MASARYK UNIVERSITY

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Heirman, W., Walrave, M., Ponnet, K., & Gool, E. V. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3), article 3. http://dx.doi.org/10.5817/CP2013-3-3

Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model

Wannes Heirman[1], Michel Walrave[2], Koen Ponnet[3], Ellen Van Gool[4]

[1,2,4] Department of Communication Studies, University of Antwerp, Antwerp, Belgium
[3] Department of Communication Studies & Department of Sociology, University of Antwerp, Antwerp, Belgium

Abstract

This study examines the relationship between the level of trust that adolescents place in a specific commercial website and their behavioural intentions to disclose four categories of personal information (identity information, geographical information, profile information and contact information) to the website. Following the integrative model of organisational trust, we hypothesise that respondents' level of trust in a specific commercial website is determined by three dimensions of trustworthiness: ability, integrity and benevolence. In order to test the proposed model, we conducted a survey among 1042 Flemish adolescents. Analyses indicate that perceived ability and integrity predicted adolescents' level of trust in the focal website. The respondents' trust in the website subsequently predicted their willingness to disclose. The influence of the discerned trustworthiness beliefs was fully mediated by the level of trust adolescents had in the specific commercial website. Adolescents' risk perception about disclosing information to this website also affected their willingness to disclose information. Finally, our analysis identified an individual's disposition to trust (i.e. trust propensity) as significantly predicting (1) the three trustworthiness beliefs and (2) the willingness to disclose the four discerned categories of personal information. Surprisingly no significant association was found between trust propensity and adolescents' trust in the specific commercial website.

Keywords: Information privacy; trust; trustworthiness; risk; disclosure

doi: 10.5817/CP2013-3-3

Introduction

Commercial websites are increasingly soliciting people to disclose personal information for a variety of data-processing activities (Paine Schofield & Joinson, 2008). On many youth-oriented websites, underage visitors cannot gain full access to web content without first completing a registration form that requests some extent of personal information (Montgomery, 2001; Paine Schofield & Joinson, 2008). In this regard, a content analysis of 133 popular youth-oriented websites revealed that most of them (87%) process personal data (Cai & Zhao, 2010). These data-processing activities have sparked concerns amongst parents' organisations, consumer advocates and policymakers (Paine Schofield & Joinson, 2008; Youn, 2005). With regard to susceptibility to commercial incentives in exchange for information disclosure, Turow and Nir (2000) report that minors are more likely than adults are to divulge personal information in exchange for commercial incentives. Adolescents also seem less concerned about possible privacy-related risks, including identity theft and loss of control over personal data (Earp & Baumer, 2003). This raises questions about the extent to which minors are capable of providing informed consent for the collection and use of their personal data when requested by online marketers as a means of informing marketing campaigns and targeted advertising using data-mining techniques.

As argued in several studies (Baker & White, 2010; Premazzi et al., 2010), the disclosure of personal information to commercial websites is accompanied by both benefits and risks. Benefits include increased user convenience, greater personalisation and enhanced relevance of web content (Chellappa & Sin, 2005; Mothersbaugh, Foxx, Beatty, & Wang, 2012). Most of the risks associated with online self-disclosure result from the ways in which personal information is collected, stored, aggregated and analysed online.

The technicality of online media enables marketers to construct detailed descriptions of individuals. This information is highly valued by companies, as it allows them to distil detailed consumer profiles of individual Internet users (Malhotra, Kim, & Agarwal, 2004). The information privacy of adolescents could therefore be seriously jeopardised in cases of far-reaching information collection practices by commercial websites.

The Role of Trust in Online Disclosure Settings

The role of trust is considered particularly relevant in online environments, as the intentions of others are less verifiable in such contexts than they are in offline environments (Bargh & McKenna, 2004; Taylor, Davis, & Jillapalli, 2009). For example, Pavlou (2003) argues that trust is a crucial component of online transactions between consumers and marketers. In general, previous researchers have conceptualised trust in three distinct ways: (1) a general belief that another party can be trusted (e.g. Gefen, 2000), (2) a set of specific beliefs about a specific party (e.g. Jarvenpaa, Tractinsky, & Vitale, 2000; Johnson-George & Swap, 1982) and (3) specific beliefs as antecedents of a general trust belief in another party (e.g. Mayer, Schoorman, & Davis, 1995). This study adopts the third option, thus following the theoretical framework proposed by Mayer, Schoorman and Davis (1995): The integrative model of organisational trust. In the context of this theoretical framework, trust is being defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." (Mayer et al., 1995, p. 712). One discerning feature of Mayer et al.'s (1995) framework is that it clearly separates trust from other related concepts (e.g. perceived trustworthiness, trust propensity, perceived risk etc.), thereby making it the most nuanced trust-decision making model available in literature. Other trust studies have tended to operationalize trust as an amalgam of both its antecedents and its consequences (Colquitt, Scott, & LePine, 2007). A first distinction, however, made in Mayer et al.'s (1995) theory is the one between trust and its antecedent beliefs of trustworthiness (encompassing three types of beliefs: perceived ability, benevolence and integrity beliefs). An additional distinction is made between trust as a situational concept (i.e. pending on the characteristics and context in which a specific trustee appears) and trust as a personality trait (i.e. one's general trust in others, also referred to as 'trust propensity'). In subsequence of other studies that have found indications that trust determines a great variety of online intentions and behaviours on the part of internet users (Gefen, 2002; Reichfeld & Schefter, 2000), this study therefore aims to explore the role of trust and disentangle the influence exerted by other trust-related concepts on Flemish adolescents' decision-making with respect to the disclosure of their personal data to a specific well-known commercial website based in Belgium: http://www.msn.be.

The Integrative Model of Organisational Trust

As stated in the previous paragraph, this study proceeds from the differentiation between the central concepts of trust propensity, perceived risk and trust, as contained in the model developed by Mayer et al. (1995). According to the model, trust is preceded by a set of specific trustworthiness beliefs. One advantage of differentiating between these trust-related concepts is that it allows us to obtain a broader picture of the influence of trust in situations affecting the online information privacy of adolescents. The model proposed by Mayer et al. (1995) is designed specifically for situations in which people feel vulnerable in relation to an organisation. It is based on the axiom that, in such situations of vulnerability, an individual's level of trust and perceived risk related with a specific party determines the individual's willingness to take risks in the relationship with this specific party to be trusted (hereafter designated as 'trustee') (Mayer et al., 1995). This relationship could include the engagement to cooperate or exchange something with the organisation (i.e. the trustee). The sharing of personal information can also be considered a sign of trust in this regard. For example, Joinson and Paine (2007, p. 247) argue that trust is relevant in the context of online disclosure and information privacy, because "by disclosing information, we are making ourselves vulnerable." This vulnerability stems partially from the fact that internet users disclose information within contexts of spatial and temporal separation. The situation is further characterised by information asymmetry, thus creating situations of uncertainty in which internet users are unaware of what will happen with personal data collected for marketing purposes. According to Gefen (2002), the main function of trust is to reduce the uncertainty of the social environment. Without trust, only short-term transactions would be possible. Given the uncertainty-reducing function of trust, it is plausible that a user's decision to disclose personal data depends largely upon the extent to which the user trusts a commercial website.

The model developed by Mayer et al. (1995) is particularly known for several applications in management and leadership studies, although its applicability has been tested in other contexts (e.g. adoption of e-commerce) as well (Lee & Turban, 2001). According to its developers (Mayer et al., 1995, p. 712), the model is applicable to all types of human relationships "with another identifiable party who is perceived to act and react with volition toward the trustor." To the best of our knowledge, it has not yet been applied to adolescents' disclosure of information online for commercial purposes.

