

Job Applicants' Information Privacy-Protective Response: Exploring the Roles of Technology Readiness and Trust

Completed Research Paper

Yichuan Wang
Auburn University
yzw0037@auburn.edu

Shiwei Sun
Auburn University
szs0100@auburn.edu

John R. Drake
East Carolina University
drakejo@ecu.edu

Dianne Hall
Auburn University
halldia@auburn.edu

Abstract

Firms need to acquire a wealth of information about job applicants prior to offering employment. However, the recruitment process in most firms is plagued by rising personal privacy concerns. This article draws upon the socio-cognitive theory of trust to understand the interconnected relationships among technology readiness, disposition to trust HR professionals, institutional-based trust and information privacy-protective response. The conceptual model argues that job applicants' responses to privacy protection is determined by their trust disposition on HR professionals and social networking sites and personalities toward social technologies. The model was tested with U.S. students using a job recruitment related scenario. The results provide an understanding of how job applicants respond to the privacy issue, and shed some light on the role of technology readiness and trust dispositions. This should help human resource professionals improve the recruitment process for hiring employees with perspectives that are consistent with organizational interest and culture.

Keywords

Privacy, social networks, technology readiness, trust

Introduction

An effective recruitment process is integral to a firm's prosperity; not only does it assist in maintaining a high quality of employees, but also promotes the firms' reputation in the market. Nevertheless, recruitment in most firms is plagued by rising personal privacy concerns and limited access to outside information about job applicants (Smith and Kidder 2010). Indeed, the Rasmussen Reports recently completed a survey of online users showing that 69% of American adults agree that the companies' request for access to their private information would intensify their distrust of hiring firms (Rasmussen Reports 2012). Such doubt may increase the risk of hiring an employee with perspectives contrary to organizational interest and culture (Frampton and Child 2013; Smith and Kidder 2010). To maximize the effectiveness of recruitment, it seems critical to understand the factors that affect job applicants' trust disposition and privacy-protective responses. Studies in sociology and ethics have conceptually discussed the issues of privacy and trust in job recruitment (e.g., Clark and Roberts 2010; Palm 2009; Smith and Kidder 2010). However, there is a need for a study to empirically examine the antecedents of job applicants' trust and how they respond to the firms' requests for information privacy during the recruitment process.

Antecedents such as gender, age, education, cultural difference, and personality traits have been seen as important elements in predicting intentions and behaviors with respect to privacy concerns (Chakraborty et al. 2013; Lowry et al. 2011). Particularly, personality traits have been found to influence individuals'

intention to trust on information privacy (Bansal et al. 2010; Smith et al. 2011; Stutzman et al. 2011). For example, Smith et al. (2011) developed an integrative model, namely, APCO Macro model (antecedents, privacy concerns and outcomes) emphasizing that whether one person trusts others and their responses to privacy disclosure are affected by that individual's personality differences. It is, therefore, advisable to treat personality differences as an antecedent to study privacy and trust-related issues; however, no research is being conducted in the context of the recruitment process. In this regard, this study selects technology readiness to serve as a personality-based antecedent (Jin 2013) that affects a job applicant's disposition to trust, and in turn, information privacy-protective responses. Technology readiness is viewed as personality characteristics toward technologies (Walczuch et al. 2007). It is chosen because our research context is to examine how job applicants undertake privacy protective actions as they face a request for access to their social networking sites (SNSs) by human resource (HR) department in hiring firms. In line with the above argument, this research answers the following research question: *Does a job applicant's technology readiness affect his or her disposition to trust HR professionals or SNSs, and in turn, his or her protective responses to information privacy in the recruitment process?*

To achieve this, we draw on the theory of socio-cognitive theory of trust. This theory not only emphasizes that a person's reaction is based on the degree of trust disposition, but also identifies that the trustor's personality as an antecedent has an impact on the degree of trust (Castelfranchi and Falcon 2010). By using this theory as a base, we examine the relationships among technology readiness, disposition to trust HR professionals, and protective responses of information privacy. The remainder of this paper is structured as follows: the next two sections review the existing literature and develop the hypotheses for this study. Section 4 describes the research methodology; we then present the results of the data analysis in Section 5. Finally, Sections 6 and 7 discuss the contributions of this study and implications for management scholars and practitioners.

Theoretical Framework

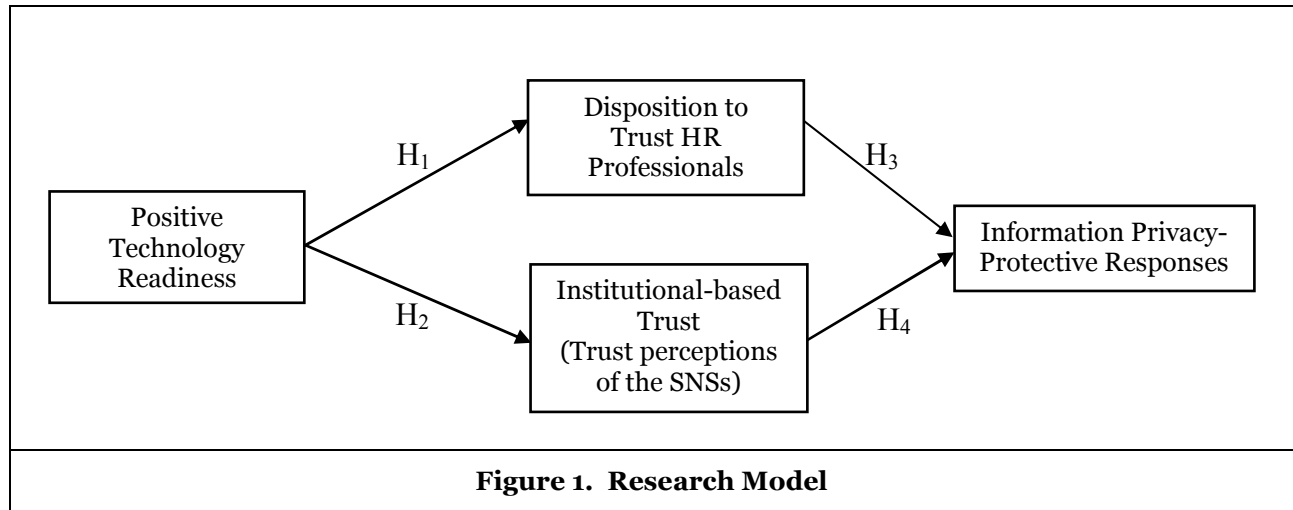
Trust research has been receiving increased attention in the context of e-commerce (e.g., Liao et al. 2011; Lu et al. 2012; McKnight et al. 2002; Wang and Hajli, 2014) and organizational behavior (e.g., Aubert and Kelsey 2003; Becerra and Gupta 2003; Jarvenpaa et al. 2004). Similarly to the context of e-commerce where trust is required between buyer and seller, trust plays an essential role between job applicants and hiring companies. The effects of trust may be changed by several contexts (Kramer 1999; Rousseau et al. 1998). Little is known about the impact of trust in the context of the recruitment process. Given the lack of trust research in the context of recruitment process, we explore the antecedents and outcomes for trust, namely disposition to trust to HR professionals and institutional-based trust as job applicants disclose their information to hiring companies. To examine this, we rely on socio-cognitive theory of trust to inform our examination of constructs that help to understand the relationships among job applicants' technology readiness, privacy trusting disposition and information privacy-protective response.

