



Is online trust and trust in social institutions associated with online disclosure of identifiable information online?

Gustavo S. Mesch

Department of Sociology & Anthropology, University of Haifa, Har Hacarmel 31905, Israel

ARTICLE INFO

Article history:

Available online 12 April 2012

Keywords:

Online/offline information disclosure
Online and offline trust
Internet
Computer mediated communication
Interpersonal trust

ABSTRACT

This study investigated the association between trust in individuals, social institutions and online trust on the disclosure of personal identifiable information online. Using the Internet attributes approach that argues that some structural characteristics of the Internet such as lack of social cues and controllability are conducive to a disinhibitive behavior it was expected that face to face trust and online trust will not be associated. In addition, it was expected that from the three components of trust, online trust only will be associated with the disclosure of identifiable personal information online. A secondary analysis of the 2009 Pew and American Life of Internet users ($n = 1698$) survey was conducted. In contrast with the Internet attribute approach the effect of trust in individuals and institutions was indirectly associated with the disclosure of identifiable information online. Trust in individuals and institutions were found to be associated with online trust. However, online trust only, was found to be associated with the disclosure of personal identifiable information. While trust online encourages the disclosure of identifiable information, perception of privacy risks predicted refraining from posting identifiable information online. The results show a complex picture of the association of offline and online characteristics on online behavior.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

The concept of privacy is variously defined, but consensus exists that privacy is about personal information, its control, and its disclosure (Altman, 1977; Joinson & Paine, 2007; Tufekci, 2008). Thus, with the increase in the use of the Internet, interest has also increased in the notion of self-disclosure, a dimension of privacy and a key area affected by Internet use (Bargh, McKenna, & Fitzsimons, 2002; Joinson, Reips, Buchanan, & Paine, 2010; Nosko, Wood, & Molema, 2009; Qian & Scott, 2007). Disclosure in the online environment has been defined as having two elements: the information unknown to others that the user decides to make common knowledge (Joinson & Paine, 2007) and the degree of user identifiability, that is, the ability of others to identify the virtual user as the real-world person (Gandy, 2000). A user's identifiability level is determined by a combination of his/her own decision to disclose details connecting his/her virtual identity with his/her real one.

Disclosing identifiable information is linked to the concept of trust. Trust refers to a "general expectancy held by an individual that the word, promise oral or written statement of another individual or group can be relied upon" (Rotter, 1980). In other words, it is a belief that in general, individuals and groups can be trusted (Smith, 2010). Trust ameliorates the perceived risks of disclosing

identifiable information (Krasnova, Spiekerman, Koroleva, & Hildebrand, 2010).

Online trust (e.g., trust in web sites, online news, social networking site providers) has been extensively studied (Corritore, Kracher, & Weidenbeck, 2003; Joinson et al., 2010; Krasnova et al., 2010; Paine et al., 2008). From these studies we learned that the formation of online trust is a difficult process, but when it is created, it serves to mitigate the perceptions of risk, uncertainty and vulnerability that are associated with the disclosure of personal and identifiable information. However, one important limitation of these studies is that to date none of them has compared online trust and the trust established through face-to-face (FtF) communication. In other words, we do not know if there is a differential effect of trust in individuals, trust in social institutions and online trust on the disclosure of identifiable information. The purpose of this study is to fill this gap in the literature and to investigate the factors associated with the disclosure of identifiable information. To do so, we examined the association between various forms of trust, perceptions of risk and the disclosure of identifiable information.

2. Literature review

In this section findings of public concerns over lack of privacy in online environments are presented. Next, the concept and

E-mail address: gustavo@soc.haifa.ac.il

dimensions of identifiable information and trust are defined. Finally, two theoretical models explaining the association of online and offline trust on disclosure of identifiable information are discussed.

Studies investigating Internet users' privacy concerns report that a sizeable percentage is concerned with the consequences of disclosing personal identifiable information online. In a study of a representative sample of the US population using a 5-point scale to measure the fear of disclosing personal information online, the average score was 3.75 (Turrow & Hennessy, 2007). Another study based on a large online survey found that the major concerns of Internet users were identity theft and access to and distribution of their personal information (Paine, Reips, Stieger, Joinson, & Buchanan, 2007). A more recent study that investigated the extent of privacy concerns in a representative US sample found that 55% of the respondents were more concerned with Internet privacy issues than 5 years ago and 38% were concerned at the same level (Hoofnagle, King, Li, & Turow, 2010). The results of these studies indicate a raising public concern over the disclosure of personal information online.

