Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Trust in the Social Computing: The Case of Peer-to-Peer (P2P) File Sharing Networks

Heng Xu
Penn State University, hxx4@psu.edu

Tamara Dinev
Florida Atlantic University, tdinev@fau.edu

Hao Wang
Penn State University, huw6@psu.edu

Rachida Parks
Pennsylvania State University, rfp127@psu.edu

Trust in the Social Computing: The Case of Peer-to-Peer (P2P) File Sharing Networks

Heng Xu
Penn State University, University Park
hxx4@psu.edu

Tamara Dinev
Florida Atlantic University, Boca Raton
tdinev@fau.edu

Hao Wang
Penn State University, University Park
huw6@psu.edu

Rachida Parks
Penn State University, University Park
rfp127@psu.edu

ABSTRACT

Social computing and online communities are changing the fundamental way people communicate and share information. Social computing focuses on how users may have more autonomy to express their ideas and participate in social exchanges in various ways, one of which may be Peer-to-Peer (P2P) file sharing. Given the risk of opportunistic behavior by malicious and/or criminal communities within the P2P networks, it is crucial to understand the factors that affect individual's usage of P2P sharing software. In this paper, we develop and empirically test a research model which includes trust beliefs and perceived risks as two major antecedent beliefs to the usage intention. Six trust antecedents are assessed including knowledge-based trust, cognitive trust, and both organizational and peer-network factors of institutional trust. Our preliminary results show general support for the model, and offer some important implications for software vendors in P2P sharing industry and regulatory bodies.

Keywords

Social Computing, Trust, Risks, Peer-to-Peer (P2P) File Sharing, Network-Based Community.

1. INTRODUCTION

A collection of new applications and services that facilitate user collective action and social interaction through the exchange of rich information and knowledge has been driving a dramatic evolution of the Web and has become increasingly important (Ip and Wagner 2008; Parameswaran and Whinston 2007). Examples include blogs, wikis, social bookmarking, user-driven ratings, peer-to-peer networks, photo and video sharing communities, and social networking. In the literature, these technologies have been variously referred to as *social computing*. Formally, social computing has been defined as a type of computing application that serves as an intermediary or a focus for a social relation (Schuler 1994). A more recent definition incorporates the concept of richness, i.e. the set of "applications and services that facilitate collective action and social interaction online with rich exchange of multimedia information and evolution of aggregate knowledge" (Parameswaran and Whinston 2007, p.762).

The name and the definition reflect the increased role of computing in social structures, in empowering individual users and communities and not just institutions (Parameswaran and Whinston 2007; Wang et al. 2007). Social computing platforms share several features that differentiate them from traditional organizational computing and content sharing. Specifically, these platforms tend to be decentralized, dynamic, and flexibly structured in terms of how information is gathered and distributed (Parameswaran and Whinston 2007; Wang et al. 2007).

Social computing is having a profound impact on the global economy by impacting the social structure (Charron et al. 2006) and the technology development (Ip and Wagner 2008). In terms of social structure, individuals increasingly take cues from one another rather than from public or private organizations such as corporations, media, religion and political institutions. Charron et al. (2006) point to several important tenets driven by the social computing: innovation shift from top-down to bottom-up; value shift from ownership to experience; power shift from institutions to communities. Such shift from institutions to communities informs also a shift in risk and trust perceptions and their importance to the community members. Through these platforms users routinely engage with members with whom they have little or no prior interaction. This exposes users to an even greater risk of opportunistic behavior by malicious or criminal communities that can make use of the anonymity, fault-tolerance,

robustness, and low cost of online communities to build platforms for illegitimate interaction, communication, and data exploration (Parameswaran and Whinston 2007). Given that users face realistic concerns pertaining to social computing, we seek in this paper to understand what steps can be taken to increase users' trust and reduce their risk perceptions so as to encourage legitimate interactions in social computing platforms.

Drawing on the conceptual and integrative development of trust in the IS literature in recent years, we develop a research model that incorporates multiple, interrelated factors contributing to the formation of trust beliefs and test the research model in the context of peer-to-peer networks. In developing the research model, we identify new trust-building mechanisms, namely peer-network situational normality and peer-network structural assurances. In what follows, we describe the theoretical foundation that guides the development of the research hypotheses, the methodology and findings. The paper concludes with a discussion of the results, the practical and theoretical implications of the findings, and directions for future research.

2. THEORETICAL FOUNDATION AND RESEARCH HYPOTHESES

2.1. Peer-to-Peer (P2P) Networks

Peer-to-peer (P2P) networks consists of nodes communicating directly for the purpose of exchanging content files, with no centralized governing node (Schoder and Fischbach 2003). Each participant in the P2P network can behave either as a client, receiving files, or as a server, sending files, or both (see Hughes et al. 2008 for a review). For this study, P2P sharing software is defined as an application running P2P sharing technology dedicated for searching, downloading and sharing digital resources among peer users. In this study, we only focus on examining the voluntary use of free P2P software.Furthermore, we focus on those P2P sharing network where all peers are equal and anonymous[1] (Reiter and Rubin 1999); without central administrators or power peers who have the capability to control other peers.

2.2. Risks in P2P File Sharing

Risk has been generally defined as the uncertainty resulting from the potential for a negative outcome (Havlena and DeSarbo 1991) and the possibility of the another party's opportunistic behavior that can result in losses for one self (Ganesan 1994; Yates and Stone 1992). Perceived risks affect individuals' intention and actual usage of a technology especially in a high uncertain environment, such as online shopping (Jarvenpaa and Tractinsky 1999). An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of these consequences (Peter and Tarpey 1975). The negative perceptions related to risk may affect an individual emotionally, materially, and physically (Moon 2000).