Socio-cognitive theory of trust is proposed by Castelfranchi and Falcone (2010). This theory presents a model of trust that comprises of three elements: antecedents of trust disposition (i.e., contexts, emotions, and personality), trust disposition, and decision to trust (Castelfranchi and Falcon 2010). Decision to trust refers to "the decision to depend on another person to achieve our own goals; the free intention to rely on others, to entrust the other for our welfare" (Castelfranchi and Falcon 2010, p. 64). At their core, they contend that people decide to trust, delegate to others, and take actions that are dependent on their dispositions to trust (Castelfranchi and Falcon 2010).

In addition, the socio-cognitive theory of trust has identified that personality factors should be directly connected with the trust disposition (Castelfranchi and Falcon 2010). A vast body of research holds that personalities have a relatively high impact on the trust-related constructs in the contexts of e-commerce (Lu et al. 2012; Walczuch and Lundgren 2004), social media (Pentina et al. 2013), healthcare (Bansal et al. 2010), and virtual teams (Brown et al. 2004). For example, Pentina et al. (2013) indicate that similarity in personality traits among SNSs' users has benefits in developing a robust trust in social media brand. This implies that online users' trust is deeply rooted in their personality.

With the above logic, our study aims to validate the socio-cognitive theory of trust in the context of recruitment process with a specific scenario, and disentangle the relationships among positive technology readiness, disposition to trust HR professions, institutional-based trust, and information privacy

protective responses. A visual representation of the theoretical framework can be seen in Figure 1 and the definition for each construct and its underlying dimensions is described in Table 1.



Construct and dimension	Definition	Source
Positive Technology Readiness	people’s propensity to embrace and use new technologies for accomplishing goals in home life and at work”	Parasuraman and Grewal (2000)
Disposition to Trust	the extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons	McKnight et al. (2002)
Institutional-based Trust	an individual’s perceptions of the institutional environment	McKnight et al. (2002)
Information privacy-protective responses	a set of people’s behavioral response to their perception of information privacy threats that result from certain information practices	Son and Kim (2008)

Table 1. The definition for each construct and its underlying dimensions in our model

Hypotheses Development

The Impact of Positive Technology Readiness on Trust

Technology readiness has been discussed in numerous contexts, indicating that different types of technology readiness influence people’s intentions and behaviors (Jin 2013; Lin and Hsieh 2007; Lu et al. 2012; Son and Han 2011; Walczuch et al. 2007). A study has mentioned the influence of experience with computers as a moderator on privacy concern and job applicants’ reactions in the context of online job selection (Bauer et al. 2006). They also recommend that the technology-related construct is what research related to applicant reaction should take into consideration. Moreover, according to the socio-cognitive theory of trust, personality factors are most likely to act as antecedents that help to determine trust disposition toward a specific situation (Castelfranchi and Falcon 2010).

Based on previous studies, we treat positive technology readiness as a personality factor used to describe a person’s readiness to use SNSs. In the context of recruitment process, job applicants usually face a privacy dilemma: sharing their account information to a prospective employer for the purposes of a background check. A job applicant’s disposition whether or not trust that HR professionals will protect their privacy may depend on their technology personality types. We argue that a job applicant with higher technology readiness are probably more aware of the dangers of posting inappropriate content on SNSs, and thus have a higher level of self-efficacy when it comes to managing their SNS usage (e.g., not posting anything incriminating). In other words, they have nothing to hide so that is why they are reporting a higher

trustworthiness – it is necessarily reflective of their confidence in the content of their SNS account. Additionally, those with a greater familiarity toward technology (which is closely related to technology readiness) are probably more accustomed to organizations using tools such as SNS to screen job applicants, which should add to the applicants trust with the process. Therefore, in this study, we examine whether a job applicant's positive technology readiness affects their disposition to trust HR professionals. We propose the following hypotheses.

Hypothesis 1: Job applicants high in positive technology readiness will exhibit high level of disposition to trust HR professionals during the recruitment process.

Studies have shown the impact of technology readiness on institutional-based trust in various contexts. Lin and Hsieh (2007) examine the role of a customer's technology readiness and conclude that the impact of overall technology readiness is significantly related to customer satisfaction and behavioral intentions towards self-service technologies. Recently, Lu et al. (2012) proposed a model that not only links the impact of technology readiness to customer-to-customer (C2C) platform users' trust in the context of e-commerce, but also subsequently identifies users' perceived trust as a significant determinant for consumer satisfaction. Their results indicate that consumers with an optimistic personality toward the C2C platform are most likely to perceive trust toward platform, thereby increasing their satisfaction. We believe that in our research context, individuals with positive technology readiness are more prone to believe the institutional context. This also indicates positive technology readiness significantly impacts institutional-based trust. Therefore, we propose the following hypotheses.