The concept of disclosure of identifiable information is closely associated with anonymity, e.g., a state where a person is not identifiable (Marx, 1999). Anonymity can be either discursive or visual (Scott, 2004). Discursive anonymity refers to the condition where textual communication cannot be attributed to a particular source. In an online environment people usually feel identifiable when their personal information (name, email, gender, location, etc.) is disclosed. Visual anonymity refers to the lack of any visual representation of a person, such as pictures or video clips. Conceptually, identifiable information is not dichotomous—it varies in degrees. Certain identity knowledge, for example, can be used to identify a person uniquely (e.g., a legal name and an address), while some other identity knowledge may not be as effectively used to trace a message source (e.g., information about social categorization or a pseudonym). By the same token, a picture, typically coupled with some other identity knowledge, may be enough for complete identification, whereas a photo with a blurred face may provide limited information about the subject. A personal name is less ambiguous information. In this study we focus on the discursive dimension and study the disclosure of identifiable information using a personal name.

A central motivation for posting identifiable information is trust. Trust can be defined as the willingness to accept a vulnerable situation based on a positive expectation regarding the actions of others (Bos, Olson, Gergle, Olson, & Wright, 2002). From trust derives an expectation that the actions of others, the use of our identifiable information, will be conducted according to our expectations (Holmes & Rempel, 1989). Three different dimensions relevant to this study can be identified from the discussion about the concept of trust: trust in individuals, trust in institutions and online trust. Trust in individuals is conceived as a characteristic of the person, encompassing his or her past and present experiences. The main sources of trust in individuals are early and later life experiences, mainly in interpersonal relationships (Erikson, 1964; Uslander, 2002). In that sense, trust in individuals is seen as a trait or disposition that is based on real past experiences.

Trust in institutions refers to the faith that people have in collective entities. Having trust in an institution means that individuals believe that the entity, on the whole, is competent, able to fulfill its obligations toward customers and acts in responsible ways (Devoski, Spini, & Schwartz, 2002). Trust in institutions is very different from trust in individuals (Giddens, 1990). Trust in institutions is impersonal in nature, a characteristic that makes the creation of this type of trust so difficult. Trust in institutions is of-

ten based on some public knowledge about the entity's reputation and performance.

Online trust is a difficult task to accomplish because it requires the establishment of trusting relationships in the online world. The Internet itself is an object of trust with uncertain conditions just because it is not based on dyadic or group relations alone (Wang & Emurian, 2005). Internet users perceive the online world as one in which they are uncertain about risks and the results of their online transactions. For this reason, the online environment is viewed as insecure (Friedman, Kahn, & Howe, 2000). Studies of online self-disclosure have shown a direct relationship between trust in online providers and self-disclosure. Users tend to adjust how much information they disclose based on a consideration of perceived risks and trust (Joinson et al., 2010; Krasnova et al., 2010).

As to the association between online and offline trust and its effect on the disclosure of personal information, the Internet attribute approach implicitly implies that the attributes of the Internet (relative anonymity, lack of sufficient cues and controllability) generate online behavior that is independent of offline behavior (Mesch & Becker, 2010; Schouten, Valkenburg, & Peter, 2007; Tidwell & Walther, 2002). According to this approach, structural attributes of the Internet encourage interactants to engage in more intimate exchanges in online settings than in face-to-face settings. The first attribute is reduced nonverbal cues. Computer mediated communication (CMC) is typically characterized by reduced visual, auditory, and context cues, such as social status cues. The second structural attribute assumed to enhance online self-disclosure is the controllability of CMC. The controllability of CMC allows users the time to review and edit their messages and to consider responses (Schouten et al., 2007; Walther, 1996). Fewer non-verbal cues and greater controllability reduce people's inhibitions when interacting online, perhaps leading to the rapid development of online trust that in turn may lead to increased online self-disclosure. According to the Internet attribution approach, the Internet, through its disinhibiting effect, will be positively associated both with the development of online trust and the disclosure of identifiable information. It is important to note, that according to this approach, online trust is not associated with trust in individuals or trust in institutions, but develops as a result of the attributes of the online environment.

Supporting this view, a recent study that investigated the differential effect of offline and online norms of personal information disclosure found that the correlation between online and offline norms of disclosure of personal information was very low, and online norms alone predicted the disclosure of personal information (Mesch & Becker, 2010).

In the following section the specific hypotheses (H1–H6) to be tested are described. These hypotheses are influenced by aspects of the reflective approach and the Internet attributes approach and prior research on disclosure of identifiable information in online environments. Below, we explain each hypothesis in more detail and provide references to influencing prior research.

The reflective view assumes that offline trust (e.g., trust in individuals and trust in institutions) affects online interactions. For example, people who are more trusting in general, are more trusting on the Internet as well (Katz & Rice, 2002). Furthermore, it appears that individuals who are less trusting are more likely to perceive the Internet as threatening (Uslander, 2000). Supporting this argument, a study in the UK reported that Internet users in Britain trust the Internet more, simply because they are more trusting of social institutions (Dutton & Shepherd, 2006).