Research Model

Given that trust is situational and context-specific, Lee and Turban (2001, p. 78) argue that "it should be investigated under specific contextual and situational parameters." As discussed before, the specific context of the present study is the willingness of adolescents to disclose personal data to msn.be. We took this website as the focal website of our study to demonstrate the role of trust in online

disclosure settings, as it was evidenced by website-visit figures (Metriweb, 2012) that this Belgian portal website of Microsoft was well known among the population of Flemish adolescents. It therefore provides an adequate context for testing our hypotheses, as the proposed model can be tested only with reference to a specific trustee. In Figure 1, we have integrated the important concepts of the trust model developed by Mayer et al. (1995), adapted to the context of information disclosure by adolescents. With regard to our outcome variables, the dearth of previous research indicates that the type of information requested by marketers affects respondents' motivation intention to disclose (Mothersbaugh et al., 2012; Walrave, Vanwesenbeeck, & Heirman, 2012). In the present study, we therefore discern four categories of personal information regularly requested by commercial websites for data-processing activities: identity data (forename, family name, birth year, sex), geographical information (home city, school city), contact data (email address, messenger ID, mobile phone number) and profile data (hobbies, faith orientation, political orientation, relationship status, favourite brands).

The influence of trustworthiness beliefs on adolescents' willingness to disclose is expected to be fully mediated by the trust adolescents express in the website. The other components of the model and the hypotheses of the present study are also displayed in the figure. In the following section, we discuss how we inferred our hypotheses from literature.

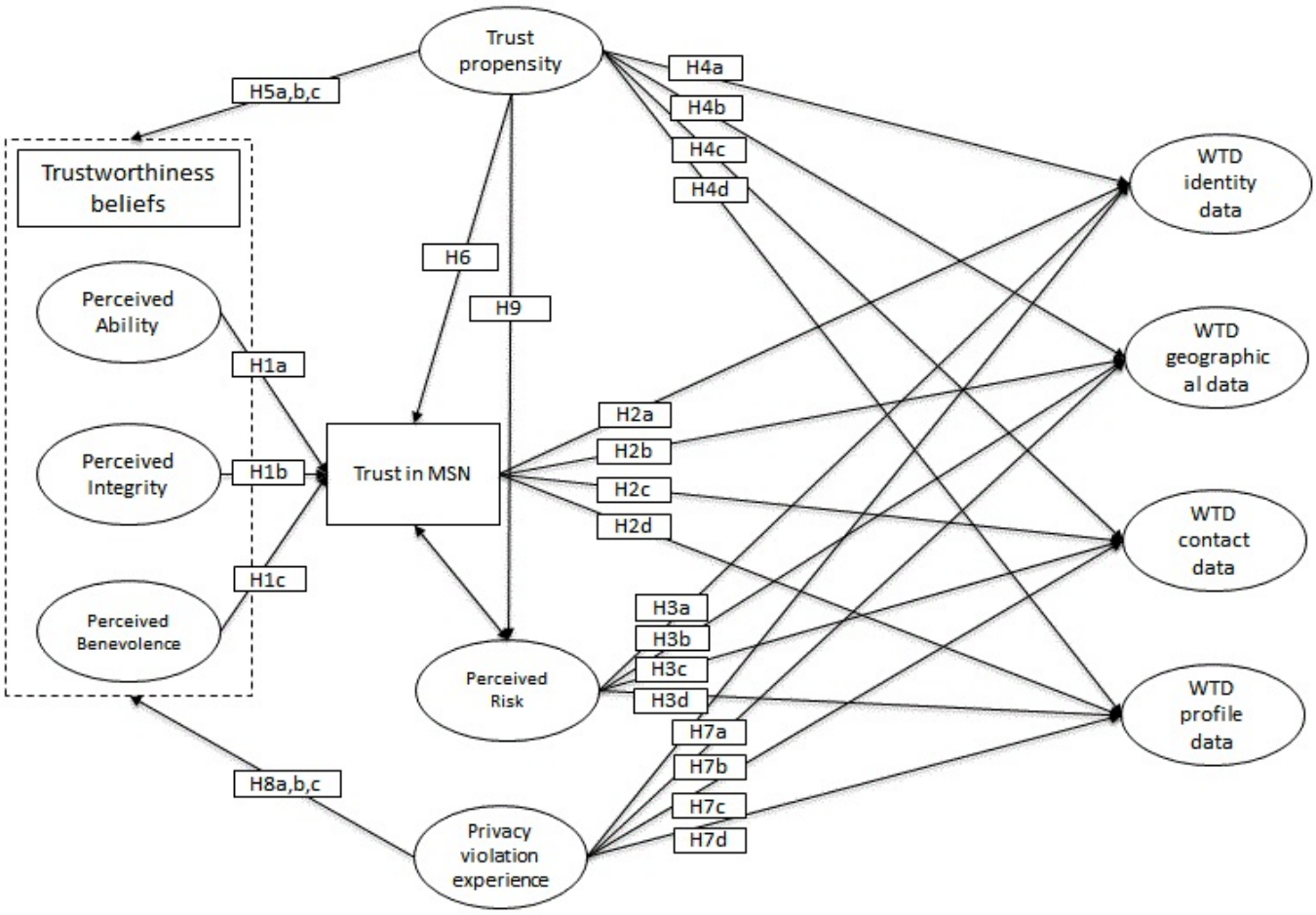

Figure 1: Proposed integrative model of organisational trust applied to adolescents' willingness to disclose (WTD).

Perceived Trustworthiness: A Multidimensional Concept

Mayer et al. (1995) treat perceived trustworthiness as a conjunction of specific trustworthiness beliefs held by the trusting party (hereafter designated as 'trustor') regarding the trustee. According to their model, in offline environments, trustworthiness consists of three dimensions: perceived ability, integrity and benevolence. In this regard, they state that "each of these three factors captures some unique elements of trustworthiness" (Mayer et al., 1995, p. 722). In 2002, Gefen tested the general applicability of this three-factor structure in the online environment. His analyses confirmed that the three components of trustworthiness could also be applied in online environments. In the following sections, we discuss each of these dimensions in greater detail, elaborating on how we expect each dimension to influence the level of trust that adolescents express in the focal commercial website of this study.

Perceived ability. Mayer et al. (1995, p. 717) define ability as "that group of skills, competencies, and characteristics that enable a party to have influence within some domain." Perceived ability thus refers to the capabilities of the trustee in relation to the trustor.

Studies have shown that perceived competence is especially important on the Internet, as online organisations must prove that they have the resources and competences necessary for successful performance (Belanger, Hiller, & Smith, 2002; Flavián & Guinalíu, 2006). For example, a study investigating the willingness of respondents to engage with a commercial electronic vendor reveals that perceived competence significantly influences the willingness of individuals to follow the advice of online commercial organisations, as well as their willingness to share personal information with these organisations (McKnight, Choudhury, & Kacmar, 2002). More specifically, in the context of online data disclosure, the competence of a website owner could be understood to include the company's ability to protect the collected personal data from unauthorised access (McKnight et al., 2002). We therefore predict that adolescents who doubt the professionalism of the focal commercial websitewill be less likely to trust the website.

> H1a: The higher adolescents rate the perceived ability of the focal commercial website, the higher will be their reported level of trust in this website.

Perceived integrity. Mayer et al. (1995, p. 719) describe integrity as "the perception that the trustee adheres to a set of principles that the trustor finds acceptable."As demonstrated in the study by Lee and Turban (2001), the level of integrity that respondents perceive an online organisation to have strongly determines their level of trust in purchasing goods online. This indicates that, in addition to a company's competence, ethics-based characteristics (e.g. integrity) could be relevant in the context of trust and online information privacy (McKnight et al., 2002). Concerning integrity, adolescents who are sceptical about the honesty of a website and who suspect that they are being deceived are likely to demonstrate less trust in the online platform, thus possibly affecting their willingness to disclose personal information.