Hypothesis 2: Job applicants high in positive technology readiness will exhibit high level of institutional-based trust towards SNSs during the recruitment process.

The Impact of Disposition to Trust on Information Privacy-protective Responses

There has been extensive research on how people respond to information privacy concerns in the e-commerce and social media environment, but less attention has been paid in the human resource management field, particularly in the recruitment process. For example, Frampton and Child (2013) demonstrated that companies can mitigate employees' privacy resistance behaviors, by developing organization privacy orientation to encourage more openness and create an environment with high levels of communication satisfaction. This might imply that an employee's trust can be built through a robust privacy management program that reduces the employees' negative responses to privacy protection.

In the specific context of the recruitment process, job applicants have no disposition to trust HR professional during the recruitment process, which leads to raising their fears for privacy infringement. Given this circumstance, job applicants will make decisions, such as refusing employers' requests in order to protect their personal privacy. If the hiring companies cannot provide a trusting environment to share private information for job applicants, this will increase the likelihood of refusing to give information to hiring companies and speaking to their friends about a bad experience with hiring companies. Therefore, we propose the following hypotheses.

Hypothesis 3: The higher the disposition to trust HR professionals job applicants have, the lower the information privacy-protective responses during the recruitment process.

The Impact of institutional-based trust on Information Privacy-protective Responses

Trust plays a critical role for individuals to overcome perceptions of insecurity and risk in a certain social context. The effects of institutional-based trust have been studied mainly in the context of e-commerce (McKnight et al. 2002). Previous studies have indicated that the impact of trust to some extent depends on the institutional context (e.g., Frampton and Child 2013). The institutional context is tied to formal regulative structures (Zucker 1986).

However, there is little research to investigate the impact of institutional-based trust in human resource management. Under the recruitment process, applicants with higher institutional-based trust towards SNSs are likely to make them feel comfortable for the employer's request, which can reduce the perceptions of risks to a controllable level. This belief may mainly come from the regulative institutional

context. This is also consistent with the institutional-based trust in e-commerce. Institutional-based trust creates the lower possibility of lower the information privacy-protective responses. Thus, we propose the following hypotheses.

Hypothesis 4: The higher the institutional-based trust towards SNSs job applicants have, the lower the information privacy-protective responses during the recruitment process.

Research Methodology

Participants and Procedures

This study employed an online survey (hosted by Qualtrics website) to collect primary data through an email invitations. All participants were required to have at least one social media account. The participants answered the questions based on a scenario related to the privacy concerns issue during a hypothetical interview.

Overall, 253 participants completed an online survey. Unfortunately, the data used in our analyses were subject to a number of missing data points. We tested our data set to determine whether it meets the assumption of missing completely at random (MCAR) by using Little's MCAR test. The result showed that the data are missing completely at random ($\chi^2(353) = 348.940, p = .551$). By using listwise deletion, we omitted 48 subjects with missing data (Little and Rubin 1987). Finally, complete records were available for 205 subjects.

Out of the 205 subjects, 55.6% were male, and 42.9% were female (1.0% chose not to answer this question). Participants were asked to indicate their education status; 15.7% received a graduate degree, 60.0% received a bachelor's degree and 22.4% were current in college or hold a high school degree. The age range of the sample was predominately under 30 (72.7%), with several subjects over 30 (27.3%). Participants were also asked to indicate their job hunting plan over the next two months. Out of the 205 subjects, 73.1% planned to list themselves as a job applicant on a website.

Measures

All items are adapted from literature and modified as needed for this study. Positive technology readiness was assessed using the Jin (2013)'s technology readiness index that includes the dimensions of optimism and innovativeness. Disposition to trust was measured by modifying McKnight's (2002) 12-item to fit our research context. Institutional-based trust was measured using Setterstrom et al. (2012) 4-item scale.

Participants were then provided a vignette requesting them to imagine themselves in an interview where the recruiter requested SNS usernames and passwords so that the recruiter could better assess the candidate's character. This vignette was chosen to place the participant in a quandary that would elicit strong reactions and intentions to protect their privacy. This was followed by information privacy-protective responses, using the Son and Kim (2008)'s 6-items scale, that includes the dimensions of refusal and negative word-of mouth. All of the constructs in our model serve as composite variable that summarized the common variation in a collection of their underlying dimensions.

Control variables. We controlled for one individual difference that may impact on the dependent variable (i.e., information privacy protective responses). Previous research suggests that the gender influences the degree of privacy concerns (e.g., Chen and Rea 2004; Culnan and Armstrong 1999). More specifically, females have more concern about privacy than males (Sheehan 1999). Therefore, we incorporated this control variable in the research model, including gender with a dummy code (0 for male subjects; 1 for female subjects).

Common Method Bias

To reduce common method bias, Podsakoff and his colleagues (2003) suggest a structural procedures during the design of study and data collection processes. Following the guidelines, we protected respondent-researcher anonymity, provided clear directions, and proximally separated independent and dependent variables (Podsakoff et al., 2003). We then tested for bias statistically. Harman's one factor test (Greene and Organ, 1973) was used to determine if common method bias cause validity issue to our

study's results. The un-rotated factor solution indicates that no factor accounts for 50% or more of the variance, which suggests that common method bias in our study is not a significant threat to the validity.