Following the reflective approach, I expected to find.

H1. A positive association between trust in individuals, trust in institutions and online trust.

The Internet attribution approach implies that the structural characteristics of the Internet produce a disinhibitive effect (Bargh et al., 2002; Suler, 2004). This effect is conducive to the rapid disclosure of personal and intimate information, much more intimate and rapid than in face-to-face interactions. Following this argument, we expect that:

H2. Online trust will be positively associated with the disclosure of identifiable personal information.

The Internet attribute approach implicitly implies that the intensity of exposure to the Internet is associated with a dissociation between the norms of online and offline disclosure of information. Individuals need to become immersed in the online communication task. The higher the use of the Internet, the more likely is the user to perceive others according to internal consciousness factors, including biased impressions that lead to disclosure of online information. It is very likely that the intensity of Internet use partially underlies this process (Suler, 2004; Walther, 1996). Weisband and Kiesler (1996) postulate that a lack of technological expertise may lead users to underestimate the risk factors of exposure associated with CMC. Supporting this argument, a recent study found that adolescents who perceived reduced non-verbal cues as more relevant, were more likely to feel uninhibited online. The lower the perceived inhibition the higher the disclosure of personal information (Schouten et al., 2007). A UK study that analyzed results from the Oxford Internet Survey found that frequency of use of the Internet is positively associated with confidence in the Internet and negatively associated with perceptions of Internet risk (Dutton & Shepherd, 2006). Furthermore, respondents with stronger online skills have fewer fears about disclosing information, probably because they believe that their knowledge helps them avoid organizations that harvest personal information from web users (Turow & Hennessy, 2007).

Following this argument, in this study we expect that:

H3. There will be a positive relationship between the intensity of Internet use and the disclosure of personal identifiable information.

Studies have reported a link between privacy concerns and perceived risk (Dinev & Hart, 2006). In other words, there is concern that the use or misuse of information provided online might represent a risk for the individual. These concerns may reduce the willingness of individuals to disclose their personal information. A study investigated beliefs about surveillance and their effects on behavioral intentions to provide personal information online. The study used two measures to assess Internet privacy concerns, one related to the finding of that information and the other related to the abuse of that information. In other words, the assumption of the study was that while using the Internet, individuals may be concerned that their personal information may be found by third parties without necessarily being used maliciously. In this case the concern is based on the fact that the information is available and can be easily found. The other type of privacy concern is information abuse, that not only can the information be found, but that it can also be used for identity theft or harassment. The study found that both measures of Internet privacy concerns were negatively associated with the willingness to provide personal information online (Dinev, Hart, & Mullen, 2008). A study on motivations for the disclosure of personal information online found that perceived privacy risks are strongly and negatively associated with

self-disclosure. Thus, users adjust how much information to disclose based on perceived threats to (Krasnova et al., 2010). Given the findings in these studies, we expect that:

H4. There will be a negative association between perceptions of online risks and the disclosure of identifiable information. The higher the perception of online risks, the lower the likelihood of posting identifiable comments and information.

Age is also an important variable to consider. During adulthood, social involvement increases, accompanied by a tendency to disclose personal information. (Buhrmester & Prager, 1995). Subrahmanyam, Garcia, Harsona, Li, and Lipana (2009) studied the weblogs of 201 young adults. Accepting the thesis that the online and offline worlds are related, they predicted young blog authors would self-disclose about important concerns, including sexual identity, peers and romantic relationships. They found that blog authors used usernames, age and location to provide basic identity information about themselves. Younger bloggers were more likely to provide pictures than older bloggers. A study on the disclosure of identifiable information on social networking sites found a negative association between age and the disclosure of phone number and home address. The younger the person, the greater the likelihood of disclosure of this information online (Tufekci, 2008). In addition, a cohort effect may be present as well. Younger adults were the early Internet adopters and have experience with and developed skills to deal with Internet risks. In contrast, older users may still be wary of Internet risks and unsure about how to avoid them. Thus, in this study we expect that:

H5. Disclosure of identifiable personal information will be associated with age, so the younger the user, the more he/she will disclose identifiable information online.

