

# Predicting the Usage of P2P Sharing Software: The Role of Trust and Perceived Risk

Heng Xu<sup>1</sup>, Hao Wang<sup>2</sup> and Hock-Hai Teo<sup>1</sup>

<sup>1</sup>*Department of Information Systems  
National University of Singapore*

*3 Science Drive 2, Singapore 117543*

*Email: {xuheng,teohh}@comp.nus.edu.sg*

<sup>2</sup>*NCS Communication Engineering Pte. Ltd.  
Singapore 918199*

*Email: wanghao@ncs.com.sg*

## Abstract

*Peer-to-Peer, or P2P sharing has gone through fast growth in recent years and drawn the interests of Information Systems (IS) researchers. However, there is a lack of empirical study on the individual's behavior of using P2P sharing software. Given the current existence of various uncertainties in P2P sharing, 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 usage intention model which includes trust in the vendor of P2P sharing software and perceived risk as two major antecedent beliefs to the usage intention. Several trust antecedents are also identified in the model. Our preliminary results show the support for the model, and offer some important implications for software vendors in P2P sharing industry and regulatory bodies.*

## 1. Introduction

Peer-to-peer, or P2P technology consists of P2P sharing software that allows Internet users to efficiently search for and exchange resources stored on other users' computers. P2P sharing has gone through fast growth in the recent years and drawn the interests of Information Systems (IS) researchers. Snir [48] examined the economical impacts of free P2P file sharing on record industry and suggested several marketing strategies for the record labels. Attention has also been paid to the problem of peer free-riding and its impact on the performance of a P2P sharing network [39, 44]. However, few studies have examined the individual's behavior of using P2P sharing software, a void this study seeks to address.

Given the current existence of various uncertainties in P2P sharing such as resource piracy [31], computer attack by malicious peers [13], privacy invasion [52, 41, 5], it is crucial to understand the factors that will affect individual's usage of P2P sharing, especially for repeat users.

Drawing on the trust literature [30, 33, 23], we developed a trust-risk-intention model by including trust in the vendor of P2P sharing software and perceived risk as two major antecedent beliefs to the usage intention. Several trust antecedents were further identified in the P2P sharing context. We empirically tested our model with a survey of 76 experienced and voluntary P2P users in a large university in Singapore. This study is novel to the extent that we have yet to find any empirical study that looks at trust and perceived risk issues in the P2P context. The research findings may provide a rich understanding of the issues affecting P2P evaluation and adoption, and therefore also benefit acceptance research in the IS discipline. Our findings can potentially be useful to regulatory bodies and P2P vendors to help shape or justify their decisions concerning P2P.

## 2. Literature Review

### 2.1. P2P Sharing Software

P2P sharing software, in this study, is defined as an application running P2P sharing technology dedicated for searching, downloading and sharing digital resources among peer users (peers), such as file sharing software like Gnutella and KaZaA, and CPU sharing software like SETI@home.

We assume peers to be anonymous in P2P sharing in this study. Reiter and Rubin [51] conceptualized anonymity in a Web context to have three degrees: 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).

In this study, we also assume the use of P2P sharing software is voluntary and free of charge. Non-voluntary

use of P2P sharing often happens within organizations and such case is excluded from our current research. Furthermore, we assume all peers in a P2P sharing network to be equal and there are no central administrators or power peers who have the capability to control other peers. For simplicity, we further assume that P2P network operators are also the producers of P2P sharing software. This assumption reflects the current practices of P2P sharing software like Gnutella and KaZaA, although logically the two roles are different.

Throughout the rest of the paper, we use the following terms: *resources* referring to files or computer hardware being shared out; *resources download* referring to retrieving resources from other users' computer over the Internet; *sharing resources* referring to allowing others to access and download the shared resources; *vendor* referring to the producer of P2P sharing software; *peer* is used in exchange with the term *user*; *peer network*, or *P2P sharing network*, is the network of peers running the same P2P sharing software. In this study, we focus on users with prior experiences in P2P sharing.