Data Analysis and Results

Descriptive Statistics, Reliability and Validity

Table 2 presents the means, standard deviations, Cronbach's alphas, the square root of the AVEs and the construct correlations. The Cronbach's alphas (ranging from .70 to .96) show a satisfactory degree of internal consistency reliability of the measures (Bollen and Lennox, 1991). As shown in Table 2, composite reliability (CR) range from 0.81 and 0.98, with greater than the commonly accepted cutoff value of .70 (Gefen et al. 2000; Hair Jr., et al. 2010), which demonstrates adequate reliability of the measures. Discriminant validity was first assessed by examining the factor correlations. Although there are no firm rules, inter-construct correlations below |.7| provide evidence of measure distinctness, and thus discriminant validity (Ping 2003). No factor correlation is greater than .7, which demonstrates discriminant validity (see Table 2).

An exploratory factor analysis with varimax rotation for all constructs was conducted to test construct validity. The results indicate that most items loaded on a distinct construct and their factor loadings were greater than 0.5, showing a good convergent validity. The results confirmed the existence of eight observed constructs with eigenvalues greater than 1.0, and only one cross-construct loading above 0.5 emerged (the fourth item in optimism construct was deleted), meaning a good discriminant validity in this study.

Measurement Model

First, we analyzed a measurement model to assess the measurement quality of constructs by using a confirmatory factor analysis (CFA). The measurement model consists of ten latent factors and 28 indicators. The range of loadings for the four technology readiness factors are as follows: optimism, .57 to .73; innovativeness, .77 to .83. The range of loadings for the four deposition to trust factors is as follows: benevolence, .83 to .93; integrity, .83 to .94; competence, .70 to .87; trusting stance, .68 to .83. The range of loadings for the institutional-based trust response factors is from .73 to .86. The range of loadings for the two information privacy-protective response factors is as follows: refusal, .87 to .99; negative word-of-mouth, .85 to .99. The model chi-square is statistically significant ($\chi^2(314) = 478.066, p < .000$), which indicates that the exact fit hypothesis is rejected. However, this test is highly sensitive (Jöreskog and Sörbom 1989). We, therefore, examined other measures of goodness-of-fit. The comparative fit index (CFI) is .960, which exceeds the cutoff value of .80 (Hair et al. 2009) and the standardized root mean square residual (SRMR) is .0587, which is less than .08 (Hu and Bentler 1999). The root mean square error of approximation (RMSEA) is .051, which is less than .08 (Byrne 2001). Thus, we conclude that our data adequately fit the measurement model.

Variable	Mean	S.D.	α	CR	TR_O	TR_I	PTD_B	PTD_I	PTD_C	PTD_T	IBT	IPPR_R	IPPR_N
TR_O	4.56	.97	.70	.71	.67								
TR_I	4.78	1.39	.84	.84	.53**	.80							
PTD_B	3.80	1.45	.90	.90	.21**	.08	.87						
PTD_I	3.96	1.26	.91	.91	.20**	.04	.51**	.88					
PTD_C	4.54	1.15	.80	.81	.38**	.17*	.24**	.43**	.76				
PTD_T	3.74	1.33	.81	.83	.36**	.09	.37**	.53**	.43**	.78			
IBT	3.57	1.24	.88	.88	.46**	.17*	.29**	.48**	.44**	.54**	.80		
IPPR_R	5.34	1.66	.96	.96	-.05	.08	-.19**	-.14*	-.08	-.15*	-.13	.94	
IPPR_N	5.85	1.52	.95	.96	-.04	-.01	-.17*	-.12	-.06	-.15*	-.15*	.42**	.94

Note: N=205; CR: composite construct reliabilities; the square root of the AVEs on the diagonal; *p<0.05, **p<0.01, ***p<0.001

Legend: TR_O: optimism; TR_I: innovativeness; PTD_B: Benevolence; PTD_I: integrity; PTD_C: competence; PTD_T: trusting stance; IBT: institutional-based trust; IPPR_R: refusal; IPPR_N: negative word-of-mouth

Table 2. Descriptive Statistics and Correlation

Hypotheses testing

As shown in Figure 2, Hypothesis 1 and Hypothesis 2 show that the job applicants with higher levels of positive technology readiness have greater level of disposition to trust and institutional-based trust when they deal with their information privacy. Thus, our results support Hypothesis 1 and 2. Hypothesis 3 stated that the job applicants with higher disposition to trust will engage less in the negative responses of information privacy protection (i.e., refusal and negative word-of-mouth). Hypothesis 4, on the other hand, indicated that there is no significant relationship between institutional-based trust and information privacy protective responses.

Relationships	β	t-Value	p-Value	Results
Technology readiness \rightarrow Disposition to trust	.804	6.089	.000	H1 supported
Technology readiness \rightarrow Institutional-based Trust	.873	5.706	.000	H2 supported
Disposition to trust \rightarrow Information privacy-protective responses	-.412	-2.315	.021	H3 supported
Institutional-based Trust \rightarrow Information privacy-protective responses	.118	.754	.451	H4 not supported