In the P2P sharing context, a user could be exposed to uncertainties related to three sources: *peers* (including the user herself), the *vendor of the P2P sharing software*, and *the Internet*. The user, therefore, may perceive that there is some probability of suffering a loss when downloading or sharing resources in the P2P network. Without proper control of the risk in P2P sharing, a user may choose not to use the software due to high risks (PEW-Internet and American-Life-Project 2004).. In this study, we define users' perceived risks in using P2P sharing software as users' perception that there is some probability of suffering a loss when downloading or sharing resources in the P2P network.

2.3. Trust

Trust has received a great deal of attention from scholars in the disciplines of social psychology (e.g., Lewicki and Bunker 1995), sociology (e.g., Lewis and Weigert 1985), management (e.g., Lane and Bachmann 1996), and marketing (e.g., Moorman et al. 1993). In examining the published literature, various definitions of trust have been proposed in many different ways. Nevertheless, across disciplines there is consensus that trust is a crucial enabling factor in relations where there is uncertainty, interdependence, risk, and fear of opportunism (Hoffman et al. 1999;

[1] Reiter and Rubin (1999) conceptualized three degrees of anonymity: 1) type, which states sender or receiver anonymity; 2) adversary, or who is trying to break the anonymity, and 3) degree, which may range from absolute privacy (imperceptible presence) to possible innocence, to exposed (to the adversary), to provably exposed (to others). In P2P sharing, peer anonymity is referred as a peer's identity hidden from other peers (type), but with the possibility of being exposed to a malicious peer (adversary and degree).

Mayer et al. 1995b; McKnight and Chervany 2002). Like most researchers, we have adopted the conceptualization of trust as a set of specific *trust beliefs* with three specific beliefs that are utilized most often (e.g., Bhattacherjee 2002; McKnight et al. 2002; Pavlou and Gefen 2004): competence (ability of the trustee to do what the trustor needs), benevolence (trustee caring and motivation to act in the trustor's interests), and integrity (trustee honesty and promise keeping).

In the context of P2P sharing, the absence of proven guarantees that vendors and other users or third parties will not engage in harmful opportunistic behaviors, trust is crucial in helping users overcome their perceptions of uncertainty and risk (Jarvenpaa and Tractinsky 1999; Kollock 1999). Research has shown that vendors' trustworthiness attributes are important to users. Following trust definition in e-commerce and other contexts (Ganesan 1994; Gefen et al. 2003a; Giffin 1967), we define *trust of P2P vendors* as a set of *specific beliefs* dealing primarily with the integrity, benevolence, and competence of vendors. Lack of trust and high risks (e.g., security risks and legal risks in terms of copyright infringement) have seriously undermined the development of consumer-friendly P2P business initiatives (Hughes et al. 2008).

Existing research on trust in information systems has examined a number of trust antecedents: institution-based trust (structural assurance beliefs and situational normality beliefs), knowledge-based trust (direct knowledge of or experiential interaction with a trustee), cognition-based trust (reputation categorization process), and personality-based trust (trust propensity). The first three types of trust antecedents are the focus of this study and are discussed below. The following sections develop and elaborate the key constructs and the theoretical rationale for the causal relationships among the constructs in the research model (See figure 1).