## 2.2. Perceived Risk in P2P Sharing

Perceived risk is defined as an individual's perceptions of the uncertainty and adverse consequences of engaging in an activity [15]. Perceived risk affects individuals' intention and actual usage of a technology especially in a high uncertain environment, such as online shopping [24]. Perceived risk is generally identified as having various facets (e.g., performance, financial, time, safety, social and psychological loss) and all risk facets stem from performance risk [12]. Featherman and Pavlou [16] identified privacy risk as a newly developed risk facet tapping the overwhelming privacy concern phenomenon in the e-service context.

In 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. For example, a peer may find her computer overloaded or attacked by malicious peers (peer-related performance risk); she may face legal suit or even jail (legal risk) when she shares pirated resources to other peers [31]; she may by mistake share her entire hard disk or other principle data repository as material available to others (peer-related privacy risk). Moreover, the user may not be informed of her online activities being disclosed to third parties by the software (vendor-related privacy risk) [52]. A peer may find the software's performance is not as good as expected, or hard to find and download her intended resources (vendor-related performance risk). Furthermore, the data transmission over Internet incurs potential channel risk as the attacker might be an eavesdropper that

can observe some or all messages sent and received over the Internet [51]. Without proper control of the risk in P2P sharing, a user may choose not to use the software due to high risks [40]. For example, Pavlov and Saeed [39] reported that the deteriorated performance of Gnutella software often cause download failed and lead users to give up the usage.

In this study, we define users' perceived risk 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. We propose that there are three facets of perceived risk involved with using P2P sharing software, namely *performance risk* and *privacy risk* that are adopted from the prior literature on the classification of perceived risk [12, 16], and the third facet, *legal risk* which is the legal liability for user actions in P2P sharing. However, we focus on the performance risk and privacy risk as the main facets of perceived risk by excluding legal risk in this study. The reasons are: 1) legal risk itself is an emerging concept in P2P context; 2) there have been no reported law suits against copyright violation in P2P sharing in Singapore at the time when we conducted this study. Hence, the subjects may not be able to perceive the legal risk as one facet of risk concerns involved with P2P sharing in Singapore.

## 2.3. Trust in P2P Sharing: Institution-based, Familiarity with Vendors, and Peer-Network Influential Factors

**2.3.1 Trust.** Trust deals with the belief that the trusted party will fulfill its commitments [42] despite the trusting party's dependence and vulnerability [43]. When a social environment cannot be regulated through rules and customs, people adopt trust as a central social complexity reduction strategy [29]. In the context of e-commerce, because of the absence of proven guarantees that the e-vendor will not engage in harmful opportunistic behaviors, trust is crucial in helping consumers overcome their perceptions of uncertainty and risk [24, 25].

In P2P sharing context, vendors' trustworthiness attributes are important to users. Lee [26] found that the four out of the top five most important features among 26 features in P2P sharing software rated by P2P users are related to vendor's ability, including the software should be "fast", "stable", "reliable", "able to resume loading". Other important vendor-related features among the top ten include "Can exit nicely" (integrity), "Gives error message" (benevolence). Tsivos et al. [52] also proposed that P2P sharing systems should have built-in self-regulatory characteristics to reduce the complexity of uncertainty. Those characteristics are such as stopping queries that are bound to match too many files and eliminating duplicate packets from overzealous users. Following trust definition in e-commerce and other

contexts [18, 19, 23], we define *trust of P2P vendors* as a set of *specific beliefs* dealing primarily with the integrity, benevolence, and competence of vendors.

### 2.3.2 Trust antecedents and institutional-based trust.

Gefen et al. [23] summarize five types of trust antecedents that can affect the formation of trust in e-vendors, namely 1) institution-based factors, 2) knowledge-based familiarity with e-vendors, 3) calculative-based factors that are based on deterrence theory, 4) cognition-based reputation which is derived from second-hand knowledge, and 5) personality-based factors which describe a person's general trust propensity towards others. In this study, we focus on examining the impacts of institution-based trust and knowledge-based familiarity with vendors on trust development for experienced users of P2P sharing software.