Gender is another important variable associated with self-disclosure. Among adults, several studies point to a higher disclosure rate among women than men (e.g., Hinson & Swanson, 1993; Murstein & Adler, 1995; Papini, Farmer, Clark, & Micka, 1990; Sprecher & Hendrick, 2004). In studies that compared self-disclosure in face-to-face and online communication, adolescent females were reported to be more inclined than males to self-disclose (e.g., Camarena, Sarigiani, & Petersen, 1990). Specifically, while women disclosed the same amount of personal information online and in FtF communication, males were more likely to disclose more personal information in FtF communication than in an online environment (Cho, 2007). The explanation for gender differences in self-disclosure is attributed to variations in gender socialization. While men are traditionally taught to exercise restraint in sharing their feelings, women are expected to be more expressive and open in their communication. In this case, women place more importance on the reduction of uncertainty and the formation of online trust than males, and for this reason, disclose more (Cho, 2007; Dindia & Allen, 1992). Given this argument, in this study we expect that:

H6. Disclosure of online information will be dependent on gender, so women will disclose more online identifiable information than men.

3. Method

3.1. Data source and sample

This study is based on a secondary analysis of the Pew and American Life Survey (September 2009 tracking survey). Data is available at <http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx>.

Data was gathered from telephone interviews conducted by Princeton Survey Research Associates International between August 18, 2009 and September 14, 2009 among a sample of 2253 adults, age 18 and older. Interviews were conducted in both English and Spanish. In the sample there were 1698 individuals who were Internet users and this sub-sample of the original sample was used for the purposes of the analysis. At least seven attempts were made to complete an interview via the telephone number indicated by the participants.

3.2. Variable descriptions and measurements

The dependent variables of the study were:

3.2.1. Posting identifiable information online

In order to measure this concept three items from the survey were used. Each item denotes a different amount of identifiable information. Respondents were asked to indicate whether they have ever posted comments, queries or information on the Internet using their real name. A “yes” response was coded as 1 and a “no” response was coded as 0.

3.2.2. Posting information using a username

Respondents were asked to indicate if they have ever posted comments, queries or information on the Internet using a username or screen name that people associated with them. A “yes” response was coded as 1 and a “no” response was coded as 0.

3.2.3. Posting anonymously

Finally, respondents were asked to indicate if they ever posted comments, queries or information on the Internet anonymously. A “yes” response was coded as 1 and a “no” response was coded 0. Given that the three dependent variables of the study are dichotomous, we conducted a series of three logistic regressions in the multivariate analysis.

The independent variables in the study were:

3.2.4. Trust

In order to measure this concept three measures were used. *Trust in individuals* was measured with an item that asked the respondents, “Generally speaking, would you say that most people can be trusted or that you can’t be too carefully in dealing with people?” A response that indicated that “most people can be trusted” was coded as 1 and a response indicating that “you can’t be too careful” was coded as 0. *Trust in institutions* was measured with three items. Respondents were asked to indicate to what degree they felt they could trust large corporations, newspapers and television and financial companies such as banks, insurance companies and stock brokers. Responses were made on a 4-point Likert scale that ranged from “never” to “just about always” and were reverse coded, with higher values indicating a greater frequency of trust. *Online trust* was measured using three items that asked the respondents to indicate the degree to which they felt they could trust news web sites, social networking sites and web sites that provide health information. Responses were made on a 4-point Likert scale that ranged from “never” to “most of the time.” Responses were combined into a single scale by summing the responses to the items.

3.2.5. Concerns about the disclosure of personal information

Concerns about the disclosure of personal information was measured using two items. Respondents were asked to indicate the extent to which they agreed with the statement, “It bothers me that people think it’s normal to search for information about others online.” Responses were made on a 4-point Likert scale with higher values indicating more agreement. The second item asked

Table 1

T-test for differences in the characteristics of individuals posting identifiable information online.

	No	Yes
Age	50.40	42.0**
Education	4.72	4.97**
Frequency of Internet use	5.00	5.88**
Trust in individuals	.40	.46**
Trust in institutions	4.67	4.78
Online trust	3.45	3.78**
Bothered	3.48	3.03**
Worried	.31	.35*

* $p < .05$.

** $p < .01$.

respondents to indicate whether they ever worried about how much information was available about them on the Internet. Responses expressing concern were coded as 1 and responses indicating no concern as 0. Both items were introduced in the analysis as single variables.

3.2.6. Socio-demographic variables

Age was measured in years, marital status was coded 1 for married and 0 for any other family status, gender was coded as 1 for women and 0 for men, and race was coded 1 for Caucasian and 0 for other. Education was measured using an item that asked the respondents to indicate the highest level of education they had completed. The variable had eight categories and was introduced as a continuous variable in the analysis. With regard to frequency of Internet use, respondents were asked to indicate about how often they used the Internet on a 7-point Likert scale, ranging from several times a day to never. Responses were reversed coded with higher values indicating more frequent use.

4. Results

4.1. Participant characteristics

While 2253 respondents participated in the survey, we used the subset of 1698 who indicated they were Internet users. On average the respondents were 51.49 years old ($SD = 18.37$)¹ and 58% were women and 42% men. In terms of family status, 52% were married and 48% reported being currently single. As to education, 37.4% had a partial or completed high school education, 27% had completed a technical degree, 24% had completed college and 12% graduate school.