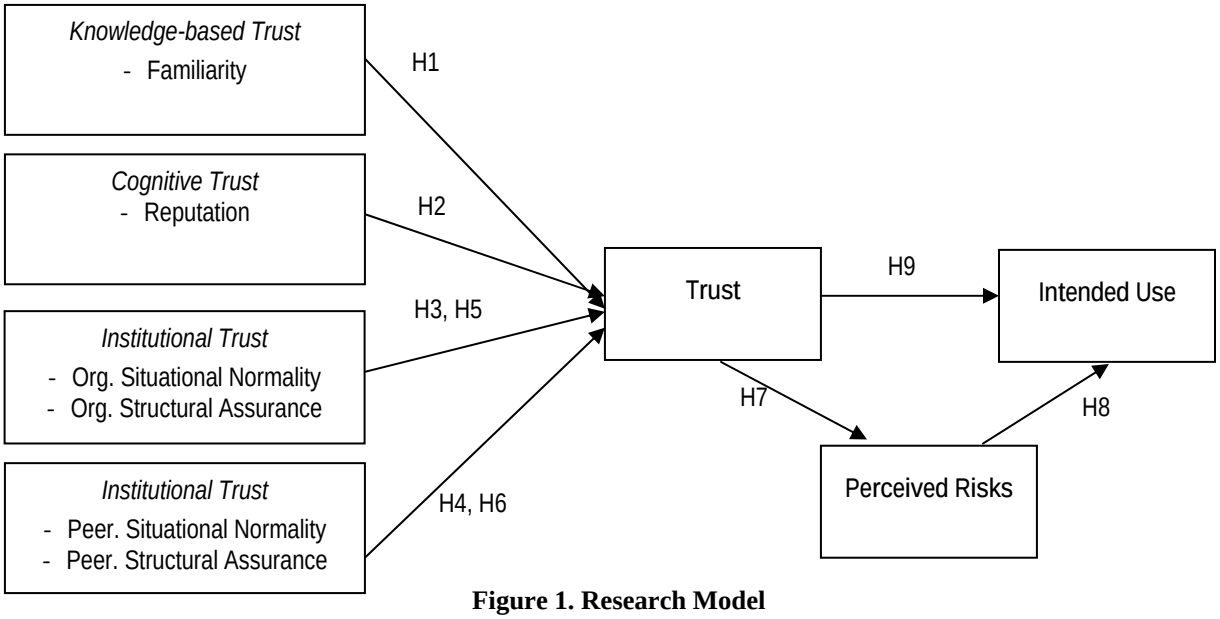


Figure 1. Research Model

2.4. Knowledge-Based Trust

Familiarity with vendors comes from prior first-hand experience. It is suggested that familiarity builds trust in a priori trustworthy party (Luhmann 1979) and validated in e-commerce context (Gefen et al. 2003a). In P2P sharing, familiarity with a vendor, for example, refers to how knowledgeable a user is about the procedures and techniques for performing P2P sharing activities. It is suggested that trust in an a priori trustworthy party grows as the trust relevant knowledge is accumulated from experience with the other party (Lewicki and Bunker 1995). In e-commerce, familiarity with e-vendors is found to lead to higher trust in vendors (Gefen et al. 2003a). In P2P sharing, trust-relevant knowledge that is derived from prior experiences, such as the procedures and techniques for performing P2P sharing activities, should help the development of trust in the software vendor. Therefore, we hypothesize:

H1: Familiarity with the vendor of P2P sharing software positively affects trusting beliefs.

2.5. Cognitive Trust

Cognition-based trust is formed via categorization processes in which individuals place more trust in people similar to themselves and assess trustworthiness based on second-hand information and on stereotypes (Gefen et al. 2003a; McKnight et al. 1998). Prior research considers reputation as an important subcomponent of the cognitive trust and suggests that a trustor may categorize a trustee as trustworthy or untrustworthy based on the reputation of the trustee (McKnight et al. 1998). The reputation categorization process infers that a trustee with a good reputation is believed to be trustworthy (McKnight et al. 1998). Therefore, if the trustee has a good reputation, trustor will quickly develop trusting beliefs about the trustee, even without firsthand knowledge or direct experiential information (Li et al. 2008; McKnight et al. 1998). Thus, in P2P sharing, we predict that vendors with a good reputation are seen as trustworthy and those with a bad reputation as untrustworthy.

H2: Reputation of the vendor of P2P sharing software positively affects trusting beliefs.

2.6. Institutional Trust

Institution-based trust means that "one believes that the necessary impersonal structures are in place to enable one to act in anticipation of a successful future endeavor" (McKnight et al. 1998, p. 478). Prior research examining the institutional trust in information systems has mostly focused on a single institutional context in the electronic market environment – the organizational context (Pavlou and Gefen 2004). However, as a specific attribute of network-based virtual communities in social computing, peer-network structure should be explicitly conceptualized as one type of institutional trust that is distinct from the organizational structure. When the network of relationships in network-based virtual community are unstructured and non-static, it is especially important for participants in such network to recognize that the peer network they are interacting with is of low-risk (cf. Dholakia et al. 2004).

We further believe that the peer-network structures would be the other important factor in forming users' trust beliefs. In a P2P network, trust of a peer is hardly developed because trust is often applicable to a relationship with another *identifiable* party (Mayer et al. 1995a) and a peer can easily hide her identify from others. Thus, peer's behaviors such as free-riding shared resources can deteriorate the performance of a P2P sharing network and thus negatively impact others' sharing activities (Pavlov and Saeed 2003; Samant 2003). Moreover, there are reports that P2P networks are inserted with low-quality or damaged versions of music files for various purposes (Borland 2002; Levine 2002). Also P2P networks are criticized being utilized for exchanging pirated resources among some peers. These uncertainties in peer-network may expose users to various risks and drive them to withdraw from the use of P2P sharing software (PEW-Internet and American-Life-Project 2004). Consequently, we propose a new dimension in institutional trust, namely *peer-network structure*, relating to one's perceptions that other users on the same peer-network appear to be normal or favorable and the P2P sharing actions are likely to incur low risk.

Below we discuss two components of institutional trust: (1) situational normality, defined as the belief that the situation appears to be normal or favorable and success is likely (Baier 1986); and (2) structural assurances, defined as the belief that success is likely because such contextual conditions as promises, contracts, regulations, and guarantees are in place (McKnight et al. 1998).

2.6.1. Situational Normality

Situation normality could be related to a greater trust belief because it assures people that everything in the setting is as it ought to be (McKnight et al. 1998; Zucker 1986) and thus their interactions with others in this setting is in accordance with what they consider to be anticipated (Gefen et al. 2003a). When people face unanticipated or abnormal situations, they are uncomfortable and tend to not trust others in this kind of setting (Li et al. 2008). Empirical studies in e-commerce context have generally supported the positive impacts of situation normality on trust (Gefen et al. 2003a; McKnight et al. 2002) and operationalized situational normality by referring to the trustee being studied, e.g., a specific online vendor or a particular web site. In current research, we operationalize two situational normality constructs: organizational and peer-network situational normality. Situational normality in the peer-network context is operationalized with collective peers who share or download resources on a P2P network. Users are more likely to have positive trusting beliefs if they believe that majority of peers are interacted in a predictable and reliable manner. Therefore, we hypothesize:

H3: Peer-network situational normality positively affects trusting beliefs.

Situational normality in the organizational context is operationalized with vendors of P2P sharing software. Users are more likely to have positive trusting beliefs in a P2P vendor if they observe that the P2P sharing software has a typical user interface, a set of expected procedures and a typical set of functionalities for P2P sharing activities based on their knowledge and experiences of other similar P2P sharing software. Therefore, we hypothesize:

H4: Organizational situational normality positively affects trusting beliefs.