Among the above-mentioned five types of trust antecedents, only institution-based is consistently found to have positive impacts on the development of trust in e-vendors for both experienced [23] and inexperienced users [24, 20, 33]. Institution-based trust is one's perception of the existence of guarantees, safety nets or other impersonal structural conditions to facilitate achieving the expected outcomes [45, 55].

There are two types of institution-based trust: structural assurance and situational normality. Situational normality is one's belief that the situation appears to be normal or favorable and success is likely [3]. Structural assurances refer to one's beliefs that there exist structures (such as guarantees, regulations, promises, the legal recourse, guarantees, and regulations) to promote success [32, 45, 55].

In P2P sharing, we refer institution-based trust to an individual's perceptions of the institution environment of a P2P sharing network. There are some vendor guarantee such as the code of conduct of P2P United [37], the association of P2P sharing software vendors like BearShare, Grokster and eMonkey, which regulates member vendors in areas such as users' privacy, security and respect for copyright laws. In the light of recent call for self-regulation among P2P sharing vendors [39], there has yet no study examining the impacts of institution-based trust in trust development in vendors.

### 2.3.3 Knowledge-based familiarity with vendors.

Familiarity with vendors comes from prior first-hand experience. It is suggested that familiarity builds trust in a priori trustworthy party [29] and validated in e-commerce context [23]. Familiarity with vendors is different from situational normality because the latter does not involve the knowledge about the actual vendor [23]. 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.

**2.3.4 Peer-network normality.** In P2P sharing, trust of a peer is hardly developed because trust is only applicable to a relationship with another *identifiable* party [30] and a peer is assumed to hide her identity from others (see also Section 2.1). However, 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 [39, 44]. Moreover, there are reports that P2P networks are inserted with low-quality or damaged versions of music files for various purposes [27, 4]. Also P2P networks are criticized being utilized for exchanging pirated resources among some peers. The abnormal situation in peer-network may expose users to various risks and drive them to withdraw from the use of P2P sharing software [40].

Therefore, it is important for us to propose a new construct, namely *peer-network normality*, to refer to one's perceptions that the peer network appears to be normal or favorable and the P2P sharing actions are likely to incur low risk. On a network with perceived normality, a peer may believe that the next anonymous peer whom she will work with for resource sharing or downloading may own the trustworthy attributes such as integrity and benevolence. Peer-network normality is distinguished from knowledge-based familiarity with a P2P vendor, or cognitive-based trust, in two ways: 1) the peer-network normality is the perception about collective peers who are *not* identifiable, and 2) the perceptions of peer-network normality can be derived from first-hand experiences of using P2P sharing software, second-hand information such as news from media, or a combination of both.

## 3. Research Model and Hypotheses

In this study, we developed a trust-risk-intention model by including trust in the vendor of P2P sharing software and perceived risk as two major antecedent beliefs to the usage intention. We further identified several trust antecedents in the P2P landscape. Figure 1 presents our research model. The following sections develop and elaborate the key constructs and the theoretical rationale for the causal relationships among the constructs in the research model.

### 3.1. Institution-based Influential Factors on Trust Building

There are two types of institution-based trust: structural assurance and situational normality. Below, we will discuss how these two types of institution-based factors influence the trust formation.