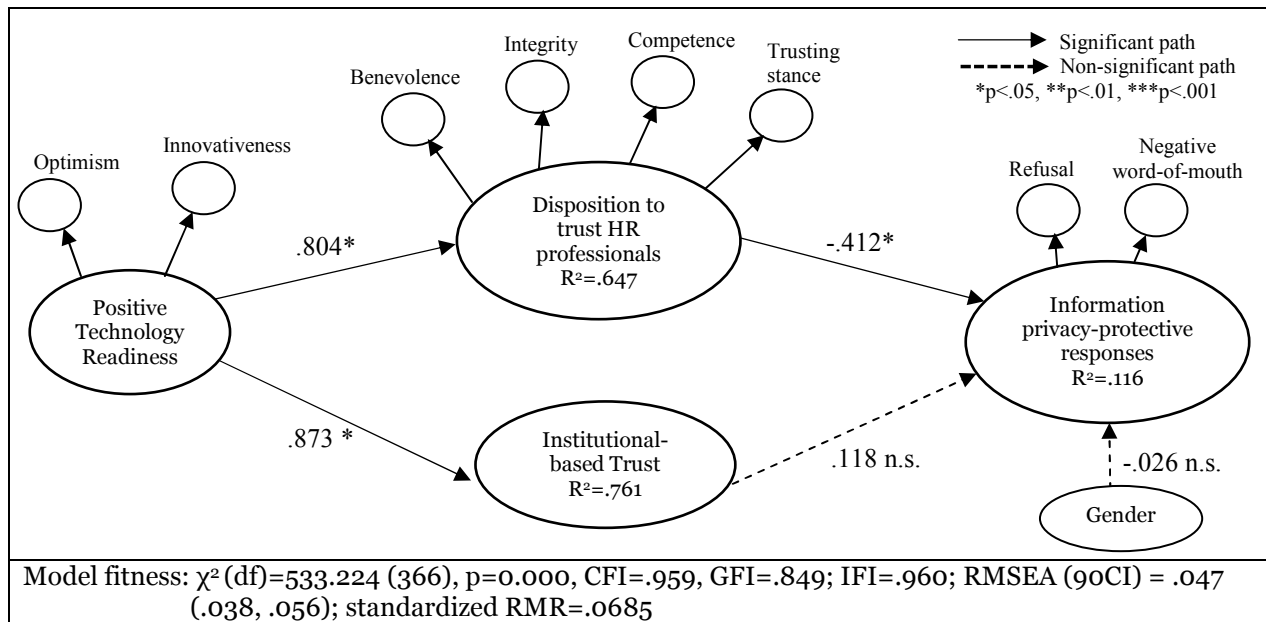


Table 3. Overview of Results

Figure 2. Estimation Results Structural Model

Discussion

Our findings not only confirm that technology readiness is an important antecedent of disposition to trust HR professional and SNSs, but also suggest that information privacy protective responses are affected by disposition to trust. The empirical evidence support our three key findings as follows.

First, our results revealed that a job applicant with a positive personality toward SNSs has a high degree of disposition to trust the recruitment process of hiring companies as well as institutional-based trust to SNSs. Studies shows that people with a tendency to be extroverted and explore new activities on SNSs are willing to make greater use of SNSs as a communication tool and belong to more SNS groups, resulting in more knowledge of SNSs feature and being sociable on SNSs (Amichai-Hamburger and Vinitzky 2010; Ross et al. 2009). It would be logical to expect that applicants with perceived optimism and

innovativeness towards SNSs should have a tendency to trust their prospective employers and SNSs to protect their privacy and to disclose their information to prospective employers because applicants have the ability to control their personal information.

Second, our result support that with a higher disposition to trust HR professionals, job applicants are less likely to refuse personal information to prospective employers and engage in negative word-of-mouth responses to other people. Specifically, when job applicants hold a positive benevolence, integrity, competence and trusting stance toward HR Professions it will reduce the probability of responding to negative privacy protective actions (i.e., refusal and negative word-of-mouth). These findings are consistent with the views of socio-cognitive theory of trust, showing that the impact of trust disposition helps to predict an applicant's decisions to privacy protection actions.

Third, contrary to our expectation our results do not show a strong link between job applicants' trust perception towards SNSs and information privacy-protective responses in the context of recruitment process. In other words, no matter what job applicants trust the SNSs or not, they do not change their privacy protection behaviors as they suffer a privacy dilemma. Based on these three key findings, we next offer insights regarding theoretical and managerial implications.

Theoretical implications

This study provides important theoretical implications in several ways. First, the impact of technology readiness as an antecedent of intention-related constructs is well discussed in the IS literature. Most studies have incorporated technology readiness into technology acceptance model (TAM) based on the theory of planned behavior (Ajzen 1991) for explaining technology usage behavior (Jin 2013; Liljander et al. 2006; Lin and Hsieh 2007; Son and Han 2011; Walczuch et al. 2007). This is one of the pioneering studies to explore the role of technology readiness as a personality trait to study people's disposition to trust. Because a handful of studies explain this relationship, our study provides new knowledge to researchers by the view of socio-cognitive theory of trust, demonstrating that technology-related personality types are able to predict trust disposition on information privacy. In this regard, this study empirically examines socio-cognitive theory of trust regarding the relationship between personality traits and trusting disposition in the context of the recruitment process.

Second, in the McKnight et al. (1998) initial trust formation model, they assert that disposition to trust is a personality-based trust, which acts as an antecedent of this model that affects trusting beliefs and intentions. However, Castelfranchi and Falcon (2010) redefined trust disposition as a threshold for a person's acceptance or avoidance on a situation, and can be affected by context, emotion, and personality factors. With this, we explored an antecedent, that is, technology readiness for trust disposition constructs. This movement may induce further research to improve McKnight et al. (1998) trust model by identifying factors for initial trust formation.

Third, job applicants' trust perception towards SNSs did not affect their responses to privacy protection in the context of recruitment process. Instead, this study indicates that job applicants' disposition to trust HR professionals will lead to their protective responses to hiring companies. This finding is inconsistent with some studies (e.g., Bansal et al. 2010; Hajli et al., 2014; Lowry et al. 2011; McKnight et al. 2002; Lu et al. 2012), who believed that users' trust toward specific technologies such as shopping websites, and self-service technologies must affect certain intentions or behaviors. For example, Bansal et al. (2010) found that users' trust in a health website is a utility enabler that positively influences users' willingness to disclose health information online. A possible explanation for the different effect of institutional-based trust is that we tested in a different context. Indeed, in the recruitment process, HR professionals play an important role in determining the applicants' perception of the organizations' image. If HR professionals are knowledgeable about the consequences of privacy violations, and they do have a higher level of proficiency with privacy protection, the job applicants will not communicate this bad experience about recruitment to their friends or others. Because of these inconsistent results, we conclude that the impact of institutional-based trust on Information privacy-protective responses will differ by context.