2.6.2. Structural Assurances

Structural assurances refer to the beliefs that structures like regulations, guarantees, and legal resources could guide, empower, and constrain the conduct of individuals and organizations (McKnight et al. 2002; McKnight et al. 1998; Shapiro 1987). Similar to situational normality, two structural assurance constructs were operationalized in current research: organizational and peer-network structural assurances. In a peer-network context, techniques such as reputation building, prevention of pirated resources from being injected into P2P network, and risk reduction mechanisms like anti-flooding and anti-attack have been proposed and implemented into P2P sharing software (Borland 2003; Oram 2001). These peer-network structures can prevent opportunistic behaviors of peers (Waldman et al. 2001) and thus can build user confidence and trust in the P2P systems and their vendors. Thus, users who perceive high peer-network structural assurances would attribute this to the competence and integrity of the system and thus increase trust in the vendor. Therefore, we hypothesize:

H5: Peer-network structural assurance positively affects trusting beliefs.

In the e-commerce context, it has been found that organizational structural assurance could limit the firm's ability to behave in negative ways, allowing consumers to form and hold beliefs about expectations of positive outcomes (Johnson and Cullen 2002). In this research, we refer the organizational structures to a user's perceptions of the institution environment of a P2P sharing network. Influential factors in forming users' trust beliefs include the organizational resources and procedures, vendor guarantee such as the code of conduct of P2P United (2004), the association of P2P software vendors like BearShare, Grokster and eDonkey, which regulates member vendors in terms of user privacy, security and respect for copyright laws. Hence, we hypothesize:

H6: Organizational structural assurance positively affects trusting beliefs.

2.7. Trust, Perceived Risk and Intended Use

The effect of trust on risk reduction has been empirically supported in e-commerce context (Gefen et al. 2003b; Jarvenpaa and Tractinsky 1999; Kollock 1999; Stewart 2003). Trust could reduce information complexity and lower the perceived risk of a transaction. It has been established in e-commerce that trust in an e-vendor reduces the level of perceived risk (Jarvenpaa and Tractinsky 1999). Based on these findings, in P2P sharing, we propose that trusting beliefs in vendor's capabilities should lower users' risk perception in P2P sharing such as privacy invasion, free-riding, virus attack and injection of pirated resources and et al. Hence, we hypothesize:

H7: Trusting beliefs reduce perceived risks in P2P file sharing.

Along the line of Theory of Reasoned Action (Ajzen 1985; Ajzen 1991), risk perception viewed as the negative antecedent belief, and trust viewed as the positive antecedent belief, could both affect a person's attitude that in turn influence a person's behavioral intention (Jarvenpaa and Tractinsky 1999). Empirical evidence supports the above expectations of the negative relationship between perceived risk and behavioral intention, and the positive relationship between trust and behavioral intention in e-commerce context (Gefen 2002; Pavlou 2003). We suggest that the same logic can be extended to P2P sharing context and thus we hypothesize:

H8: Perceived risks in P2P file sharing decrease intended use of P2P sharing software.

H9: Trusting beliefs increase intended use of P2P sharing software.

3. RESEARCH METHOD

To examine the effects of perceived risk in P2P sharing and trust in vendors on the intention to use P2P sharing software, a survey technique was employed. Email addresses of 600 undergraduate students were randomly collected from an online learning system in School of Engineering at a large university in Singapore. Invitation emails explained the purpose of the study and stated that only those who have prior experience in P2P sharing were eligible to participate in the online survey. Measurement items were developed based on procedures advocated by

Churchill (1979) and Moore and Benbasat (1991). As far as possible, constructs were adapted from existing measurement scales used in prior studies to fit the P2P context where necessary (see Appendix A).

To ensure that the data is collected among experienced users of P2P sharing software, respondents were requested to complete the online questionnaire by answering the questions regarding the recent P2P sharing software which they used for resource searching, download or sharing. Respondents were also required to indicate the name of that P2P sharing software and the usage frequency during past three months. Questionnaires from respondents who had not indicated the previous usage of P2P sharing software were discarded. A total of 136 responses were resulted. The mostly used software applications from the respondents were KaZaA (72%), BitTorrent (12%), Emule (9%) and Shareaza (6%).

4. DATA ANALYSIS

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold (1982), was used for data analyses. PLS assesses the measurement model (relationships between questions and constructs) within the context of the structural model (relationships among constructs). Additionally, it seeks to maximize the explanation of variance and prediction in the theoretical model and does not demand multivariate normal distributions. It is suitable for our exploratory study because PLS is generally more appropriate for testing theories in the early stages of development (Fornell and Bookstein 1982).

4.1. Testing the Measurement Model

The measurement model was evaluated by examining the relationships between the constructs and the indicators. Such examinations may include the test of the convergent and discriminant validity of constructs. Three tests are used to determine the convergent validity (Cook and Campbell 1979): reliability of questions, the composite reliability of constructs, and the average variance extracted by constructs. Reliability of these questions was assessed by examining the loading of each question on the construct. In order for the shared variance between each question and the construct to exceed the error variance, the reliability score for the question should be at least 0.707. However, a reliability score of at least 0.5 might be acceptable if some other questions measuring the same construct had high reliability scores (Chin 1998). Given that all questions had reliability scores above 0.5, and most questions had reliability scores above 0.707 (see Appendix B), the questions measuring each reflective construct had adequate reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7 while the average variances extracted for these constructs were all above 50 percent and the Cronbach's alphas were also all higher than 0.7. Overall, the above test results indicate that the convergent validity of all constructs is adequate.