> H1b: The higher adolescents rate the perceived integrity of the focal commercial website, the higher will be their reported level of trust in this website.

Perceived benevolence. Perceived benevolence constitutes the third dimension of trustworthiness. It is described as "the extent to which the trustee is believed to want to do good to the trustor, aside from an egocentric profit motive" (Mayer et al., 1995, p. 718). In marketing literature benevolence has often been associated with consumer trust (Flavián & Guinalíu, 2006). Studies of e-commerce have reported significant correlations between benevolence and individual intentions to buy online (Lu, Zhao, & Wang, 2010), as well as between benevolence and the intention to entrust personal data to online organisations (McKnight et al., 2002) and users' loyalty towards the website (Gupta & Kabadayi, 2010). We predict that adolescents who think that the commercial website is not committed to their welfare will demonstrate lower trust in this website.

> H1c: The higher adolescents rate the perceived benevolence of the focal commercial website, the higher will be their reported level of trust in this website.

Trust. In essence, the trust-based model proposed by Mayer et al. (1995) holds that, in situations in which risks are present, trust determines an individual's behavioural intention to take risks in the relationship with the trustee. One effect of trust is the trusting party's willingness to engage with the trustee in situations where the trustor is vulnerable (Doney & Cannon, 1997; Mayer et al., 1995). As stated by Riegelsberger, Sasse, and McCarthy (2005), this vulnerability goes beyond the potential loss of financial goods. The loss of money, time and personal information are also potentially important in trusting situations. Releasing personal information could thus place the person disclosing this information in a position of vulnerability. Previous studies of the internet have suggested that people who trust e-commerce platforms are more inclined to engage in transactions with online firms (Bhattacherjee, 2002) or to make purchases from online shops (Gefen, 2002), in addition to being more likely to disclose personal information (Mesch & Beker, 2010). In line with these studies, we predict the following:

> H2: There is a positive relationship between adolescents' trust in the focal commercial website and their willingness to disclose identity information (H2a), geographical information (H2b), contact information (H2c) and profile information (H2d).

Perceived risk. The level of perceived risk reflects the extent to which trustors believe that they will lose something in relationship with particular trustees (Mayer et al., 1995). Research has shown that many online consumers consider the release of their personal information as risky, as doing so could expose them to potential opportunistic behaviour on the part of a company (Malhotra et al., 2004; Friedman et al., 2000). For this reason, we argue that it is not possible to examine the ways in which adolescents cope with information privacy without considering the level of risk that they perceive to be associated with information disclosure. As noted by Gefen, Benbasat, and Pavlou (2008), trust and perceived risk are closely related concepts. Studies have clearly shown that high levels of perceived risk regarding information disclosure constitute an important reason that consumers have for not participating in e-commerce and data-collection activities for purposes of online marketing (Jarvenpaa et al., 2000; Reichfeld & Schefter, 2000). Results from a more recent study by Mesch (2012), based on the secondary analyses of the 2009 Pew Internet data, also indicate that perception of privacy risks refrain users from posting personal information online. Another study found support for the fact that internet users adapt their level of personal information disclosure to the level of perceived threats (Krasnova, Spiekerman, Koroleva, & Hildebrand, 2010). We therefore predict the following:

H3: There is a negative relationship between the perceived risk associated with disclosing personal information to a commercial website and the willingness of adolescents to disclose identity information (H3a), geographical information (H3b), contact information (H3c) and profile information (H3d).

Trust propensity. In trust literature it is recognised that some people are generally more willing to trust other people and organisations than others are (Mayer et al., 1995). Dispositional trust might thus influence intentions and behaviours related to information privacy to a certain extent (Malhotra et al., 2004). Studies have also demonstrated that the propensity to trust is especially relevant in determining behavioural intentions when little or no information is available concerning the trustee (McKnight & Kacmar, 2004). Given the potential importance of trust propensity in situations involving unfamiliar actors (Bigley & Pearce, 1998; Gefen, 2000), adolescents with higher trust propensity might be more amenable to disclosing their personal information in online environments without thorough knowledge or clear perceptions of the website proprietor. We therefore hypothesise the following:

H4: The more adolescents are inclined to trust others in general, the more willing they will be to disclose their identity information (H4a), geographical information (H4b), contact information (H4c) and profile information (H4d).

In several studies among adult samples, a relation has been observed between people's tendency to have trust in others and the perceptions they hold of a specific party's trustworthiness (McKnight & Cummings, 1998; Ross & LaCroix, 1996). For instance, a meta-analytic study conducted by researchers from Florida University (Colquitt et al., 2007) revealed that the average correlations between trust propensity and trustworthiness beliefs of ability ($r = .15$, $p < .05$), benevolence ($r = .20$, $p < .05$) and integrity ($r = .29$, $p < .05$) were significant across the trust-studies taking this relationship into account. Another study supporting this relation between disposition to trust and people's trust-related perceptions, yielded the interesting result that people with a low tendency to trust, were also more inclined to perceive the Internet as more dangerous compared to people with high trust propensity (Uslander, 2000). To the best of our knowledge, no study has focussed on the question whether propensity to trust among adolescents affects their perceptions of a website's perceived trustworthiness. Therefore, we expect that:

H5: The more adolescents are inclined to trust others in general, the more positive will be their perception regarding the ability (H5a), the benevolence (H5b) and the integrity (H5c) of the this study's focal website.

Current trust literature has produced mixed empirical findings with respect to the predictive value of trust propensity on trust. For instance, based on their study focussing on the construction of 'trust in specific parties'-scale, Johnson-George and Swap (1982) come to the conclusion that people's disposition to trust, does not accurately determine an individual's trust in a specific context and under particular circumstances. Other studies, however, do point in the direction of a significant positive relation between both concepts ($r = .27$, $p < .05$ in the meta-analyses by Colquitt et al., 2007). For instance, Mesch (2012) found that generalized trust in individuals and social institutions is associated with trust online: About one fifth in total variance (20%) of online trust could be attributed to respondents' tendency to trust other persons and organizations. Katz and Rice (2002) reported that people who are more inclined to trust others in general offline are also more trusting in online environments. Therefore, we expect:

H6: The higher adolescents' trust propensity, the higher will be their level of trust expressed in the focal website of this study.

Experience with privacy violation. Personal experiences can affect an individual's level of privacy concern and subsequent protective behaviours (Harris, 2004). Negative experiences in the area of online privacy can range from receiving relatively innocent unsolicited emails to more serious infractions (e.g. identity theft, fraud). The most serious privacy infringements are particularly likely to cause young people to reconsider the value of privacy and thereby to attach more importance to the risks of online disclosure. Most adolescents have experienced both positive and negative outcomes of digital media (Livingstone, Ólafsson, O'Neill, & Donoso, 2012). A recent study reports that 9% of European young people reported that their personal information had been misused on the internet during the preceding 12 months (Livingstone et al., 2012). Strater and Lipford (2008) observed that respondents reporting events about intrusive contacts made on SNS were more likely to give thorough consideration to their online disclosure and the level of access allowed to data on their social network profiles. Moreover, research has demonstrated a negative association between users' personal experiences with privacy violation and their willingness to be profiled on the internet (Awad & Krishnan, 2006). The experiences that adolescent internet users have had with privacy on the internet might generate knowledge and perceptions that reshape their intentions to disclose personal information to commercial websites. We therefore predict the following:

H7: The more adolescents have been confronted with a violation of their online privacy in the past, the less willing they will be to disclose identity data (H7a), geographical information (H7b), contact information (H7c) and profile information (H7d).