Managerial implications

Our findings suggest HR professionals and hiring companies should be careful using SNS technologies to improve their job candidate screening process. The relationship between disposition to trust and

information privacy protective response suggests that companies should establish a trust mechanism embedded in screening process prior to requesting privacy information. Considering our research scenario, requesting personal SNSs information is a double-edged sword recruitment strategy, which may pose huge threats to companies by extremely poor trust mechanisms. On the other word, when its power is appropriately and ethically harnessed, it has potential to understand a job applicant's usage of SNSs, thereby enabling companies to make an employment decision valid in determining who will be suitable for organizational culture and perform better on the job. Trust mechanisms such as extending friendship status to applicants by current employees (Frampton and Child 2013; Smith and Kidder 2010), and building a clear privacy policy for appropriate use of social networking information (Smith and Kidder 2010) can be a means of improving hiring quality and avoiding the adverse impacts on a job market. From these perspectives, this study is beneficial to companies struggling to improve their recruitment process.

Limitations and future research directions

There are several limitations to this study. First, with an exclusive focus on an extreme ethical quandary, our results may not be applicable to other contexts. Second, this study did not observe the actual behaviors of privacy protection for the recruitment process. As a consequence, this situation may increase the difficult making strong inferences.

In response to these limitations, we offer some suggestions regarding future research. First, future research should be considered to assess the different age groups. Similarly, our participants may not be representative of all job applicants since their ages are mostly under 30. Older job applicants may be more concerned about their private information. It is likely that for these applicants, trust in HR professionals will be harder than younger due to their lack of security, therefore this might reflect the different privacy protective actions. Second, we used socio-cognitive theory of trust to be the first study to empirically examine the relationships among proposed constructs of this theory in a specific recruitment context. Yet research is needed to consider whether other contexts will have the same results. Additionally, this theory offers other antecedents of trusting disposition, such as emotion and context factors. It should be taken into consideration for future research. Third, future research should be considered to use mixed methodologies to better understand applicants' privacy concern and privacy protective response in the recruitment process since actual privacy protective behavior is harder to evaluate. In doing so, qualitative methods, such as focus group method may offer valuable insights to complement the insufficient of survey method that allows making strong inferences.

Conclusions

Our contribution is to extend trust literature by understanding how job applicants trust and reply when they face a privacy dilemma that is triggered by hiring firms. Partial paths were supported by the socio-cognitive theory of trust and extended the applicability of this theory to the context of the recruitment process. The significant finding of this study is the impact of technology readiness on disposition to trust and institutional-based trust, and in turn, its responses to information privacy protection. As a result, this study has increased an understanding of privacy and trust perspectives in the recruitment process that will fuel the next leap in knowledge in the human resource management field.

Reference

- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.
- Amichai-Hamburger, Y., and Vinitzky, G. 2010. "Social Network Use and Personality," *Computers in Human Behavior* (26:6), pp. 1289-1295.
- Arbuckle, J. L. 2011. *Amos (Version 20.0)*. Chicago: IBM SPSS.
- Baier, A. C. 1986. "Trust and Antitrust." *Ethics* (96:2), pp. 231-260.
- Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp.138-150.

- Bauer, T. N., Truxillo, D. M., Tucker, J. S., Weathers, V., Bertolino, M., Erdogan, B., and Campion, M. A. 2006. "Selection in the Information Age: The Impact of Privacy Concerns and Computer Experience on Applicant Reactions," *Journal of Management* (32:5), pp. 601-621.
- Bollen, K., and Lennox, R. 1991. "Conventional Wisdom on Measurement: A Structural Equation Perspective," *Psychological Bulletin* (110:2), pp. 305-314.
- Brewer, M. B., Campbell, D. T. and Crano, W. D. 1970. "Testing a Single-Factor Model as an Alternative to the Misuse of Partial Correlations in Hypothesis-Testing Research," *Sociometry* (33:1), pp. 1-11.
- Brown, H. G., Poole, M. S., and Rodgers, T. L. 2004. "Interpersonal Traits, Complementarity, and Trust in Virtual Collaboration," *Journal of Management Information Systems* (20:4), pp. 115-137.
- Byrne, B. M. 2001. *Structural Equation Modeling With Amos: Basic Concepts, Application, and Programming*. New Jersey: Lawrence Erlbaum Associates.
- Caers, R., and Castelyns, V. 2011. "LinkedIn and Facebook in Belgium: The Influences and Biases of Social Network Sites in Recruitment and Selection Procedures," *Social Science Computer Review* (29:4), pp. 437-448.
- Castelfranchi, C., and Falcone, R. 2010. *Trust Theory: A Socio-Cognitive and Computational Approach*. Chichester: Wiley.
- Chakraborty, R., Vishik, C., and Rao, H. R. 2013. "Privacy Preserving Actions of Older Adults on Social Media: Exploring the Behavior of Opting out Of Information Sharing," *Decision Support Systems* (55:4), pp. 948-956.
- Chen, K. C., and Rea, A. I. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *Journal of Computer Information Systems* 44(4), pp. 85-92.
- Clark, L. A., and Roberts, S. J. 2010. "Employer'S Use of Social Networking Sites: A Socially Irresponsible Practice," *Journal of Business Ethics* (95:4), pp. 507-525.
- Cole, M. S., field, H. S., Giles, W. F., and Harris, S. G. 2009. "Recruiters' Inferences Of Applicant Personality Based On Resume Screening: Do Paper People Have A Personality?" *Journal of Business and Psychology* (24:1), pp. 5-18.
- Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.
- Cvetkovich, G., Siegrist, M., Murray, R., and Tragesser, S. 2002. "New Information and Social Trust: Asymmetry and Perseverance of Attributions about Hazard Managers," *Risk Analysis* (22:2), pp. 359-367.
- Dipboye, R. L., and Jackson, S. L. 1999. "Interviewer Experience and Expertise Effects," In *The Employment Interview Handbook*, R. W. Eder and M. M. Harris (eds.), Thousand Oaks, CA: Sage.
- Falcone, R., and Castelfranchi, C. 2001. "Social Trust: A Cognitive Approach," In *Trust and Deception in Virtual Societies*, C. Castelfranchi, Y. H. Tan (eds.), Dordrecht: Kluwer, pp. 55-90.
- Frampton, B. D., and Child, J. T. 2013. "Friend or Not to Friend: Coworker Facebook Friend Requests as an Application of Communication Privacy Management Theory," *Computers in Human Behavior* (29:6), pp. 2257-2264.
- Gefen, D., Rigdon, E. E., and Straub, D. 2011. "An Update and Extension to SEM Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. Iii-Xiv.
- Gefen, D., Straub, D., and Boudreau, M. 2000. "Structural Equation Modeling And Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:7), pp. 1-77.
- Greene, C. N. and Organ, D. W. 1973. "An Evaluation of Causal Models Linking the Received Role with Job Satisfaction," *Administrative Science Quarterly* (18:1), pp. 95-103.
- Greene, C. N., and Organ, D. W. 1973. "An Evaluation of Causal Models Linking the Received Role with Job Satisfaction," *Administrative Science Quarterly*, 95-103.
- Hair Jr., J., Black, W., Babin, B. and Anderson, R. 2010. *Multivariate Data Analysis: With Readings (7th Ed.)*, Upper Saddle River NJ: Pearson Education Inc.
- Hair, J. F., Anderson, R. E., Tatham R. L., and Black, W. C. 2009. *Multivariate Data Analysis*. Englewood Cliffs, New Jersey: Prentice Hall.
- Harman, H. H. 1960. *Modern Factor Analysis*, Chicago, IL: University of Chicago Press.
- Hajli, N., Lin, X., Featherman, M.S., Wang, Y. 2014. "Social Word of Mouth: How Trust Develops in the Market," *International Journal of Market Research*, (56:5), pp. 673-689.
- Hu, L. T., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.