In terms of posting comments and information online, 27.7% had posted comments and information online using their real names, 31.4% had posted online using a screen name that others could identify and 11.3% had posted comments online anonymously. Regarding trust, 39% of the sample expressed a positive response on the item that measured generalized trust. The average trust in social institutions was higher ($M = 4.66$, $SD = 1.60$) than trust online ($M = 3.47$, $SD = 1.57$), both of which were measured on a scale of 1 to 10.

As to attitudes toward online privacy, 24.6% of the sample expressed concern over the amount of information that was available about them online and 53% agreed with the statement that they were concerned that people think is normal to search for information about others online.

As Table 1 illustrates, there were differences in attitudes about posting identifiable information based on trust and perceived risk.

¹ M refers to mean and SD , means standard deviation from the mean.

Some interesting differences emerge when comparing individuals who posted information using their real names and those who did not use their real names when posting information. The average age of those posting identifiable information was lower than the average age of those who did not post (42 years old vs. 50.4 years old). Level of education was also statistically significant. Those posting identifiable information tend to be more educated than the ones who post information that cannot be traced to their real names. Differences in the frequency of Internet use are statistically significant as well, with heavier Internet users being more likely to post identifiable information online. The results regarding trust provide preliminary support for the Internet attribute approach. Internet users who report posting identifiable information report, on average, higher levels of online trust than those who do not post identifiable information (3.78 vs. 3.45). At the same time, the level of trust in social institutions, is non-significant, indicating that individuals posting identifiable information and individuals who do not post such information do not differ in their reported levels of trust in social institutions. However, the measure of trust in individuals is statistically significant. The proportion of individuals reporting they trust individuals is higher for those posting identifiable information than for those who did not post identifiable information. Individuals posting identifiable information also differ from those who refrain from doing so in their perception of

risks. The former report a lower level of concern that people believe it is normal to search online information for on others than the latter. At the same time, a higher percentage of those posting identifiable information report being worried about the information about them online than those who do not post. *Multivariate Analysis.*

Next, a multivariate analysis was conducted to test the association between generalized trust, trust in social institutions and online trust. Hypothesis 1 expected to find that generalized trust and trust in institutions is positively associated with online trust. In the preliminary analysis the bivariate Pearson correlations (r) were examined. The findings from the correlation matrix indicated that the three measures of trust are associated with each other. The correlation between trust in individuals and online trust is positive and statistically significant ($r = .18, p < .01$) and there is a medium size and statistically significant correlation between online trust and trust in social institutions ($r = .42, p < .01$). At the same time, the measure of trust in individuals was associated with trust in institutions ($r = .22, p < .01$).

The multivariate analysis presented in Table 2 confirms these findings. Two socio-demographic variables were statistically significant, indicating that young respondents and those who are single express higher levels of online trust than the older and the married. Intensity of Internet use is statistically significant as well, indicating that the more hours per day individuals use the Internet, the more likely they are to express trust in websites. However, age and marital status explained only 5% of the variation in online trust. Both trust in individuals and trust in institutions are positively associated with online trust. The addition of the trust variables make an important contribution to the explained variance, as their addition increases it from 5% to 25%.

Taken together, the findings indicate that individuals who report trusting in people, also report trusting in social institutions and trusting in online websites. Thus, the findings support Hypothesis 1, which expected a reflective effect of the face to face environment on online trust.

In accordance with the Internet attribute approach, Hypothesis 2 argued that online trust will be associated with disclosure of identifiable information online. As shown in Table 3, trust in individuals is not associated with posting identifiable information online. Furthermore, trust in individuals is not associated with posting using a screen name or anonymously. Trust in social institutions was also found not statistically significant as a predictor of the likelihood of posting information with an identifiable name, using a screen name or anonymously. However, online trust had

Table 2
Ordinary Least Squares Regression predicting online trust.

Variables	B	S.E.	Beta
Age	-.006	.003	-.060*
Marital status (1 = married)	-.17	.080	-.05*
Gender (1 = female)	-.07	.07	-.02
Race (1 = white)	-.07	.11	-.01
Education	-.02	.02	-.02
Trust in individuals	.21	.08	.07**
Trust in institutions	.45	.02	.47**
Worried	-.07	.08	-.02
Bothered	.01	.02	.01
Frequency of Internet use	.05	.02	.06**
Constant	1.60	.25**	
Adj. R square	.25		

Note: B is unstandardized coefficient, S.E. standard error and Beta standardized coefficient.

* $p < .05$.

** $p < .01$.

Table 3
Logistic regression predicting posting online information.

