transaction experience have alpha scores above 0.70, which indicate adequate reliability (Hinton, 2008). Table 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.

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

Hierarchical multiple regression analysis, which enabled the entrance of the different variables in blocks, was performed 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 corresponded with the three-fold categorization of the hypothesized determinants of online trust (Beldad et al., 2010).

Internet user-based trust determinants, primarily propensity to trust and level of Internet experience, were entered in the first block resulting in an explained variance of 2% ($F_{2, 956} = 11.83$, $p < 0.001$). Organizational reputation and quality of previous e-government transaction experience, both organization-based trust determinants, were entered in the second block raising the explained variance to 19% ($F_{4, 954} = 57.28$, $p < 0.001$). Website quality, website security, and confidence in privacy statements were eventually entered in the third block with an explained variance pegged at 33% ($F_{7, 951} = 65.84$, $p < 0.001$).

Looking at the complete model, it is evident that confidence in privacy statements on government websites ($b = 0.41$, $p < 0.001$), government organizational reputation ($b = 0.22$, $p < 0.001$), and the quality of Internet users' online transaction experience with government organizations ($b = 0.09$, $p < 0.01$) 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 Hypothesis 7.

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 in the organization. Hence, Hypothesis 3 is also accepted. 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 4 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 5 shows both the non-standardized and the standardized coefficients of the different variables hypothesized to positively influence respondents' trust in government organizations in terms of their processing and usage of citizens' personal data.

3.5. 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 multiple regression analysis was also conducted. 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 explained variance of 3% ($F_{2, 194} = 2.72$, *p value not significant*). The entrance of government organizational reputation in the second block spurred a slight increase in the explained variance of 5% ($F_{3, 193} = 3.07$, $p < 0.05$). In the third block, website quality, website security, and confidence in privacy statements were entered resulting in an explained variance of 16% ($F_{6, 190} = 5.88$, $p < 0.001$).

In the final model, only confidence in privacy statements ($b = 0.34$, $p < 0.001$) positively influences trust in government organizations among respondents without e-government transaction

Table 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	0.34		0.02 (0.02)***
Propensity to trust	0.42	0.09	0.16***	
Internet experience (measured in years)	−0.00	0.01	−0.01	
Step 2				
Constant	3.27	0.37		0.19 (0.17)***
Propensity to trust	0.20	0.08	0.07*	
Internet experience (measured in years)	−0.01	0.01	−0.02	
Government organizational reputation	0.60	0.05	0.35***	
Quality of previous online government transaction experience	0.28	0.07	0.13***	
Step 3				
Constant	2.28	0.35		0.33 (0.14)***
Propensity to trust	0.09	0.08	0.03	
Internet experience (measured in years)	−0.01	0.01	−0.01	
Government organizational reputation	0.37	0.06	0.22***	
Quality of previous online government transaction experience	0.18	0.06	0.09**	
Website quality	−0.12	0.06	−0.06	
Website security	0.03	0.04	0.02	
Confidence in privacy statements	0.76	0.06	0.41***	

*** $p < 0.001$.
** $p < 0.01$.
* $p < 0.05$.

Table 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	0.73		0.03 (0.03)
Propensity to trust	0.43	0.19	0.16*	
Internet experience (measured in years)	0.01	0.03	0.02	
Step 2				
Constant	4.45	0.76		0.05 (0.02)*
Propensity to trust	0.44	0.19	0.17*	
Internet experience (measured in years)	0.01	0.03	0.03	
Government organizational reputation	0.16	0.08	0.14	
Step 3				
Constant	3.61	0.75		0.16 (0.11)***
Propensity to trust	0.28	0.18	0.11	
Internet experience (measured in years)	−0.00	0.03	−0.01	
Government organizational reputation	−0.03	0.09	−0.03	
Website quality	0.08	1.00	0.06	
Website security	0.05	1.00	0.04**	
Confidence in privacy statements	0.50	0.11	0.34***	

*** $p<0.001$.
** $p<0.01$.
* $p<0.05$.

experience. This precipitates the acceptance of Hypothesis 7. 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 of 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, it 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 are the non-standardized and the standardized coefficients of the different variables hypothesized to increase trust in government organizations in terms of their processing and usage of citizens' personal data among respondents without e-government experience.

4. Discussion

Several factors have been identified to enhance 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 usage, privacy statements on websites, and website quality could 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 vary 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 existing 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 & Cacioppo, 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 might 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 as potential determinant of online trust.