- Jiang, Z., Heng, C. S., and Choi, B. C. F. 2013. "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.
- Jin, C. H. 2013. "The Effects of Individual Innovativeness on Users' Adoption of Internet Content Filtering Software and Attitudes toward Children's Internet Use," *Computers in Human Behavior* (29:5), pp. 1904-1916.
- Jöreskog, K. G., and Sörbom D. 1988. *Prelis: A Program for Multivariate Data Screening and Data Summarization. A preprocessor for LISREL*. Mooresville: Scientific Software, Inc.
- Kline, R. B. 2010. *Principles and Practice of Structural Equation Modeling (3rd Edition)*. New York: The Guilford Press.
- Kluemper, D. H., and Rosen, P. A. 2009. "Future Employment Selection Methods: Evaluating Social Networking Web Sites," *Journal of Managerial Psychology* (24:6), pp. 567-580.
- Kluemper, D. H., Rosen, P. A., and Mossholder, K. W. 2012. "Social Networking Websites, Personality Ratings, and the Organizational Context: More Than Meets the Eye?" *Journal of Applied Social Psychology* (42:5), pp. 1143-1172.
- Kramer, R. M. 1999. "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions," *Annual Review of Psychology* (50), pp. 569-598.
- Lankton, N. K., McKnight, D. H., and Thatcher, J. B. 2012. "The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue Using a Social Networking Website," *IEEE Transactions on Engineering Management* (59:4), pp. 654-665.
- Lee, H. Y., Qu, H., and Kim, Y. S. 2007. "A Study of the Impact of Personal Innovativeness on Online Travel Shopping Behavior - A Case Study of Korean Travelers," *Tourism Management* (28:3), 886-897.
- Lewis, J. D. and Weigert, A. J. 1985. "Trust as a Social Reality," *Social Forces* (63:4), pp. 967-985.
- Lin, J. S. C., and Hsieh, P. L. 2007. "The Influence of Technology Readiness on Satisfaction and Behavioral Intentions toward Self-Service Technologies," *Computers in Human Behavior* (23:3), pp. 1597-1615.
- Little, G. L., and Robinson, K. D. 1987. "One-Day Dropouts from Correctional Drug Treatment. II.," *Psychological Reports* (60:2), pp. 454.
- Lowry, P. B., Cao, J. W., and Everard, A. 2011. "Privacy Concerns versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems* (27:4), pp. 163-200.
- Lu, J., Wang, L. Z., and Hayes, L. A. 2012. "How Do Technology Readiness, Platform Functionality and Trust Influence C2c User Satisfaction?" *Journal of Electronic Commerce Research* (13:1), 50-69.
- McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model," *Journal of Strategic Information Systems* (11:3-4), pp. 297-323.
- Mcknight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), pp. 473-490.
- Metzger, M. J. 2004. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9:4).
- Möllering, G. 2001. "The Nature of Trust: From Georg Simmel to A Theory of Expectation, Interpretation and Suspension," *Sociology* (35:2), pp. 403-420.
- Palm, E. 2009. "Securing Privacy at Work: The Importance of Contextualized Consent," *Ethics and Information Technology* (11:4), pp. 233-241.
- Parasuraman, A., and Grewal, D. 2000. "The Impact of Technology on the Quality-Value-Loyalty Chain: A Research Agenda," *Journal of the Academy of Marketing Science* (28:1), pp. 168-174.
- Pentina, I., Zhang, L., and Basmanova, O. 2013. "Antecedents and Consequences of Trust in a Social Media Brand: A Cross-Cultural Study of Twitter," *Computers in Human Behavior* (29:4), pp. 1546-1555.
- Ping, R. A. 2003. *Testing Latent Variable Models with Survey Data*. Retrieved from www.wright.edu/~robert.ping/lv/toc1.htm.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology*, (88:5), 879.
- Rasmussen Reports. 2012. *33% Think Employers Have Right To Fire Those Who Post Inappropriate Facebook Content*. Retrieved from: http://www.rasmussenreports.com/public_content/business/jobs_employment/march_2012/33_think_employers_have_right_to_fire_those_who_post_inappropriate_facebook_content.
- Rigdon, E. E. 1998. "Advanced Structural Equation Modeling: Issues and Techniques," *Applied Psychological Measurement* (22:1), pp. 85-87.
- Ross, C., Orr, E. S., Sisc, M., Arseneault, J. M. Simmering, M. J., and Orr, R. R. 2009. "Personality and Motivations Associated with Facebook Use," *Computers in Human Behavior* (25:2), pp. 578-586.
- Rousseau, D. M. 1998. "Trust in organizations: Frontiers of Theory and Research," *Administrative Science Quarterly* (43:1), pp. 186-188.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.
- Smith, W. P., and Kidder, D. L. 2010. "You've Been Tagged! (Then Again, Maybe Not): Employers and Facebook," *Business Horizons* (53:5), pp. 491-499.
- Son, J. Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.
- Son, M., and Han, K. 2011. "Beyond the Technology Adoption: Technology Readiness Effects on Post-Adoption Behavior," *Journal of Business Research* (64:11), pp. 1178-1182.
- Stutzman, F., Capra, R., and Thompson, J. 2011. "Factors Mediating Disclosure in Social Network Sites," *Computers in Human Behavior* (27:1), pp. 590-598.
- Urbano, J., Rocha, A. P., and Oliveira, E. 2013. "Chap. 23: A Socio-Cognitive Perspective of Trust," In *Agreement Technologies, Law, Governance and Technology Series*, S. Ossowski (eds.), Springer, pp. 419-429.
- Walczuch, R., and Lundgren, H. 2004. Psychological Antecedents of Institution-Based Consumer Trust in E-Retailing," *Information & Management* (42:1), pp. 159-177.
- Walczuch, R., Lemmink, J., and Streukens, S. 2007. "The Effect of Service Employees' Technology Readiness on Technology Acceptance," *Information & Management* (44:2), pp. 206-215.
- Wang, Y., and Hajli, M. N. 2014. "Co-creation in Branding through Social Commerce: The Role of Social Support, Relationship Quality and Privacy Concerns," *In Proceedings of Twentieth Americas Conference on Information Systems*, Savannah, Georgia.
- Wiedmann, K. P., Hennins, N., Varelmann, D., and Reeh, M. O. 2010. "Determinants of Consumers' Perceived Trust in IT-Ecosystems." *Journal of Theoretical and Applied Electronic Commerce Research* (5:2), pp. 137-154.
- Xu, X. W., and Galloway, R. 2005. "Using Behavioral Modeling Technology to Capture Designer's Intent," *Computers in Human Behavior* (21:2), pp. 395-405.