	Posting with personal name			Posting with a screen name			Posting anonymously		
	B	S.E.	Odds	B	S.E.	Odds	B	S.E.	Odds
Age	-.03	.005	.96**	-.03	.005	.96**	-.03	.006	.96**
Marital status (1 = married)	-.007	.13	.99	-.22	.14	.79	-.35	.17	.69*
Gender (1 = female)	.02	.13	1.03	-.19	.13	.82	-.15	.16	.85
Race (1 = white)	.25	.18	1.28	.44	.19	1.55*	.21	.23	1.24
Education	.06	.04	1.06	-.003	.04	.99	.11	.05	1.11
Trust in individuals	.16	.13	1.18	-.03	.14	.97	-.03	.17	.86
Trust in institutions	-.07	.04	.92	-.08	.05	.92	-.04	.06	.95
Online trust	.11	.05	1.12*	.14	.05	1.15**	.03	.06	1.03
Worried	.24	.13	1.23	.37	.14	1.44**	.50	.17	1.65**
Bothered	-.13	.04	1.25**	-.12	.04	.87**	-.04	.06	.95
Frequency of use	.22	.04	1.25**	.26	.04	1.30**	.20	.05	1.22**
Constant	-.49	.43	.61	-.50	.46		-1.46	.58	.23**
-2 LL	1402.14			1304.67			938.49		
Chi square	131.19**			159.01			97.81		

Note: B is logistic regression coefficient, S.E. standard error and Odds are the variable contribution to the likelihood of the dependent variable.

* $p < .05$.

** $p < .01$.

a positive effect on the likelihood of posting information online using an identifiable name, thereby supporting Hypothesis 2. Furthermore, online trust was also associated with posting using a screen name that people could associate with the Internet user. At the same time, online trust did not have a significant effect on posting information online anonymously. Taken together, the results support Hypothesis 2, which argued that online trust, not trust in face-to-face communication, will be associated with self-disclosure.

Hypothesis 3 expected a positive relationship between intensity of Internet use and disclosure of identifiable information. According to Table 3, the hypothesis is not confirmed. While frequency of use is positively associated with posting identifiable information on the web, it is also positively associated with posting with an identifiable screen name and posting anonymously. Thus, frequent Internet users engage in all three types of behavior and the variable does not differentiate among them.

Hypothesis 4 expected an association between perception of risk and posting identifiable information online. The results support this hypothesis. According to the logistic regression models presented in Table 3, individuals who are concerned that others think it is normal to search for information about them online are less likely to post information or comments on the web using their real name or using a screen name that can be identified with them. The effect on posting anonymously is not statistically significant. Concerns about the amount of information available about them online also prompts people to post using a screen name and to post anonymously.

Hypothesis 5 expected a negative relationship between age and the disclosure of identifiable information. The results consistently support this hypothesis. As shown in Table 1, the average age of individuals posting comments and information using their real name is lower than those who report not doing so ($M = 42$ vs. $M = 50.4$). In the multivariate analysis shown in Table 3, age is negatively related with posting information with an identifiable name.

Hypothesis 6 expected that women would be more likely to post identifiable information than males. The multivariate analysis shown in Table 3 does not support the hypothesis. No differences were found in the behavior of men and women.

5. Discussion

Studies on online behavior have been conducted using two different approaches. One approach studies the Internet as a social space in its own right, exploring the forms of communication, sociability and behavior that are produced within this social space and how they are sustained by the resources available within the online setting. From this perspective, the Internet is viewed not as a communication channel but as a space for being or dwelling, capable of sustaining complex social spaces. In this sense, online behavior is conceived as different and even separate from one's offline norms and motivations. In this view, some Internet attributes such as the lack of cues, controllability and anonymity provide individuals with the opportunity to disclose more intimate and personal information.

A second approach regards the Internet as a cultural artifact, immersed in a social context, considering how technology is incorporated in the everyday life of individuals (Hine, 2005). In this case, the online environment is a reflection of the offline world. In such a view, individuals use the Internet to expand the possibilities of face-to-face communication and the search for information. Existing characteristics of the relationships are instrumental and central in determining which channels to use and when. Strong ties communicate using all the channels, weak ties use only some of them (Haythornthwaite, 2002). The emphasis in this view is on the actor.

The integration of the Internet into existing relationships reflects the actor's rational choices in maintaining existing social ties. Although these viewpoints are diametrically opposed, they share the view that online and offline realities are distinct or disconnected from each other, possessing different and even antagonistic properties.