Moreover, it is possible that not only adolescents' behavioural intentions are changed in response to one or more privacy infringements experienced by them, but that at the same time also their perception of the trustworthiness of specific websites is affected by an event or a transaction during which their personal information was abused. Indeed, it has been shown that when

teenagers find out their personal information has been treated in a way they did not approve of beforehand, this causes feelings of distrust, anger and anxiety (boyd, 2008). Such feelings might influence young internet user's perception of a specific website. Hence, we expect that:

> H8: The more adolescents have experienced a violation of their privacy in the past, the more negative will be their perception regarding the ability (H8a), the benevolence (H8b) and the integrity (H8c) of this study's focal website.

People with a high disposition to trust have been found to express greater trust towards specific others. Gefen (2000) reports a highly significant positive relationship between individuals' disposition to trust and their actual trust in a specific commercial website (i.e. Amazon.com). Less literature, however, is available on the question whether a high level of trust propensity will also lead to lower levels of perceived risk to enter in a relation with a specific person or organization. It is plausible to assume that adolescents with higher levels of generalized trust in others, will to a lesser extent think about the possible risks and dangers they are exposed to by disclosing their personal information to a specific website. Therefore, we expect to find the following association in our data:

> H9: The more adolescents will be inclined to trust other persons in general, the lower will be the level of perceived risk they associate with disclosing personal information to msn.be.

Control variables. We control for the influence of age and gender, as the strengths of the associations posited in the model are likely to vary according to these factors. Previous studies have yielded significant relations between both socio-demographics on the one hand and young people's willingness to disclose their personal information online on the other hand (Mesch, 2012). With respect to gender, a pattern of results that has been observed across several studies is that females in general are more concerned about the protection of their personal information and their privacy on the internet (Graeff & Harmon, 2002; Moscardelli & Divine, 2007; Youn, 2005, 2009). For instance, on social network sites (SNSs), females are more inclined to protect the information shared on their profile with more restrictive privacy settings (Madden et al., 2013). With respect to age, a considerable body of research has demonstrated a positive relation between age and disclosure, with older adolescents disclosing significantly more personal details online than younger youth (Lenhart & Madden, 2007; Schouten, Valkenburg, & Peter, 2007; Youn, 2005). Also, given the possible correlation of familiarity (i.e. how frequently does the respondent visit the focal website?) with trust, this construct is included as a covariate (e.g. Gefen, 2000).

Method

Procedure and Sample

Data were collected through anonymous self-administered paper-and-pencil questionnaires distributed in classrooms in January 2011. From an exhaustive list of schools obtained from the Flemish Ministry of Education, we selected six schools from each of the five provinces in Flanders, resulting in a total selection of 30 schools. Flanders has an educational system that consists of three educational types in secondary education: 'General Secondary Education'-schools which provide broad theoretical education preparing for further education at college or university, 'Technical Secondary Educations'-schools which focus more on technical skills and practical matters, and 'Vocational Secondary Education' which directly prepares pupils for employment after secondary school by teaching very job-specific skills. In order to guarantee the equal representation of students from each of these three educational types in the sample, two schools per province were selected of each educational type. We asked the principals of the selected schools for permission to conduct a survey in three classes of their school. In order to guarantee the equal representation of students in various age categories, we randomly selected for each school three classes from different grades (1st grade: 1st and 2nd year secondary education; 2nd grade: 3rd and 4th year secondary education; 3rd grade: 5th and 6th year secondary education). All students from a selected class were asked for their permission to participate in the survey study. In all, 1042 respondents (519 males and 523 females) participated. The participants ranged in age from 12 to 18 years (M_{age} = 15.35; SD = 1.75).

It was made clear at the beginning of the survey that the respondents were under no obligation (nor explicit or implicit) to participate. No pupil indicated that he/she did not want to participate in the research. A researcher explained the purpose and procedure of the survey. Moreover, the questionnaires also contained clear written instructions that allowed pupils to singly complete the questionnaire, although pupils could ask additional instructions whenever they deemed this necessary during questionnaire completion. The students were assured that their responses would remain anonymous and confidential, and that no information would be passed along to teachers, parents or fellow students. Provisions were made to guarantee the participants' privacy and confidentiality during the administration.

Measures

Trustworthiness beliefs. Consistent with the tenets of the integrative model of organisational trust (Mayer et al., 1995), the concept of trustworthiness consists of three factors: ability (4 items), integrity (3 items) and benevolence (3 items). All items were measured

along a Likert scale ranging from 1 (*strongly disagree*) to 6 (*strongly agree*). Table 1 displays the items used to build the factors. Each factor exhibited good internal consistency (see Cronbach's alpha scores in Table 1).

Table 1. Operationalization of perceived trustworthiness and perceived risk.

	α	Mean	SD	Range
Perceived Trustworthiness				
Ability	.83			
1. TRUSTEE is a successful website		4.34	1.13	1-6
2. TRUSTEE is a professional website		3.83	1.22	1-6
3. TRUSTEE never disappoints me		3.78	1.29	1-6
4. TRUSTEE is a specialised website		3.52	1.27	1-6
Integrity	.81			
1. TRUSTEE fulfils its promise to its users		3.79	1.12	1-6
2. TRUSTEE is honest to its users		3.88	1.10	1-6
3. TRUSTEE maintains values I approve of		3.72	1.15	1-6
Benevolence	.79			
1. TRUSTEE is concerned about its users		3.47	1.20	1-6
2. TRUSTEE finds the needs of its users important		3.50	1.18	1-6
3. TRUSTEE considers the priorities of its users		3.44	1.24	1-6
Perceived Risk	.88			
1. I can get into trouble by disclosing my information to TRUSTEE		3.64	1.46	1-6
2. Disclosing my information to TRUSTEE involves risks		3.74	1.35	1-6
3. In my opinion, there are more disadvantages than advantages to disclosing my information to TRUSTEE		3.77	1.36	1-6

Note: TRUSTEE = website http://www.msn.be

Perceived risk. Participants rated three self-constructed items along a Likert scale ranging from 1 (*strongly disagree*) to 6 (*strongly agree*). Table 1 displays the three items used to measure this construct. The internal consistency of the items was good (α = .88).

Trust propensity. The measurement of trust propensity was based on a six-item adaptation of Rotter's trust-propensity scale (Rotter, 1967) (e.g. "I'm inclined to trust others, even if I don't know them"; *1 = strongly disagree* to *6 = strongly agree*). High scores indicate that respondents are more inclined to trust others in general. The scale exhibited good internal consistency (α = .85).

Privacy violation experience. This construct was measured using three dichotomous items (e.g. "I have experienced a misuse of personal data"; yes/no).

Willingness to disclose personal information. Consistent with previous research (Malhotra et al., 2004; Meinert, Peterson, & Criswell, 2006), respondents were asked to rate their willingness to provide 14 types of personal data to msn.be along a scale ranging from 1 (*would definitely not disclose*) to 7 (*would definitely disclose*). Factor analyses revealed four dimensions of willingness to disclose: identity data (α = .89), geographical data (α = .89), contact data (α = .84) and profile data (α = .87).

Trust. We chose to measure trust by directly asking respondents to score the extent to which they trusted the specific trustee included in this study (http://www.msn.be) along a six-point Likert scale ("msn.be can be trusted"; *1 = strongly disagree – 6 = strongly agree*).

Familiarity with the website. Adolescents' familiarity with the specific website was assessed with a single-item measure. Respondents were asked to indicate the frequency with which they visited the focal website, using a scale ranging from 1 (*never*) to 6 (*very often*).