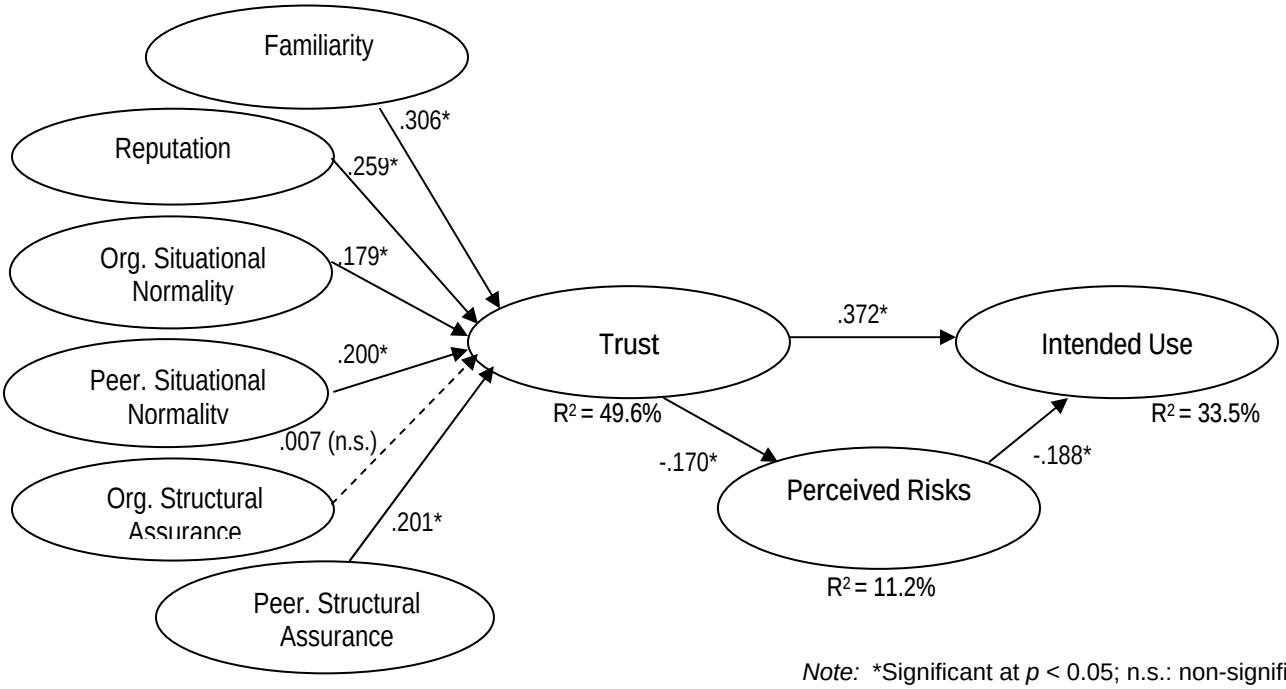
Discriminant validity is the degree to which measures of different constructs are distinct (Campbell and Fiske 1959). To test discriminant validity, the squared correlations between constructs (their shared variance) should be less than the average variance extracted for a construct. Table 1 reports the descriptive statistics and the results of discriminant validity, which is checked by comparing the diagonal to the non-diagonal elements. All items fulfilled the requirement of discriminant validity.

	VR	FV	OSA	OSN	PSA	PSN	TRU	RISK	INT
VR	0.885								
FV	0.604	0.881							
OSA	0.547	0.585	0.844						
OSN	0.379	0.185	0.300	0.812					
PSA	0.467	0.364	0.422	0.261	0.902				
PSN	0.433	0.378	0.460	0.309	0.378	0.882			
TRU	0.590	0.578	0.470	0.361	0.458	0.467	0.857		
RISK	0.100	0.119	0.335	0.287	0.022	0.106	-0.351	0.928	
INT	0.253	0.086	0.008	0.513	0.128	0.260	0.389	-0.217	0.979

Table 1. Discriminant Validity

4.2. Testing the Structural Model

With adequacy in the measurement model affirmed, the PLS structural model was next examined to assess their explanatory power and the significance of the hypothesized paths. The explanatory power of the structural model was assessed based on the amount of variance in the endogenous construct (intended use) for which the model could account. Our structural model can explain 33.5% of the variance for intended use. Each hypothesis (H1 to H9) corresponded to a path in the structural model. Bootstrapping technique was applied to obtain the corresponding T-values in order to assess the significance of the path estimates. Except H5 (Organizational Structural Assurance → Trust), all hypotheses were supported. Figure 2 depicts the structural model.



Note: *Significant at $p < 0.05$; n.s.: non-significant

Figure 2. Structural Model

5. DISCUSSION AND CONCLUSION

Social computing focuses on how users may have more autonomy to express their ideas and participate in social exchanges in various ways, one of which may be P2P file sharing. While technical issues are still relevant from a social computing perspective, this research examines P2P file sharing from a more social perspective to understand how factors influencing individuals in groups or networks affect their online behavior. The results show that experienced users' continuous use of P2P sharing software depends on both trust beliefs in the software vendor and risk perceptions associated with P2P sharing. Most prior IS studies on trust have reported knowledge-based factors, cognitive factors and institutional factors as significant determinants of trusting beliefs. Our results confirmed the effects of these trust antecedents in a social computing context. In addition, this research has identified two different components of institutional trust: the organizational structures and the peer-network structures. Our results showed that the organizational structures were overshadowed when peer-network structures, knowledge-based trust, and cognitive trust were also assessed. Specifically, the proposed organizational structural assurances did not have impact on trust in P2P vendor. A possible reason for this could be that the survey participants are not aware of the existence of any legal protection or not familiar with the industry's self-regulation body. In fact, none of the survey respondents lastly used a P2P sharing software that is provided by a member vendor in P2P United (2004).