The results of this study show that the online and offline worlds are connected. When investigating the antecedents of the disclosure of identifiable personal information, we found that offline trust (measured as trust in social institutions and trust in individuals) is associated with trust online. The results presented in Table 2 indicate that about 20% of the explained variance in online trust is explained by offline trust. This finding provides an important indication of the existing association between the offline and online worlds. At the same, the association is far from perfect, indicating that there are additional sources of online trust that were not measured. But even in that case, a substantial percentage of the trust that is expressed in the disclosure of online information is dependent on offline resources.

When investigating the antecedents of the disclosure of identifiable information online, offline sources of trust failed to be associated and trust in the online environment was. One might think that this finding indicates that Internet attributes (online trust) are, after all, more important than our offline values and attitudes. However, recall the previous finding indicating that offline values are indirectly related to the disclosure of personal identifiable information through their effect on online values. Furthermore, the association between attitudes about the availability of online information and self-disclosure tend to provide further support. Both measures reflect respondents' worries about the existence of private information about them online and the concern that this information is searchable. The items represent the concern with information about the real person, not the virtual one. The results of this study expand our understanding of online behavior by highlighting the complexity of the mechanism that links offline attitudes and values and online behavior.

6. Study limitations

This study has a number of limitations. First, the study is based on an existing data set whose strength is in providing information about a representative sample of the US population of Internet users. At the same time, the data set includes limited measures of trust. Furthermore, it does not include items to measure the self-disclosure of personal information in face-to-face settings, making it impossible to compare disclosure of personal information in such venues with online venues. Future research must develop measures that allow the comparison of these behaviors and their antecedents.

A second limitation is that the study relied on a single measure of identifiable information, namely disclosure of personal name. Disclosure of identifiable information is more complex and includes disclosure of visual information and narratives. Future studies should address the extent that disclosure of name is associated with the disclosure of other measures such as address, phone numbers, pictures and videos online.

This study was based on data gathered in the US. Studies have found that privacy concerns and their effect on online behavior tend to be dependent on cultural values. It is apparent that every society values privacy in some form, but the expression of this privacy varies across cultures. Cultural values may influence online privacy and disclosure concerns. For example, there is evidence that internet users from individualistic cultures were more concerned about online privacy than internet users from collectivistic cultures (Cho, Rivera, & Lim, 2009). Future studies need to address

cultural differences in the association of online trust and disclosure of identifiable information.

This study was concerned with the disclosure of identifiable information online. As more and more economic, social and leisure activities are conducted online, the environment supports exchanges with a wide variety of institutions (banks, health service providers, goods suppliers). Future studies need to address privacy concerns, trust and disclosure of personal information for specific institutions.

Another limitation is the cross sectional nature of the study. An important question that needs to be at the center of research in the coming years is that of directionality. In other words, there is a need to develop studies that allow us to examine not only how our online behavior is affected by offline values and attitudes, but how our online behavior is affecting our offline behavior. In other words, is the disclosure of identifiable information online changing our offline behavior?

Despite these limitations, this study contributes to the literature on the link between online and face-to-face trust and the differential effects of trust on the disclosure of identifiable information as the use and misuse of identifiable information remains an important topic of public concern.