Data Analysis

Our analyses begin with a discussion of the descriptive findings. To investigate the hypothesised relationships, we applied structural equation modeling (SEM) to the data using Mplus 6 (Muthén & Muthén, 2010). We first conducted confirmatory factor analyses on the

items measuring the latent constructs specified in Figure 1, in order to establish a valid and reliable measurement model. We then examined the relationship between the control variables and our study variables. We subsequently conducted structural equation modeling to test the significance of the model paths.

Results

Descriptive Results

Of the 1042 respondents, 87.9% (*n* = 916) knew the focal website addressed in this study. With respect to frequency of use, one out of four (26.3%; *n* = 274) respondents reported that they never used the website. Other respondents reported using the website seldom (25.6%; *n* = 267), sometimes (15.6%; *n* = 163), regularly (13.5%; *n* = 141), often (9.1%; *n* = 95) or very often (8.2%; *n* = 85). In Table 2, we display the extent to which respondents were willing to disclose their personal information to the focal commercial website. As a general trend we can see that respondents are relatively more inclined to disclose their identity data than other categories of information, especially contact data and data concerning their geographical location. For instance, a majority of adolescents was rather willing to definitely willing to disclose their gender, whereas a majority was definitely not planning to divulge their mobile phone number. Also a majority of respondents did not show eagerness to reveal their home city or the city where they go to school.

Table 2. Adolescents' intention to disclose specific types of personal information.

	n	Definitely not	Probably not	Rather not	Rather yes	Probably yes	Definitely yes
Identity data							
Forename	1009	12.3%	5.9%	8.0%	29.8%	22.3%	21.6%
Family name	1004	21.8%	10.6%	16.9%	21.3%	15.5%	13.8%
Birth year	1005	12.4%	7.3%	11.4%	29.6%	23.0%	16.3%
Gender	998	8.5%	4.1%	6.1%	32.9%	25.3%	23.1%
Geographical							
Home city	1000	26.7%	14.7%	25.4%	14.6%	10.5%	8.1%
School city	1002	24.8%	12.3%	21.8%	20.6%	11.6%	9.1%
Profile information							
Hobbies	1004	11.5%	8.3%	13.0%	29.1%	21.8%	16.3%
Faith	999	25.6%	11.7%	16.1%	22.3%	13.9%	10.3%
Political	995	32.5%	13.6%	21.4%	15.8%	9.4%	7.3%
Relationship	1004	26.2%	12.2%	17.3%	21.4%	11.9%	11.1%
Favourite brands	1000	19.7%	10.1%	14.0%	25.5%	16.9%	13.8%
Contact							
Email address	1002	27.8%	11.4%	19.3%	18.9%	12.3%	10.4%
Messenger ID	999	30.0%	12.7%	21.5%	15.9%	10.4%	9.4%
Mobile phone	1001	55.8%	13.8%	21.1%	4.2%	2.3%	2.8%

Measurement Model

The measurement model provided a good fit for the data (see Figure 2). The variables were treated as latent constructs, with exception of the single-item measures. All factor loadings were significant and above .49 (see Table 3).

Table 3. Unstandardised and standardised parameter estimates.

Results for measurement model				
Observed variable	**Latent construct**	***β***	***B***	**Two-tailed *p***
Ability_item1	Ability	.708	1.000	
Ability_item2	Ability	.821	1.282	.000
Ability_item3	Ability	.838	1.382	.000
Ability_item4	Ability	.689	1.111	.000
Integrity_item1	Integrity	.870	1.000	
Integrity_item2	Integrity	.864	0.972	.000
Integrity_item3	Integrity	.651	0.747	.000
Benevolence_item1	Benevolence	.790	1.000	
Benevolence_item2	Benevolence	.786	0.977	.000
Benevolence_item3	Benevolence	.710	0.932	.000
Identity_item1	WTD Identity data	.851	1.000	
Identity_item2	WTD Identity data	.781	0.989	.000
Identity_item3	WTD Identity data	.860	0.985	.000
Identity_item4	WTD Identity data	.811	0.864	.000
Geographical_item1	WTD Geographical data	.908	1.000	
Geographical_item2	WTD Geographical data	.884	0.993	.000
Profile_item1	WTD Profile data	.777	1.000	
Profile_item2	WTD Profile data	.602	0.848	.000
Profile_item3	WTD Profile data	.568	0.765	.000
Profile_item4	WTD Profile data	.714	1.012	.000
Profile_item5	WTD Profile data	.815	1.152	.000
Profile_item6	WTD Profile data	.772	1.182	.000
Contact_item1	WTD Contact data	.924	1.000	
Contact_item2	WTD Contact data	.946	1.007	.000
Contact_item3	WTD Contact data	.540	0.439	.000
TrustProp_item1	Trust propensity	.696	1.000	
TrustProp_item2	Trust propensity	.652	0.928	.000
TrustProp_item3	Trust propensity	.868	1.211	.000
TrustProp_item4	Trust propensity	.814	1.199	.000
TrustProp_item5	Trust propensity	.496	0.706	.000
Perceived_risk_item1	Perceived risk	.839	1.000	
Perceived_risk_item2	Perceived risk	.899	0.997	.000
Perceived_risk_item3	Perceived risk	.771	0.862	.000
Privacy_violation_item1	Privacy violation experience	.749	1.000	
Privacy_violation_item2	Privacy violation experience	.525	0.558	.000
Privacy_violation_item3	Privacy violation experience	.714	1.128	.000

Note: WTD = willingness to disclose

Structural Model

Figure 2 presents the structural model, including the standardised regression coefficients. The fit indices indicated a good fit for the model, except for Chi-square (due to its sensitivity to sample size). Furthermore, the model explained a fair amount of the variance in the outcome variables. As displayed in Figure 2, 53.3% of the variance in trust in the focal website could be attributed to the three trustworthiness beliefs. In all, the model accounted for 22.8% of the variance in willingness to disclose identity data, 19.6% of the variance in willingness to disclose geographical data, 23.9% of the variance in willingness to disclose contact data and 18.9% of the variance in willingness to disclose profile data.