Our preliminary findings have several practical implications in the P2P landscape. First, this study highlights the important roles of P2P vendors and peer-network in building effective online communities. As discussed earlier, building trustworthy dependency on other peers is difficult due to high uncertainties of peers. P2P vendors, therefore, should contribute to provide functions into the sharing software to build a safe, effective and stable P2P network that can lead to users' perception of peer-network situational normality and structure assurance (Aringhieri

et al. 2006). P2P vendors should also actively take efforts in addressing such issues like free-riding, content piracy, malicious computer attack, rather than passively leaving these issues as they were and merely playing a role as software provider. This is also supported by the call for the self-regulation in P2P industry by researchers (Hughes et al. 2008) and by lawmakers (Borland 2003). In practice, more and more P2P software vendors are implementing such mechanisms, like providing peers with incentives for opening more shares in exchange for faster download speed, and offered the accounting functions in the software to protect against malicious users. Second, reputation of the vendor and user familiarity with the vendor should also be actively promoted, for example, via promoting the new features and procedures of the software through mass media. Third, both organizational and peer-network situational normality, such as a typical user interface, and effective mechanisms like free riding prevention and anti-flooding, are important strategies for trust building.

Organizational structural assurances were shown not important in trust building by our data analysis. This insignificant effect is probably due to the participants' lack of knowledge about available organizational safeguards. One interpretation of this result is that, users of social computing applications increasingly take trust cues from one another and communities rather than from organizational sources. As such, user communities are increasingly driving innovations and communications from the bottom up, and the information flow, economic value, and power is starting to shift from organizations to user communities. Although the data generally support the proposed model, caution must be exercised when generalizing these findings. Since the respondents for this study were Asian students in an engineering school, the generalizability of the respondents' behaviors to the actual P2P users may be somewhat limited. Care must be taken when generalizing these findings to consumers in other social, economic, and cultural environments. Most P2P sharing networks are running globally over the Internet, and the legal risks presented in one country may be absent in other countries. How to effectively prevent global P2P users from sharing and downloading copyright violated materials? Who will play the most important role in regulating the usage behavior in using P2P sharing software? These would be fruitful questions for future research.

In conclusion, this research constitutes one of the first empirical studies to identify the antecedents to trust formation in P2P context. Through the causal modeling of the antecedents affecting reuse intentions in P2P, our findings provide preliminary empirical support to understand trust and perceived risk issues in P2P context. Nevertheless, since some characteristics of this study may limit the generalizability of our findings, several avenues for future work remain. We hope this study makes a modest contribution to stimulating further research in the field of P2P sharing.

ACKNOWLEDGMENTS

This research is partially supported by the National Science Foundation under Grant No NSF-CNS 0716646. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Appendix A. Measurement Items (measured on seven-point, Likert-type scale)

	Intended Use (INT): (Pavlou and Gefen 2004)
INT1	I intend to continue using the P2P file sharing software to search for, download or share resources.
INT2	I predict I would reuse the P2P file sharing software.
INT3	I plan to continue using the P2P file sharing software.
	Perceived Risk (RISK): (Pavlou and Gefen 2004)
RISK1	There is a high potential for loss involved in using the P2P file sharing software.
RISK2	There is a considerable risk involved in using the P2P file sharing software to search for, download and/or share resources.
RISK3	My decision to use the P2P file sharing software is risky.
	Trust in P2P Vendor (TRU): (Gefen et. al. 2003)
TRU1	I believe the vendor is honest.
TRU2	I believe the vendor cares about its users.
TRU4	I believe the vendor is reliable.
	Reputation (VR): (McKnight et. al. 2002)
VR1	The vendor has a reputation for being honest.
VR2	The vendor has a reputation for being concerned about the users.
VR3	Most users think that this vendor has a reputation for being fair.
	Familiarity (FV): (Gefen et. al. 2003)
FV1	I am familiar with the vendor through resource searching and download by the P2P file sharing software.
FV2	I am familiar with the vendor through sharing resources to other peers by the P2P file sharing software.
FV3	I am familiar with the vendor through reading magazine/newspaper articles or ads.

	Peer-Network Structural Assurances (PSA): (McKnight et. al. 2002)
PSA1	The peer-network has enough safeguards to make me feel comfortable transferring and sharing resources with other peers.
PSA2	I feel assured that the technological structures adequately protect me from peers' opportunistic behavior.
PSA3	I feel assured that other peers cannot free ride on my shared resources.
	Peer-Network Situational Normality (PSN): (McKnight et. al. 2002) *Based on your experiences with peers whom you have downloaded resources from, or shared resources to, among those peers:*
PSN1	Most peers are in general predictable and consistent regarding their behaviors.
PSN2	Most peers are trustworthy in transferring and sharing resources with other peers.
PSN3	Most peers are reliable to download resources from, and/or share resources to.
	Organizational Structural Assurances (OSA): (Gefen et. al., 2003)
OSA1	I feel assured that downloaded resources are legal because the vendor provides statements of guarantees that all shared resources are legal.
OSA2	I feel safe using the P2P sharing software because the vendor is on the list of P2P United.
OSA3	I am comfortable searching, downloading or sharing resources because of the regulatory and technological structures built by the vendor.
	Organizational Situational Normality (OSN): (Gefen et. al. 2003) *Based on your experiences with other similar P2P sharing software…*
OSN1	The mechanisms built into the software to encourage peers to download/share resources are typical of other similar P2P file sharing software.
OSN2	The steps required to search for, download and share resources are typical of other similar P2P file sharing software.
OSN3	The approach used by the software to encourage peers to download/share resources is the type of approach most similar P2P sharing software employs.