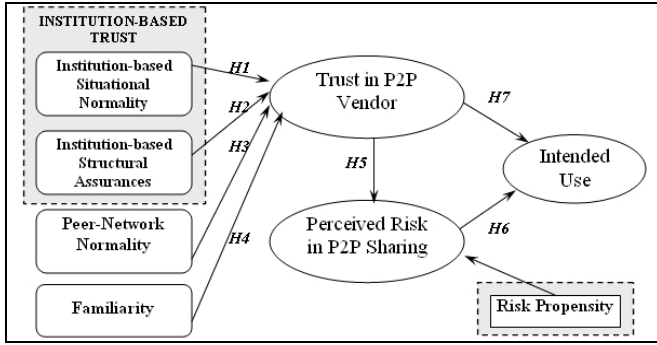


Figure 1. Research Model

**3.1.1. Situational normality.** Situational normality can be perceived from the appropriateness of the Internet as a channel for online activities [33], or from the Web-based user interface of an e-vendor [23]. Empirical studies in e-commerce context support that situation normality has positive impacts on individual’s trust in an e-vendor [33, 23].

In P2P sharing context, a user who perceives high situational normality would believe that the Internet is an appropriate and favorable channel for P2P searching, transferring resources and communicating with others. With such belief of high situational normality, the user would believe in general that vendors for P2P sharing over the Internet would have the trustworthy attributes such as integrity, benevolence and competence. Furthermore, the user will be more inclined to trust the vendor if she observes that the software has a typical user interface, a set of expected procedures and a typical set of functionalities for P2P sharing activities based on her knowledge and experiences of other similar P2P sharing software. For example, some P2P software encourage users to share their resources by offering some rewards, i.e., the more being shared, the faster download a peer can enjoy. As a result, a user would expect such a rewarding mechanism to be built in her P2P sharing software and tend to build trust into the vendor if the vendor provided such functionality.

Therefore, we hypothesize:

H1: *Perceptions of situational normality will positively affect trust in the vendor of a P2P sharing software.*

**3.1.2. Structural assurances.** In e-commerce context, perceptions of the legal and technological protections, such as those safeguards built into a Web site like third parties’ reliability seals and vendor’s own guarantees, are found to help build trust in e-vendors [23, 33, 51].

P2P sharing software has been challenged for its legal status to exist due to the pirated contents distributed in P2P sharing network. In a recent lawsuit in the U.S., Grokster won the case thanks to its pure peer-to-peer network architecture [50]. This assures the legal status to

exist for P2P sharing software with similar network architecture. On the other hand, those P2P sharing software running on networks with centralized servers and relay servers, will have legal problems and face the possibility of being shutdown as what Napster experienced in September 2002 [50]. Therefore, users would be more likely to trust those P2P vendors whose networks are running on the pure peer-to-peer architecture due to the legal protection of status to exist. Furthermore, industry self-regulation body such as P2P united, created code of conduct which regulates member vendors in areas such as users’ privacy, security and respect for copyright laws. Users should be more inclined to trust vendors who are members of P2P United due to the statements of guarantees. Besides these, safety guards such as vendor’s privacy statement could also lead to higher trust in vendors. Hence, we hypothesize:

H2: *Perceptions of structural assurance will positively affect trust in the vendor of a P2P sharing software.*

**3.2. Peer-Network Normality Influential Factors on Trust Building**

Since there is no superpower peer who has the capability to control other peers on a peer network, the peer network needs to be self-regulated to reduce the associated uncertainties in order to achieve user perceived peer network normality. In fact, P2P software is being designed towards an ideal goal of totally removing a peer’s dependency on others and preventing opportunistic behaviors of peers [53]. Techniques such as reputation building, prevention of pirated resources from being injected into P2P network, and risk reduction like anti-flooding and anti-attack have been proposed and implemented into P2P sharing software towards building confidence and trust in the P2P systems and their vendors [6, 36]. Thus, users who perceive high peer-network normality would attribute this to the competence and integrity of the software and thus increase trust in the vendor. Therefore, we hypothesize:

H3: *Perceptions of peer-network normality will positively affect trust in the vendor of a P2P sharing software.*

**3.3 Knowledge-based Familiarity with Vendors in Trust Building**

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 [28]. In e-commerce, familiarity with e-vendors is found to lead to higher trust in vendors [23]. 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:

H4: *Familiarity with the vendor of a P2P sharing software will positively affect trust in that vendor.*

### 3.4. Trust, Perceived Risk and Intended Use

The effect of trust on risk reduction has been empirically supported in e-commerce context [22, 24, 25, 51]. 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 [24]. Based on these findings, in P2P sharing, we propose that trusting beliefs in vendor's attributes such as competence, benevolence, and integrity should lower users' risk perception in P2P sharing. With the trusting belief in the vendor's capabilities, a user may perceive a lower level of risk such as privacy invasion, free-riding, virus attack and injection of pirated resources and et al. Hence, we hypothesize:

H5: *Trust in the vendor of a P2P sharing software will reduce perceived risk in P2P sharing.*

Along the line of Theory of Reasoned Action [1, 2], 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 [24]. 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 [21, 38]. We suggest that the same logic can be extended to P2P sharing context and thus we hypothesize:

H6: *Perceived risk in P2P sharing will decrease intended use of a P2P sharing software.*

H7: *Trust in the vendor of a P2P sharing software will increase intended use of a P2P sharing software.*

### 3.5. Control Variable

Prior research in the risk-taking literature suggests that risk propensity, the tendency of a decision maker to take risky actions, has a positive influence on an individual's risk perception [47]. Therefore, it is included as the control variable for perceived risk in this study.

## 4. Research Method

To examine the effects to perceived risk in P2P sharing and trust in vendors on the intention to use P2P sharing software, a survey technique was employed.

### 4.1. Instrument Development

Measurement items were developed based on procedures advocated by Churchill [10] and Moore and Benbasat [34]. As far as possible, constructs were adapted from existing measurement scales used in prior studies to fit the P2P context where necessary. Consistent with the measurement scales adopted in [23, 33], all the constructs except perceived risk are *reflective* constructs. The items for usage intention, trust in P2P vendor, structural assurance, situational normality, familiarity with P2P vendor were adapted from e-commerce trust studies [23, 33] and modified to reflect the specific context of the P2P sharing in the survey questions. The four items for peer-network normality were adapted from the measurement of trustworthy attributes of an e-vendor in [23] and modified to reflect our own definition for this construct.

Four items formed the construct of perceived risk in P2P sharing, based on the risk perception measurement in the consumer research and IS acceptance literature [16, 46]. The four items represent the main facets of perceived risk in P2P sharing: vendor performance risk, vendor-related privacy risk, peer performance risk, and peer-related privacy risk. Because these facets of risk perceptions are not expected to be always correlated – e.g., users may perceive high level of peer performance risk and peer-related privacy risk but may perceive little or no vendor performance risk and vendor-related privacy risk, we treat perceived risk as a *formative* construct comprising of these four facets. All items in the questionnaire were anchored on seven-point Likert scale. Appendix A presents the final questions measuring each construct in this study.

### 4.2. The Survey

Email addresses of 500 undergraduate students were randomly collected from an online learning system in School of Engineering at a large university in Singapore. Invitation emails explaining the purpose of the study were sent to the selected students. The emails stated that only those who have prior experience in P2P sharing were eligible to participate in the online survey. Also included in the invitation emails is the URL link to the web-based survey questionnaire. The respondents were told that their anonymity would be assured and the results would be reported only in aggregate. As an incentive for participation, three monetary awards of Singapore dollar \$40<sup>1</sup> per person were raffled among the participants.

<sup>1</sup>The reward was framed in Singapore dollars. As of April 2004, one Singapore dollar = 59 U.S. cents.

To insure 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 the previous year (i.e. from April 2003 to April 2004). Questionnaires from respondents who had not indicated the previous usage of P2P sharing software were discarded. A total of 76 responses were resulted. Respondents had used P2P sharing software an average of 21 times for searching resources, 19 times for downloading resources and 15 times for sharing resources during the previous year. The mostly used software applications were KaZaA (72%), BitTorrent (12%), Emule (9%) and Shareaza (6%).