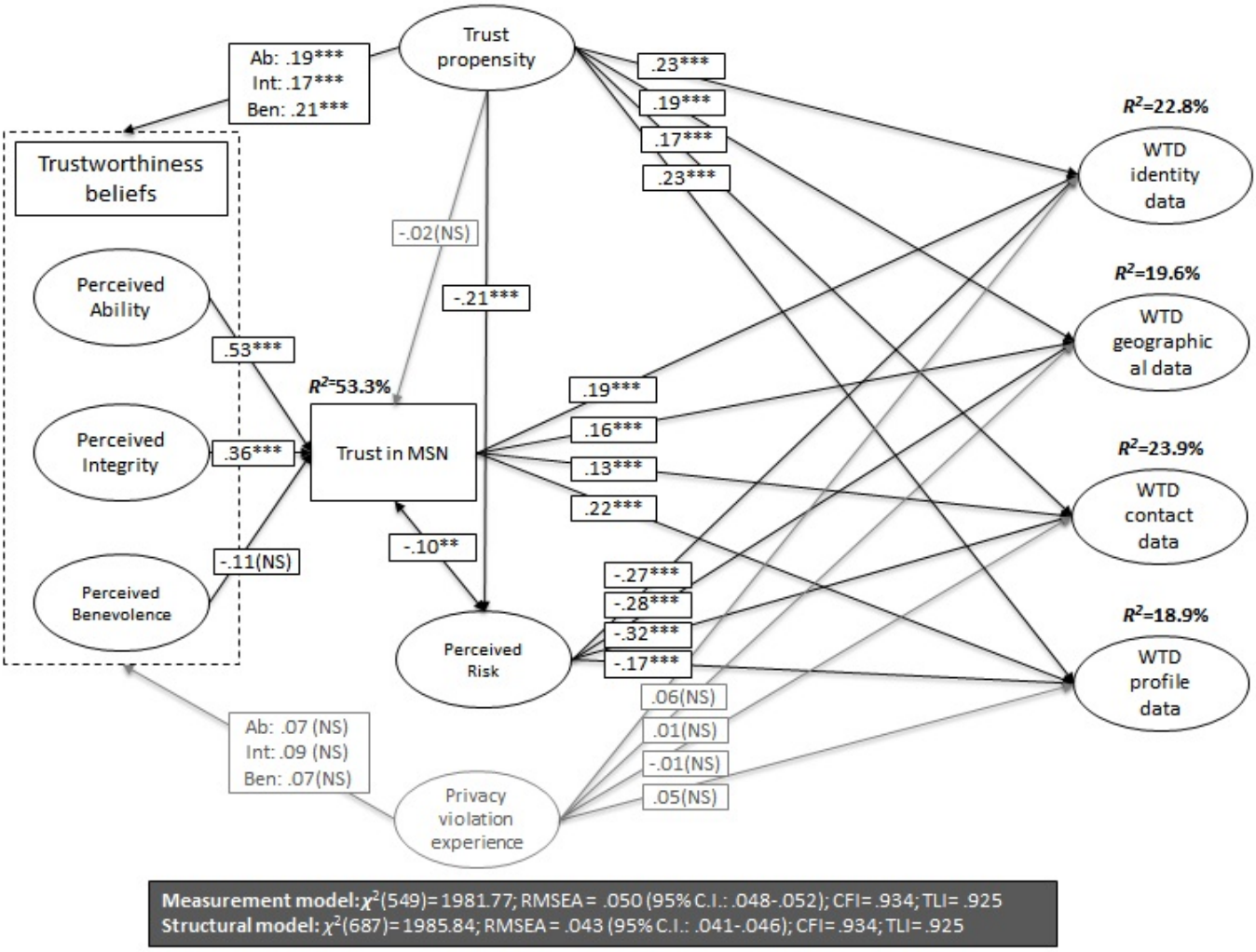

Figure 2. The integrative model of organisational trust applied to adolescents' disclosure. All reported coefficients are standardised values, adjusted for the influence of covariates. *** p<.001. Only latent constructs are displayed, while omitting manifest indicators due to space constraints.

Although the model seems to provide a succinct representation of the collected data, we found that the influence of gender (as a socio-demographic control) had a non-negligible effect, with females more inclined to disclose identity data (β =.08; p < .05), but significantly less willing to provide their contact details to msn.be (β = -.11; p < .001). Our analyses revealed no significant age effect for the disclosure of any type of personal information. The third control variable, familiarity with the focal website, was positively related to willingness to disclose all categories of personal information (identity data: β = .11, p < .001; geographical data: β = .08, p < .01; contact data: β = .16, p< .001; profile data: β = .14, p < .001).

Many of the main hypotheses were supported by the SEM analyses. Of the three factors constituting perceived trustworthiness in the focal website, perceived ability was the most important determinant of adolescents' trust in msn.be. The higher the perceived ability of msn.be was rated, the more adolescents were inclined to report that they trusted this website, thus confirming H1a (see Figure 2). The second most important determinant of trust in msn.be was perceived integrity. Confirming H1b, the more adolescents perceived this website to be honest towards it users and to act according to a set of principles of which they approved, the more they reported trust in gmsn.be. No significant relationship was found between perceived benevolence and trust in msn.be. We must therefore reject H1c.

As shown in Figure 2, our analyses demonstrate that there is no direct relationship between the trustworthiness beliefs and respondents' willingness to disclose, but that instead the influence of trustworthiness is fully mediated by the trust variable. Trust is significantly positively related to the four outcome variables of this study: willingness to disclose identity information (confirming H2a), geographical information (confirming H2b), contact information (confirming H2c) and profile information (confirming H2d). Differences, however, can be observed in the size of the regression coefficient joining each of these paths, with trust to a somewhat lesser extent predicting willingness to disclose contact data (β = .13, p < .001) compared to adolescents' willingness to disclose profile data (β = .22, p < .001).

Conversely, we found negative relationships between perceived risk and willingness to disclose these types of personal information (confirming H3a, H3b, H3c and H3d). The path between perceived risk and the willingness to disclose contact information displayed a higher regression coefficient than the paths joining perceived risk and willingness to disclose other types of data.

Additional positive relationships were found between trust propensity and intention to disclose, thereby confirming H4a, H4b, H4c and H4d. The expected positive relationships between trust propensity and perceived ability (H5a), integrity (H5b) and benevolence (H5c) were confirmed by our statistical tests. Contrary to our expectations, no significant relations could be observed between privacy violation experience and any of these trustworthiness beliefs, which implies the rejection of H8(a, b, c). Privacy violation experience was likewise no significant predictor of behavioural intention to disclose (H7a-H7d). Another relation in the model that failed to reach significance was the path between trust propensity and adolescents' level of trust in msn.be (H6). Finally, a significant negative relation was observed, as expected, between trust propensity and the perceived risk of disclosing personal data to msn.be

In the next paragraph we discuss more thoroughly the observed significant relations in the model and possible explanations for non-significant results.

Discussion

Today's commercialised digital landscape offers many opportunities for underage internet users to disclose personal data on commercially driven websites. This study aims to assess the contribution of trust and perceived risk in understanding young people's inclination to disclose four categories of personal data to a specific website (msn.be). The results of this research demonstrate that adolescents' decision-making with respect to the disclosure of their personal data to a commercial website is influenced partially by (1) their trust in the specific commercial website, (2) the level of risk they perceive to be associated with disclosure to the specific website. Our analyses, however, also indicate that (3) trust propensity – so the trust one has in general in other persons and organizations – influences adolescents' motivation to release personal data to the focal website of this study. Finally, (4) familiarity with msn.be was included in our analyses as control variable and it was shown that it significantly influences adolescents' willingness to disclose. With this result, our study supports the notion that adolescents' intention to disclose their personal data online is a mixed outcome of both adolescents' situational trust (devoted to a specific party), their level of perceived situational risk, dispositional trust and the frequency of visiting the specific website. Our analyses show that trustworthiness beliefs help to inspire trust in a specific website, but they do however lack a unique direct effect with adolescents' willingness to disclose, as their influence is fully mediated by the trust in msn.be. The full mediation of trustworthiness beliefs by trust has been found in the majority of other studies testing Mayer et al.'s model in other contexts than youth disclosure processes (Colquitt et al., 2007).