Appendix 1. Research Scenario

In order to understand job applicants' trust and privacy perspectives to hiring firms, this study considers the following scenario in this study.

Scenario: Imagine you are interviewing with an organization for a position that perfectly fits your skills, location, salary, and working conditions. During the interview, the interviewer informs you that due to problems in the past, they now request all job applicants to share their username and password to all social media accounts to help establish the character of the applicants. The interviewer indicates that they will review these accounts over the coming two weeks and then make their decision. This scenario aims for examining how job applicants respond to privacy protection, as they face a privacy dilemma that is triggered by hiring firms.

Appendix 2. Scale items and EFA factor loadings

Technology readiness (adopted from Jin 2013)

Optimism

1. Technological functions and services provided by SNS gives people more control over their daily lives. (.556)
2. You prefer to use the most advanced technological functions and services provided by SNS available. (.652)
3. Technological functions and services provided by SNS make you more efficient in your occupation. (.829)
4. Learning about technology can be as rewarding as the technology itself. (-)

Innovativeness

1. You keep up with the latest technological developments and the advanced services provided by SNS in your areas of interest. (.809)
2. You enjoy the challenge of figuring out high-tech gadgets and new issues. (.897)
3. You find you have fewer problems than other people in making technology work and advanced function of SNS for you. (.794)

Disposition to Trust (adopted from McKnight et al. 1998; 2001)

Benevolence

1. In general, people really do care about the privacy of others. (.864)
2. The typical person is sincerely concerned about respecting the privacy of others. (.8905)
3. Most of the time, people care enough to try to be considerate of others privacy, rather than just looking out for themselves. (.819)

Integrity

1. In general, most folks keep their promises to keep private things private. (.819)
2. I think people generally try to back up their promises of confidentiality with their actions. (.865)
3. Most people are honest in their desire to protect the privacy of others. (.792)

Competence

1. I believe that most professional people do a very good job at protecting privacy. (.673)
2. Most professionals are very knowledgeable about the consequences of privacy violations. (.860)
3. A large majority of professional people are competent at keeping personal information private. (.790)

Trusting Stance

1. I usually trust people to respect my personal information until they give me a reason not to trust them. (.581)
2. I generally give people the benefit of the doubt that they can protect personal information when I first meet them. (.819)
3. My typical approach is to trust new acquaintances with respecting personal information until they prove I should not trust them. (.826)

Institutional-based Trust (adopted from Setterstrom et al. 2012)

1. I believe social networks have enough safeguards to make me feel comfortable using it. (.811)
2. I feel assured that legal and technological structures adequately protect me from problems on social networks. (.800)
3. I feel confident that encryption and other technological advances on social networks make it safe for me to use. (.826)
4. In general, social network technology provides robust and safe environment to share private information. (.719)

Information privacy-protective response (adopted from Son and Kim 2008)

Refusal

Please specify the extent to which you would refuse to give your username and password to the organization because you think it is too personal.

1. Very unlikely/very likely (.933)
2. Not probable/probable (.914)
3. Impossible/possible (.930)

Negative Word-of-Mouth

Please specify the extent to which you would speak to your friends and/or relatives about the interviewer's request.

1. Very unlikely/very likely (.942)
2. Not probable/probable (.903)
3. Impossible/possible (.943)