## 5. Data Analysis

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold [54], 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 [17].

### 5.1. 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. The strength of the constructs modeled with formative indicators can be assessed with the significance of the indicators' weights. While for reflective constructs, three tests are used to determine the convergent validity [11]: reliability of questions, the composite reliability of constructs, and the average variance extracted by constructs. Table 1 presents an assessment of the measurement model for reflective 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 [9]. Given that all questions had reliability scores above 0.5, and most questions had reliability scores above 0.707 (see Table 1), the questions measuring each reflective construct had

adequate reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's [35] 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 reflective constructs is adequate. The strength of formative constructs can be tested by assessing the significance of the formative indicators' weights. Hence, the weights of the construct (i.e., perceived risk) modeled with formative indicators are tested for significance. The results presented in Table 2 reveal that the indicators of perceived risk are significant ( $\alpha = .001$ ).

Discriminant validity is the degree to which measures of different constructs are distinct [7]. To test discriminant validity, the squared correlations between constructs (their shared variance) should be less than the average variance extracted for a construct. Table 3 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.

### 5.2. 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 21.2% of the variance for intended use. Since all hypotheses are unidirectional, they were tested with one-tailed t-tests at 5% significance level. Figure 2 depicts the structural model.

Each hypothesis (H1 to H7) 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 H2 (Structural Assurances  $\rightarrow$  Trust), all the hypotheses were supported.

Table 1. Psychometric Properties of Constructs with Reflective Indicators

Items	LD	CA	CR	AVE
Intention:				
INT1	.983		.986	.959
INT2	.984			
INT3	.971			
Trust:				
TV1	.897	.872	.888	.572
TV2	.767			
TV3	.605			
TV4	.844			
TV5	.686			
TV6	.702			
Structural Assurance:				
SA1	.892	.776	.857	.603
SA2	.840			
SA3	.680			
SA4	.669			
Situational Normality:				
SN1	.743	.756	.846	.582
SN2	.880			
SN3	.701			
SN4	.713			
Peer-network Normality:				
PN1	.876	.860	.909	.714
PN2	.815			
PN3	.896			
PN4	.788			
Familiarity:				
FV1	.923	.854	.912	.776
FV2	.896			
FV3	.820			
Risk Propensity:				
RP1	.641	.707	.804	.509
RP2	.667			
RP3	.800			
RP4	.734			

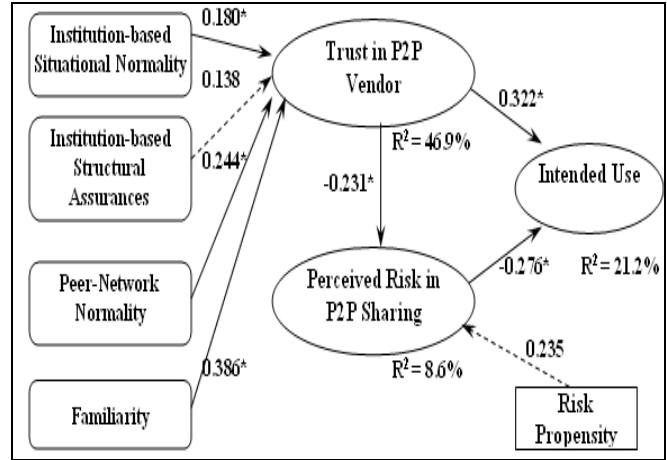
(LD = Loading; CA = Cronbach's Alpha; CR = Composite Reliability; AVE = Average Variance Extracted)

Table 2. Formative Indicators' Significance Test

Items	Weights	t-Statistics
Perceived Risk:		
PR1	.313	5.120
PR2	.324	6.382
PR3	.348	5.015
PR4	.271	4.298