One surprising result of our study is that no positive significant relationship was found between trust propensity and adolescents' trust in msn.be. Several explanations are possible for this finding. First, in order to measure trust propensity we used an adapted scale from Rotter's original scale (1967). This scale dates back to a pre-internet era and thereby it is possibly not adapted to measure people's tendency to trust individuals and organizations online (including commercial websites). Another explanation is that trust propensity appears to be especially important in deciding whether or not to trust an 'unknown' trust referent. As demonstrated in early trust literature (Bigley & Pearce, 1998; McKnight & Kacmar, 2004), the less one knows about the person or organization, the more influencing could be the role of trust propensity in predicting trust in this trustee. In our sample, about nine out of ten adolescents had already heard at least to some extent about the website msn.be, whereas only a small share of respondents did not know the website at all. This could explain why the analyses did not yield predictive value for the relation between trust propensity and trust in msn.be

One of the strengths of Mayer et al.'s theory (1995) is that it allows us to examine the relative importance of three dimensions of trustworthiness in predicting trust in a specific party. In our study, clearly the strongest pathway was found between perceived ability and trust, followed by the path connecting trust in msn.be with perceived integrity. In short, when respondents perceived msn.be as a good and professional website, they were more likely to report higher levels of trust in the website. With respect to integrity, the more adolescents felt that the website of msn.be and its developers adhere to a set of moral ethical principles they approve of, the more likely they were to express high levels of trust in it. Contrary to expectations, we did not find a positive relationship between perceived benevolence and adolescents' trust in msn.be. Several explanations are possible for this result, including possible redundancy between perceived integrity and benevolence (Colquitt et al., 2007), although in establishing our measurement model we were able to disentangle two separate factors. Early research using both variables also failed to discern any unique effect on trust for either of the variables (Jarvenpaa, Knoll, & Leidner, 1998). Other authors (Gabarro, 1978) have combined benevolence and integrity into a single 'character' variable, thereby suggesting that the two concepts are redundant. As suggested by Mayer et al. (1995), another explanation could be that benevolence generally has less influence in early-stage exchanges between an individual and an organisation because, at that point, the trustor has little or no information on the trustee's benevolence. It is only when the relationship develops further that the trustor can gain further insight in this regard, thus allowing the relative impact of benevolence to grow. It is possible that the relationship between adolescents and the focal website of this study did not develop to the level of reciprocity in which benevolence typically emerges as a factor determining the level of trust.

We found no relationship between adolescents' experience with online privacy infringements and their willingness to disclose the four categories of personal information. Similarly, privacy violation experience did not influence adolescents' perceptions of msn.be's trustworthiness. One explanation is that only 7.4% (n = 77) of the respondents had been confronted with violations of their privacy. It is possible that due to the limited size of this small subsample our analyses failed to reach significance for the hypothesized relationships between privacy and perceived trustworthiness and trust in msn.be. Another possible explanation could be that the adolescents did not feel strongly about such negative experiences or that they considered the losses associated with disclosing their information as small relative to the benefits that the commercial website offered them in return (e.g. free access to digital content such as news, e-mail and games). Such benefits may well erase the potential negative effects of privacy violation experiences in the past. A third explanation may be that such negative experiences remain mentally linked only with the website that misused their information, thus having no effect on the level of disclosure to other websites. A fourth and final explanation may be that the lack of significance was caused by the broad operationalization of privacy violation experience. Only three general questions were asked with dichotomous answering categories (e.g. "I have experienced a misuse of my personal data"; yes/no). Possibly, measuring this concept by asking for adolescents' experience with more specific situations encompassing a violation of online privacy (e.g. "How often has your e-mail account been hacked in the past?") would have yielded significant relations between these specific experiences of privacy infringement and trust in the specific commercial websites or the discerned trustworthiness beliefs.

One strength of the present study is that it is one of the few studies so far that has tested a trust-theory based model among an adolescent sample. The overlarge majority of studies within trust literature have been conducted among adult samples (Lee & Turban, 2001; Mayer & Davis, 1999; McKnight et al., 2002). Certainly, within the area of adolescents' online information disclosure and privacy, this study is to our best knowledge the first that provides a comprehensive framework that includes characteristics of both the trustor (e.g. propensity to trust) and trustee (perceived ability and perceived integrity) in explaining the amount of data adolescents are willing to disclose to a specific site. Moreover, this study makes a further distinction between four types of personal information that adolescents typically disclose online. In doing so, this study demonstrates that adolescents' level of trust in a specific commercial website is based on a conjunction of a set of trustworthiness beliefs and at the same time the general tendency to trust. Also, the degree with which adolescents are already familiar with the trustee (i.c. msn.be) influences their willingness to entrust their personal details to this website.

One limitation of this study is the limited generalisability of its research results. In our study, the influence of the discerned trustworthiness beliefs on trust, may have been affected by the choice of one specific commercial website as trustee in the research model. As was reported before, this website was well-known among the research population, which we thought was essential for testing the proposed research model, as it would have been very difficult –if not impossible- for respondents to answer questions regarding the perceived ability, integrity and benevolence of a specific website unknown to most of them. However, based on the research methodology used in our study, we cannot exclude that the significant influence of perceived ability and perceived integrity would hold, if we had selected another commercial website as trustee in this study. Despite this limitation, we think that the importance of our study is unaffected, because it demonstrates that adolescents' willingness to disclose their personal information is the outcome of a process in which the level of trust in the specific website is determined by a conjunction of trustworthiness beliefs. Next to situational trust in the specific website, also dispositional trust plays a role in the decision adolescents make on whether or not to disclose their personal data.

Another limitation of this study is that our data are cross-sectional. We assume directionality in the observed relationships between latent variables in the model (e.g. the influence of the discerned trustworthiness beliefs on adolescents' level of trust in the specific website), but we acknowledge that reciprocal causation cannot be ruled out for any of the significant relationships yielded by our analyses. In this study, causality can only be inferred theoretically. There are indications in literature that a trustor's level of trust in a specific trustee is primarily determined by the trustworthiness beliefs that person holds on the trustee and not the other way around (Lee & Turban, 2001; Malhotra, Kim, & Agarwal, 2004). In conjunction with the present study's results, corroboration of our findings yielded by additional longitudinal analyses in the context of future research would lend additional credibility to our findings.

Another possible venue for future research is to compare the applicability of the research model by means of multi-group SEM-analyses using a larger sample than the present study did. An interesting comparison would be to split this large total sample into two groups, respectively a group with respondents with little or no experience in using the specific commercial website and another group containing respondents who use the website at a more regular pace. A possible hypothesis that could be tested in such study is whether the standardized regression coefficients displayed on the paths between trust and the disclosure variables would be higher in the 'little or no experience'-group compared to the group of regular users. Such hypothesis sprouts from the insight generated by early literature that trust functions as an 'uncertainty-reducing' mechanism (Lewis & Weigert, 1985; Luhmann, 1979). It is plausible that being unfamiliar with a specific website creates a situation of greater uncertainty from the perspective of the individual (McKnight & Cummings, 1998), who has to decide on whether or not to entrust personal details to this website. Hence, in such conditions, it may well be that trust has a stronger effect on the decision whether or not to disclose personal information. Moreover, in future research it could also be verified whether the order of importance of the discerned beliefs of trustworthiness (perceived ability, perceived benevolence and perceived integrity) is the same in both groups or whether importance of these beliefs varies across both groups.

As demonstrated by previous research (Hugl, 2011; Milne & Culnan, 2004), considerable work remains with regard to sensitising and informing internet users about how to safeguard their online privacy rights by using privacy control settings or by reading privacy policies. As observed by Malhotra et al. (2004, p. 336),"Consumers, managers and researchers should consider personal information as a double-sword." Used carefully and with the provision of sufficient information, these personal data could increase the public utility and user-friendliness of web applications. The reckless and irresponsible use of such information could lead to serious violations of the information privacy of users. Marketers should be aware that, without the online trust of adolescent internet users, the future of youth-oriented online marketing is tenuous.

Appendix

Table 4. Zero-order correlation among the variables.

Variables	1	2	3	4	5	6	7	8	9	10	11
1. Perceived ability	1										
2. Perceived integrity	.67	1									
3. Perceived benevolence	.65	.82	1								
4. WTD identity data	.19	.17	.17	1							
5. WTD geographical data	.16	.15	.14	.66	1						
6. WTD profile data	.21	.19	.18	.67	.60	1					
7. WTD contact data	.14	.12	.12	.65	.70	.53	1				
8. Trust propensity	.18	.17	.21	.31	.27	.29	.26	1			
9. Perceived risk	-.04	-.04	-.05	-.33	-.35	-.24	-.40	-.21	1		
10. Privacy violation experience	.06	.08	.05	.06	.00	.04	-.02	-.06	.01	1	
11. Trust	.70	.62	.53	.25	.21	.27	.18	.11	-.09	.05	1

References

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to we profiled online for personalization. *MIS Quarterly, 30*, 13-28.