The absence of the impact of website security on trust in online government transaction seems discomforting since 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 toward a more general variable 'trust in government organizations.'

It is to be expected that security measures used by different government organizations vary. For instance, one organization might be using a more stringent security mechanism than another organization. While this study did not look into people's 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 influence citizens' trust in those organizations.

5. 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 often not read, the availability of privacy statements on websites are effective in quelling Internet users' apprehensions of supplying their personal information online. This online survey somehow provides enough empirical evidence to assert that confidence in privacy statements on the websites of government organizations is important 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 marked 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 privacy 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 read them 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 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. Therefore, taking people's trust for granted in a competitive market could be catastrophic for a particular commercial organization.

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. Nonetheless, despite the aforementioned monopoly, a particular government organization that channels its services online still faces an unwarranted but real competition. It competes with itself in terms of its service delivery mode. Citizens who opt not to 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 by capitalizing on visible 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 in the Netherlands. 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 aforementioned construct was measured in terms of the navigability of government websites and the availability of relevant information on those websites only. However, other indicators such as the use of colors, the types and quality of photographs, and the completeness and correctness of information on websites should also be included to measure 'website quality.'

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 vary, one can expect that the impact of the different trustworthiness cues on trust would differ. Looking into the determinants of trust in a particular government organization, therefore, could be regarded as a logical research pursuit.

6. Conclusion

The proliferation of investigations into 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 done 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.

Acknowledgment

This study is part of a large research project on trust in Dutch e-government financially subsidized by Alliantie Vitaal Bestuur.

References

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. *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

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.
Barber, B. (1983). *The logic and limits of trust*. New Brunswick, NJ: Rutgers University Press.
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.
Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The 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. *The 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). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, *26*(5), 857–869.
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.
Boyd, J. (2003). The rhetorical construction of trust online. *Communication Theory*, *13*(4), 392–410.
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.
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.
Chen, C. (2006). Identifying significant factors influencing consumer trust in an online travel site. *Information Technology and Tourism*, *8*, 197–214.
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.
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.
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.
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., & Tauber, E. R. (2003). How do users evaluate the credibility of websites? A study with over 2,500 participants. *Proceedings of the 2003 conference on designing for user experiences; San Francisco, California* Retrieved from http://portal.acm.org/citation.cfm?id=997097
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.
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.
Herbig, P., Milewicz, J., & Golden, J. (1994). A model of reputation building and destruction. *Journal of Business Research*, *31*, 23–31.
Hinton, P. R. (2008). *Statistics explained* (2nd ed.). East Sussex, UK: Routledge.
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
Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. *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.
Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, *39*(1), 31–36.
Keh, H. T., & Xie, Y. (2009). Corporate reputation and behavioral intentions: The roles of trust, identification, and commitment. *Industrial Marketing Management*, *39*, 732–742.
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. *Proceedings of the 5th international conference on electronic commerce, Pittsburg, PA* Retrieved from http://portal.acm.org/citation.cfm?id=948005.948046
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.
Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*, 323–331.
Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, *63*(4), 967–985.
Luhmann, N. (1979). *Trust and power*. Chichester: John Wiley.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organization trust. *Academy of Management Review*, *20*(3), 709–734.
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. *The 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.
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.
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.
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.
Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331–338.
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.
Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York, NY: Springer-Verlag.
Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*(4), 651–665.
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.
Salam, A. F., Iyer, L., Palvia, P., & Singh, R. (2005). Trust in e-commerce. *Communications of the ACM*, *48*(2), 73–77.
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.
Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems*, *11*, 325–344.
Simon, H. A. (1955). A behavioural model of rational choice. *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.
Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge, UK: Cambridge University Press.
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.
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.

Ardion Beldad is an assistant professor of Communication Studies at the University of Twente, the Netherlands. His main research interests include trust, information privacy, and new media usage in organizations. Contact: a.beldad@utwente.nl.

Thea van der Geest is an associate professor of Communication Studies at the University of Twente, The Netherlands. Her recent research projects are focusing on user-centered design and evaluation of e-government services and systems for Dutch and international government agencies. Contact: t.m.vandergeest@utwente.nl.

Menno de Jong is a professor of Communication Studies at the University of Twente, the Netherlands. His main research interests concern the methodologies of applied communication research and organizational communication. Contact: m.d.t.dejong@utwente.nl.

Michael Steehouder is a professor emeritus of Communication Studies at the University of Twente, the Netherlands. His main research interests include document design and rhetoric. Contact: m.f.steehouder@utwente.nl.