Table 3. Discriminant Validity of Constructs

Construct	INT	PR	TV	SA	SN	PN	FV	RP
INT	.979							
PR	-.335	.791						
TV	.372	-.182	.757					
SA	.076	.211	.521	.776				
SN	.566	-.029	.328	.270	.763			
PN	.190	-.056	.483	.442	.282	.845		
FV	.088	.094	.571	.600	.110	.337	.881	
RP	.270	.187	.207	.036	.457	.286	.067	.713



\*Significant at  $p < 0.05$

Figure 2. Structural Model

## 6. Discussion and Conclusion

This study examined two aspects of users' decisions to use P2P sharing software: trust and perceived risk. The present study shows that experienced users' intentions to reuse a P2P sharing software depends on both trust in that software vendor and risk perception associated with P2P sharing. Trust in a P2P vendor played a weaker role in reducing risk perception in P2P sharing. By examining the relative importance of the four antecedents of trust formation in P2P vendor, we found that familiarity with P2P sharing software ( $b=0.386$ ) plays a more important role in trust formation, compared to peer-network normality ( $b=0.244$ ) and institution-based situational normality ( $b=0.180$ ). Contrary to our expectation, the proposed institution-based 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 (none of the survey respondents lastly used a P2P sharing software that is provided by a member vendor in P2P United.)

This exploratory study examines the experienced users' reuse intentions in P2P sharing context by using a survey approach. Our research results can also be applied to users who do not have initial experiences, as the information about the vendor's trustworthiness and the level of perceived risk can be passed to and propagated among initial users and affect their adoption of P2P sharing software [49]. Although the data generally support the proposed model, caution must be exercised when generalizing these findings. First, although the structured equation modeling technique used was able to handle small samples, more statistical validity could be achieved with a larger population. Second, 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. Third,

actual adoption behavior was not measured, rather, we assumed, based on a significant body of prior work in IS (e.g., [23]), that intention is a good predictor of actual behavior. However, future research could examine the findings of this study in a context where actual usage behavior can be observed for added validation of the model. Fourth, since trust in a P2P vendor played a weaker role in reducing risk perception in P2P sharing, future research could further explore whether the four antecedents of trust and other antecedents, could contribute to reduce users' risk perception. Fifth, our operationalization of perceived risk excluded the measurement of legal risk for its inappropriateness in Singapore, because there have been no reported law suits against copyright violation in P2P sharing in Singapore. Therefore, it would be a challenge to continue improving the operationalization of perceived risk in a P2P context. Finally, this study was conducted in Singapore, care must be taken when generalizing these findings to consumers in other social, economic, and cultural environments, and future research should attempt to replicate this study in other countries, especially those in North America and in Europe, to further explore the impact of legal risks (e.g., P2P sharing of copyright violated materials). 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.

Our preliminary findings have several practical implications in the P2P landscape. First, this study highlights the important role of P2P vendors in boosting the usage of P2P sharing software. As discussed in Section 2.3.4, building trustworthy dependency on other peers is difficult due to the anonymity of peers. Hence, the perceived peer-network normality needs to be developed to provide a peer with the feeling of trustworthy dependency on other peers through building user's trust belief in the vendors. 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 normality. 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 [52] and by lawmakers [6]. 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, 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, situational normality, such as a typical user interface, and interface consistency in the software upgrades, also directly contributes to trust formation.

Institution-based structural assurance, although shown not important in trust building by our data analysis, should still be paid attention. This insignificant effect is probably due to the participants' lack of knowledge about available safeguards. This finding suggests that policy makers and vendors should collaborate to 1) create more assurance structures via collaborating with user-trusted third-party authorities to incorporate consumer protection seals in their software and meaningful sanctions for breaching these obligations, and 2) educate the users by promoting the knowledge about the existence and details of safeguards and code of conduct.

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.