Baker, R. K., & White, K. M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. *Computers in Human Behavior, 26*, 1591-1597.

Bargh, J. A., & McKenna, K. Y. A. (2004).The internet and social life. *Annu. Rev. Psychol.,55*, 573-590.

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

Belanger, F., 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.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*(1), 211-241.

Bigley, G. A., & Pearce, J. L. (1998). Straining for shared meaning in organizational science: Problems of trust and distrust. *Academy of Management Review, 23*, 405-421.

boyd, d. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics.* (Unpublished doctoral dissertation), University of California, Berkeley, California.

Cai, X., & Zhao, X. (2010). Click here kids! Online advertising practices on popular children's websites. *Journal of Children and Media, 4*, 135-154.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*, 181-202.

Chung, G., & Grimes, S. M. (2005). Data mining the kids: Surveillance and market research strategies in online games. *Canadian Journal of Communication, 30*, 527-548.

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

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing, 61*(2), 35-51.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Commun ACM, 46*(4), 81-83.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*, 601-620.

Friedman, B., Howe, D., & Kahn, P. (2000). Trust online. *Communications of the ACM, 43*(12), 34-40.

Gabarro, J. (1978). The development of trust, influence, and expectations. In A. G. Athos & J. J. Gabarro (Eds.), *Interpersonal behavior: Communication and understanding in relationships* (pp. 290–303), Englewood Cliffs, NJ: Prentice Hall, 1978.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega-International Journal of Management Science, 28*, 725-737.

Gefen, D. (2002).Reflections on the dimensions of trust and trustworthiness among online consumers. *SIGMIS Database, 33*(3), 38-53.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems, 24*(4), 275-286.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*, 302-318. doi: http://dx.doi.org/10.1108/07363760210433627

Gupta, R., & Kabadayi, S. (2010). The relationship between trusting beliefs and web site loyalty: The moderating role of consumer motives and flow. *Psychology & Marketing, 27*, 166-185.

Harris (2004). *National survey on consumer privacy attitudes*. Available at: http://epic.org/privacy/survey/.

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. *Internet Research, 21*, 384-407.

Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is anybody out there? Antecedents of trust in global virtual teams. *Journal of Management Information Systems, 14*(4), 29-64.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology & Management, 5*(2), 45-71.

Johnson-George, C., & Swap, W. C. (1982). Measurement of specific interpersonal-trust construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology, 43*, 1306-1317.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In A. N. Joinson, K. McKenna, T. Postmes, & U.-D. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 237-253). Oxford: Oxford University Press.

Katz, J. E., & Rice R. E. (2002). *Social consequences of Internet use.* Boston: MIT Press.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst., 44*, 544-564.

Krasnova, H., Spiekerman, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*, 109-125.

Lee, M., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.

Lenhart, A., & Madden, M. (2007). *Teens, privacy & social networks*. Washington, DC: Pew Internet & American Life Project.

Lewis, J., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*, 967-985.

Livingstone, S., Ólaffson, K., O'Neill, B., & Donoso, V. (2012).Towards a better Internet for children. London: EU Kids Online.

Lu, Y. B., Zhao, L., & Wang, B. (2010). From virtual community members to C2C e-commerce buyers: Trust in virtual communities and its effect on consumers' purchase intention. *Electronic Commerce Research and Applications, 9*, 346-360.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. Washington, DC: Pew Internet & American Life Project.

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*, 336-355.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*, 709-734.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management. *Journal of Applied Psychology, 84*, 123-136.

McKnight, D. H., & Cummings, L. L. (1998). Initial trust formation in new organizational relationships. *The Academy of Management Review, 23*, 473-490.

McKnight, D., Choudhury, V., & 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., & Kacmar C. J. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. *Electronic Markets, 14*(3), 1-15.

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.

Mesch, G. S., & Beker, G. (2010). Are norms of disclosure of online and offline personal information associated the disclosure of personal information online? *Human Communication Research, 37*, 570-592.

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior, 28*, 1471-1477. doi: http://dx.doi.org/10.1016/j.chb.2012.03.010

Moscardelli, D., & Divine, R. (2007). Adolescent's concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviours. *Family and Consumer Sciences Research Journal, 35*, 232-252. doi: http://dx.doi.org/10.1177/1077727X06296622

Metriweb (2010). Centrum voor informatie over de media: De nieuwe CIM internet studie. [Center for Information about the Media: The new CIM internet study]. Retrieved from: http://www.cim.be

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 Public Policy & Marketing, 18*(3), 15-29.

Montgomery, K. C. (2001). Digital kids: The new on-line children's consumer culture. In D. G. Singer & J. L. Singer (Eds.), *Handbook of Children and the Media* (pp 650-663). Thousand Oaks: Sage.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*, 76-98.

Muthén, L. K., & Muthén, B. O. (2010). *Mplus User's Guide* (6th ed.). Los Angeles, CA.

Paine Schofield, C. B., & Joinson, A. N. (2008). Privacy, trust, and disclosure online. In A. Barak (Ed.), *Psychological aspects of cyberspace: Theory, research, applications* (pp. 13-31). Cambridge, UK: Cambridge University Press.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S. & Hofacker, C. F. (2010). Customer information sharing with E-Vendors: The roles of incentives and trust. *International Journal of Electronic Commerce, 14*(3), 63-91.

Reichfeld, F. F.,& Schefter, P. (2000). E-loyalty. *Harvard Business Review, 78*, 105-113.

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies, 62*, 381-422.

Roca, J. C., Garcia, J. J. J., & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*, 96-113.

Ross, W., & LaCroix, J. (1996). Multiple meanings of trust in negotiation trust, trustworthiness and trust propensity: A literature review and integrative model. *International Journal of Conflict Management, 7*, 314-360.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*, 651-665.

Schouten, A. P., Valkenburg, P. M., & Peter, J. (2007). Precursors and underlying processes of adolescents' online self-disclosure: Developing and testing an "Internet-Attribute-Perception" model. *Media Psychology, 10*, 292-315.

Singh, R. I., Sumeeth, M., & Miller, J. (2010). A user-centric evaluation of the readability of privacy policies in popular web sites. *Information Systems Frontiers, 13*, 501-514.

Strater, K.,& Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1* (pp. 111-119). Liverpool, United Kingdom: British Computer Society.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*, 203-223.

Turow, J., & Nir, L. (2000). *The Internet and the family 2000: The view from parents, the view from Kids,* Philadelphia: The Annenberg Public Policy Center.

Uslander, E. (2000). Social capital and the net. *Communications of the ACM, 43*(12), 60-64.

Unnever, J. D. (2005). Bullies, aggressive victims, and victims: Are they distinct groups? *Aggressive Behaviour, 31*, 153-171.

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1), article 3. Retrieved from: http://www.cyberpsychology.eu/view.php?cisloclanku=2012051201&article=3

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*,105-125.

Youn, S. (2005). Teenagers' perception of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*, 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*, 389-418.

Correspondence to:
Wannes Heirman
Department of Communication Studies
Faculty of Political and Social Sciences

University of Antwerp
Sint-Jacobstraat 2
2000 Antwerp
Belgium
E-mail: wannes.heirman(at)ua.ac.be