Appendix B. Psychometric Properties of the Measurement Model

Construct Indicators	Factor Loadings	Composite Reliability	Cronbach's Alpha	Variance Extracted
Intention to Use (INT)				
INT1	0.983	0.986	0.873	0.959
INT2	0.984			
INT3	0.970			
Perceived Risk (RISK)				
RISK1	0.976	0.949	0.889	0.862
RISK2	0.889			
RISK3	0.918			
Trust in P2P Vendor (TRU)				
TRU1	0.939	0.892	0.837	0.735
TRU2	0.805			
TRU3	0.822			
Reputation (VR)				
VR1	0.898	0.916	0.886	0.783
VR2	0.859			
VR3	0.898			
Familiarity (FV)				
FV1	0.921	0.912	0.899	0.776
FV2	0.896			
FV3	0.822			
Organizational Structural Assurances (OSA)				
OSA1	0.912	0.880	0.811	0.712
OSA2	0.890			
OSA3	0.715			
Organizational Situational Normality (OSN)				
OSN1	0.717	0.858	0.878	0.670
OSN2	0.820			
OSN3	0.908			
Peer-Network Structural Assurances (PSA)				
PSA1	0.905	0.929	0.865	0.814
PSA2	0.924			
PSA3	0.877			
Peer-Network Situational Normality (PSN)				
PSN1	0.889	0.913	0.850	0.778
PSN2	0.862			
PSN3	0.894			

6. REFERENCE

Ajzen, I. "From intentions to actions: A theory of planned behavior," in: *Action control: From cognition to behavior*, J. Kuhl and J. Beckmann (eds.), Springer Verlag, New York, NY, 1985, pp. 11-39.

Ajzen, I. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50) 1991, pp 179-211.

Aringhieri, R., Damiani, E., Vimercati, S.D.C.D., Paraboschi, S., and Samarati, P. "Fuzzy Techniques for Trust and Reputation Management in Anonymous Peer-to-Peer Systems," *Journal of the American Society for Information Science and Technology* (57:4) 2006, pp 528-537.

Baier, A. "Trust and antitrust," *Ethics* (96) 1986, pp 231-260.

Bhattacherjee, A. "Individual Trust in Online Firms: Scale Development and Initial Test," *Journal of Management Information Systems* (19:3) 2002, pp 211-241.

Borland, J. Start-ups try to dupe file-swappers. *CNET News.Com*. 2002, http://news.com.com/2100-1023-943883.html.

Borland, J. Senators ask P2P companies to police themselves. *CNET News.com*. 2003, http://news.com.com/2100-1028_3-5110785.html.

Campbell, D.T., and Fiske, D.W. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:1) 1959, pp 81-105.

Charron, C., Favier, J., and Li, C. Social Computing: How Networks Erode Institutional Power, And What to Do About It. *Forester Research*. 2006, http://www.forrester.com/Research/Document/Excerpt/0,7211,38772,00.html.

Chin, W.W. "The Partial Least Squares Approach to Structural Equation Modeling," in: *Modern Methods for Business Research*, G.A. Marcoulides (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 1998, pp. 295-336.

Churchill, G.A. "A paradigm for developing better marketing constructs," *Journal of Marketing Research* (16), February 1979, pp 64-73.

Cook, M., and Campbell, D.T. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Houghton Mifflin, Boston, 1979.

Dholakia, U.M., Bagozzi, R.P., and Pearo, L.K. "A social influence model of consumer participation in network-and small-group-based virtual communities," *International Journal of Research in Marketing* (21:3) 2004, pp 241-263.

Fornell, C., and Bookstein, F.L. "Two Structrual Equation Models: LISREL and PLS Applied to Customer Exit-Voice Theory," *Journal of Marketing Research* (19:11) 1982, pp 440-452.

Ganesan, S. "Determinants of Long-Term Orientation in Buyer-Seller Relationships," *Journal of Marketing* (58), April 1994, pp 1-19.

Gefen, D. "Customer loyalty in e-commerce," *J. Assoc. Inform. Systems* (3) 2002, pp 27-51.

Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in online shopping: an integrated model," *MIS Quarterly* (27:1), March 2003a, pp 51-90.

Gefen, D., Rao, V.S., and Tractinsky, N. "The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications," *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS)*, Big Island, HI, 2003b, pp. 192-201.

Giffin, K. "The Contribution of Studies of Source Credibility to a Theory of Interpersonal Trust in the Communication Process," *Psychological Bulletin* (68:2) 1967, pp 104-120.

Havlena, W.J., and DeSarbo, W.S. "On the Measurement of Perceived Consumer Risk " *Decision Sciences* (22:4) 1991, pp 927-939.

Hoffman, D.L., Novak, T., and Peralta, M.A. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2) 1999, pp 129-139.

Hughes, J., Lang, K.R., and Vragov, R. "An analytical framework for evaluating peer-to-peer business models," *Electronic Commerce Research and Applications* (7:1) 2008, pp 105-118.

Ip, R., and Wagner, C. "Weblogging: A Study of Social Computing and Its Impact on Organizations," *Decision Support Systems* (45:2) 2008, pp 242-250.