References

- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33, 66–84.
- Bargh, J. A., McKenna, K. Y. A., & Fitzsimmons, 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.
- Bos, N., Olson, J., Gergle, D., Olson, G., & Wright, Z. (2002). Effects of four computer-mediated communications channels on trust development. *ACM Conference on Human Factors and Computing Systems, CHI Letters*, 4, 135–140.
- Buhrmester, D., & Prager, K. (1995). Patterns and functions of self-disclosure during childhood and adolescence. In K. J. Rotenberg (Ed.), *Disclosure processes in children and adolescents* (pp. 10–56). New York: Cambridge University Press.
- Camarena, P. M., Sarigiani, P. A., & Petersen, A. C. (1990). Gender-specific pathways to intimacy in early adolescence. *Journal of Youth and Adolescence*, 19, 19–32.
- Cho, S. H. (2007). Effects of motivations and gender on adolescents' self-disclosure in online chatting. *CyberPsychology & Behavior*, 10, 339–345.
- Cho, H., Rivera, M., & Lim, S. S. (2009). Multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11, 395–416.
- Dindia, K., & Allen, K. (1992). Sex differences in self-disclosure: A meta-analysis. *Psychological Bulletin*, 112, 106–124.
- Corritore, C. L., Kracher, B., & Weidenbeck, S. (2003). On line trust: Concepts, evolving themes a model. *International Journal of Human Computer Studies*, 58, 737–758.
- Devos, T., Spini, D., & Schwartz, S. (2002). Conflicts among human values and trust in institutions. *British Journal of Social Psychology*, 41, 481–494.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17, 61–80.
- Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance—an empirical investigation. *Journal of Strategic and Information Systems*, 17, 214–223.
- Dutton, W., & Shepherd, A. (2006). Trust in the Internet as an experience of technology. *Information, Communication and Society*, 9, 433–451.
- Erikson, E. (1964). *Childhood and society* (2nd ed.). New York: W.W. Norton.
- Friedman, B., Kahn, P. H., Jr, & Howe, D. C. (2000). Trust online. *Communications of the ACM*, 43, 34–40.
- Gandy, O. H. Jr., (2000). Exploring identity and identification in cyberspace. *Journal of Law, Ethics and Public Policy*, 14, 1085–1111.
- Giddens, A. (1990). *The consequences of modernity*. Stanford, CA: Stanford University Press.
- Haythornthwaite, C. (2002). Strong, weak, and latent ties and the impact of new media. *Information Society*, 18, 385–402.
- Hine, C. (2005). Internet research and the sociology of cyber social scientific knowledge. *The Information Society*, 21, 239–248.
- Hinson, J. A., & Swanson, J. L. (1993). Willingness to seek help as a function of self-disclosure and problem severity. *Journal of Counseling & Development*, 71, 465–470.
- Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864> 17.07.10.
- Holmes, J. G., & Rempel, J. K. (1989). Trust in close relationships. In C. Henrick (Ed.), *Close relationships* (pp. 187–202). Newbury Park, CA: Sage.
- Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In A. Joinson, K. McKenna, T. Postmes, & U. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 237–252). Oxford: Oxford University Press.
- Joinson, A., Reips, U., Buchanan, T., & Paine, C. B. (2010). Privacy, trust and self disclosure online. *Human Computer Interaction*, 25(1), 24.
- Katz, J. E., & Rice, R. E. (2002). *Social consequences of Internet use*. Boston: MIT Press.
- Krasnova, H., Spiekerman, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25, 109–125.
- Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *The Information Society*, 15(2), 99–112.
- Mesch, G., & Becker, G. (2010). Are norms of disclosure of online and offline personal information associated with the disclosure of personal information online? *Human Communication Research*, 36, 603–625.
- Murstein, B. I., & Adler, E. R. (1995). Gender differences in power and self-disclosure in dating and married couples. *Personal Relationships*, 2, 199–209.
- Nosko, A., Wood, E., & Molema, S. (2009). All about me in online social networking profiles: The case of facebook. *Computers in Human Interaction*, 26, 406–418.
- Paine, C., Reips, Ulf-Dietrich, Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet user's perceptions of privacy concerns' and privacy actions. *International Journal of Human Computer Studies*, 28, 526–536.
- Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer Mediated Communication*, 12, 1228–1252.
- Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35, 1–7.
- Scott, C. R. (2004). Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations. In S. Drucker (Ed.), *Free Speech Yearbook* (Vol. 41) (pp. 127–141). Washington, DC: National Communication Association.
- Schouten, A. P., Valkenburg, P. M., & Peter, J. (2007). Precursors and underlying processes of adolescents' online self disclosure. *Media Psychology*, 10, 292–315.
- Smith, S. S. (2010). Race and trust. *Annual Review of Sociology*, 36, 453–475.
- Subrahmanyam, K., Garcia, E. C. M., Harsona, L. S., Li, J. S., & Lipana, L. (2009). In their words: Connecting on-line weblogs to developmental processes. *British Journal of Developmental Psychology*, 27, 219–245.
- Sprecher, S., & Hendrick, S. S. (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social & Clinical Psychology*, 23, 857–877.
- Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 7, 321–326.
- Papini, D. R., Farmer, F. F., Clark, S. M., & Micka, J. C. (1990). Early adolescent age and gender differences in patterns of emotional self-disclosure to parents and friends. *Adolescence*, 25, 959–976.
- Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research*, 28, 317–348.
- Tufecki, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society*, 28, 20–36.
- Turow, Joseph, & Hennessy, Michael. (2007). Internet privacy and institutional: Insights from a national survey. *New Media and Society*, 9, 300–317.
- Uslander, E. (2000). Social capital and the net. *Communications of the ACM*, 43, 60–64.
- Uslander, E. M. (2002). *The moral foundations of trust*. Cambridge, UK: Cambridge University Press.
- Walther, J. (1996). Computer mediated communication: Impersonal, interpersonal and hyperpersonal interaction. *Communication Research*, 23, 3–43.
- Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements and implications. *Computers in Human Behavior*, 21, 105–115.
- Weisband, S., & Kiesler, S. (1996). Self-disclosure on computer forms: Meta-analysis and implications. In M. J. Tauber, V. Bellotti, R. Jeffries, J. D. Mackinlay, & J. Nielsen (Eds.), *Proceedings of the ACM CHI 96 human factors in computing systems conference* (pp. 3–10). Canada: Vancouver.