Jarvenpaa, S.L., and Tractinsky, N. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer Mediated Communications* (5:2) 1999, pp 1-35.

Johnson, L.J., and Cullen, B.J. "Trust in Cross-Cultural relationships," in: *The Blackwell Handbook of Cross-Cultural Management*, M.J. Gannon and K.L. Newman (eds.), Blackwell, Oxford, UK, Malden, Mass, 2002, pp. 335-360.

Kollock, P. "The Production of Trust in Online Markets," *Advances in Group Processes* (16) 1999, pp 99-123.

Lane, C., and Bachmann, R. "The social constitution of trust: supplier relations in Britain and Germany," *Organization Studies* (17:3) 1996, pp 365-395.

Levine, D. Not the real Slim Shady. 2002, http://dir.salon.com/story/tech/feature/2002/06/10/eminem_mp3/index.html.

Lewicki, R.J., and Bunker, B.B. "Trust in relationships: A model of trust development and decline," in: *Conflict, Cooperation, and Justice*, B.B. Bunker and J.Z. Rubin (eds.), Jossey-Bass, San Francisco, CA, 1995, pp. 133-173.

Lewis, J.D., and Weigert, A.J. "Trust as a social reality," *Social Forces* (63:4) 1985, pp 967-985.

Li, X., Hess, T.J., and Valacich, J.S. "Why do we trust new technology? A study of initial trust formation with organizational information systems," *Journal of Strategic Information Systems* (17:1) 2008, pp 39-71.

Luhmann, N. *Trust and Power*, John Wiley & Sons, Chichester, England, 1979.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. "An Integration Model of Organizational Trust," *Academy of Management Review* (20:3) 1995a, pp 709-734.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. "An integrative model of organizational trust," *Academy. Management Review* (20:3) 1995b, pp 709-734.
McKnight, D.H., and Chervany, N.L. "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce* (6:2) 2002, pp 35-59.
McKnight, D.H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3) 2002, pp 334-359.
McKnight, D.H., Cummings, L.L., and Chervany, N.L. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3) 1998, pp 472-490.
Moon, Y. "Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers," *Journal of Consumer Research* (26), March 2000, pp 323-339.
Moore, G.C., and Benbasat, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3) 1991, pp 173-191.
Moorman, C., Desphande, R., and Zaltman, G. "Factors affecting trust in market research relationships," *Journal of Marketing* (57:1) 1993, pp 81-101.
Nunnally, J.C. *Psychometric Theory*, (2nd ed.) McGraw-Hill, New York, 1978.
Oram, A. *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, O' Reilly & Associates, Cambridge, MA, 2001.
P2PUnited. P2P United: Fighting For The Future Of Peer-to-peer Technology. 2004, http://wiki.morpheus.com/~p2punited/.
Parameswaran, M., and Whinston, A.B. "Social Computing: An Overview," *Communications of the Association for Information Systems* (19) 2007, pp 762-780.
Pavlou, P.A. "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce* (7:3) 2003, pp 69-103.
Pavlou, P.A., and Gefen, D. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1) 2004, pp 37-59.
Pavlov, V.O., and Saeed, K. "A Resource-Based Assessment of the Gnutella File-Sharing Network," *Proceedings of 24th Annual International Conference on Information Systems (ICIS)*, Seattle, WA, 2003, pp. 85-95.
Peter, J.P., and Tarpey, S.L.X. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of Consumer Research* (2:1) 1975, p 29.
PEW-Internet, and American-Life-Project. The state of music downloading and file-sharing online. 2004, http://www.pewinternet.org/pdfs/PIP_Filesharing_April_04.pdf.
Reiter, M.K., and Rubin, A.D. "Anonymous Web Transactions with Crowds," *Communications of the ACM* (42:2) 1999, pp 32-38.
Samant, K. "Free Riding, Altruism, and Cooperation on Peer-to-Peer File-sharing Networks," *Proceedings of 24th Annual International Conference on Information Systems (ICIS)*, Seattle, WA, 2003, pp. 914-920.
Schoder, D., and Fischbach, K. "Peer-to-peer prospects," *Communications of the ACM* (46:2) 2003, pp 27-29.
Schuler, D. "Social computing," *Communications of the ACM* (37:1) 1994, pp 28-29.
Shapiro, S.P. "The Social Control of Impersonal Trust," *American Journal of Sociology* (93) 1987, pp 623-658.
Stewart, K.J. "Trust Transference on the World Wide Web," *Organ. Sci.* (14:1) 2003, pp 5-17.
Waldman, M., Cranor, F.L., and Rubin, A. "Trust," in: *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, O. A. (ed.), O' Reilly & Associates, Cambridge, MA, 2001, pp. 242-270.
Wang, F.Y., Carley, K.M., Zeng, D., and Mao, W. "Social Computing: From Social Informatics to Social Intelligence," *IEEE Intelligent Systems* (March/April) 2007, pp 79-83.
Wold, H. "Soft Modeling: The Basic Design and Some Extensions," in: *Systems Under Indirect Observations: Part 2*, K.G. Joreskog and H. Wold (eds.), North-Holland, Amsterdam, 1982, pp. 1-54.
Yates, J.F., and Stone, E.R. "Risk appraisal," in: *Risk-taking behavior*, J.F. Yates (ed.), John Wiley & Sons, Chichester, England, 1992, pp. 49-85.
Zucker, L.G. "Production of trust: Institutional sources of economic structure, 1840-1920," in: *Research in Organizational Behavior*, B.M. Staw and L.L. Cummings (eds.), JAI Press, Greenwich,CT, 1986, pp. 53-111.