## 7. References

1. Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckmann (Eds), *Action control: From cognition to behavior* (pp.11-39). Springer Verlag, New York, New York.
2. Ajzen, I. (1991). The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, 50, 179-211.
3. Baier, A. "Trust and Antitrust," *Ethics* (96), 1986, pp. 231-260
4. Borland J. "Start-ups try to dupe file-swappers," *CNET News.Com*, July 15, 2002, <http://news.com.com/2100-1023-943883.html>
5. Borland, J. "Fingerprinting P2P pirates," *CNET News.Com.*, February 20, 2003a, [http://news.com.com/2100-1023\\_3-985027.html](http://news.com.com/2100-1023_3-985027.html)
6. Borland, J. "Senators ask P2P companies to police themselves," *CNET News.com*, November 21, 2003b, [http://news.com.com/2100-1028\\_3-5110785.html](http://news.com.com/2100-1028_3-5110785.html)
7. Campbell, D. T., and Fiske, D. W. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:1), 1959, pp. 81-105.
8. Childers, T. L. "Assessment of the psychometric properties of an opinion leadership scale," *Journal of Marketing Research* (23), May 1986, pp.184-188.
9. Chin, W. W. "The Partial Least Squares Approach to Structural Equation Modeling," *Modern Methods for*

- Business Research*, G. A. Marcoulides (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 1998, pp. 295-336.
10. Churchill Jr., G. A. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research* (16:1), 1979, pp. 64-73.
  11. Cook, M., and Campbell, D. T. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*. Boston: Houghton Mifflin, 1979.
  12. Cunningham, S. "The major dimensions of perceived risk," In: D. Cox (Ed.), *Risk Taking and Information Handling in Consumer Behavior*, Harvard University Press, Cambridge, MA., 1967.
  13. Dingleline, R., Freedman, J. M. and Molnar, D. "Accountability", In: Oram A.(Ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. O'Reilly & Associates, Cambridge, MA, 2001, pp 271-339.
  14. Donthu, N., and Gilliland, D. "The Infomercial Shopper," *Journal of Advertising Research* (36), March/April 1996, pp.69-76.
  15. Dowling, G. R., and Staelin, R. "A model of perceived risk and intended risk-handling activity," *Journal of Consumer Research* (21), 1994, pp. 119-134.
  16. Featherman, M. and Pavlou, P. "Predicting e-services adoption: a perceived risk facets perspective," *Int. J. Human-Computer Studies* (59), 2003, pp. 451-474.
  17. Fornell, C., and Bookstein, F. L. "Two Structural Equation Models: LISREL and PLS Applied to Customer Exit-Voice Theory," *Journal of Marketing Research* (19:11), 1982, pp. 440-452.
  18. Ganesan, S. "Determinants of Long-Term Orientation in Buyer-Seller Relationships," *Journal of Marketing* (58), April 1994, pp. 1-19.
  19. 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.
  20. Grazioli, S. and Wang, A. "Looking without seeing: Understanding unsophisticated consumers' success and failure to detect internet deception," *Proceedings of the ICIS*, New Orleans, Louisiana, USA, December 2001, pp.193-204.
  21. Gefen, D. "Customer loyalty in e-commerce," *Journal of the Association for Information Systems* (3), 2002, pp.27-51.
  22. 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 36<sup>th</sup> Hawaii International Conference on System Sciences*, Big Island, Hawaii, USA, 2003a, pp. 192 - 201
  23. Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in Online Shopping: An Integrated Model", *MIS Quarterly* (27:1), 2003b, pp. 51-90.
  24. Jarvenpaa, S.L. and Tractinsky, N. "Consumer trust in an Internet store: A Cross-cultural validation," *Journal of Computer Mediated Communication* (5:2), 1999, pp. 1-35.
  25. Kollock, P. "The Production of Trust in Online Markets," *Advances in Group Processes* (16), 1999, pp. 99-123.
  26. Lee, J. "An End-User Perspective on File-Sharing Systems," *Communications of the ACM* (46:2), 2003, pp.49-53.
  27. Levine, D. "Not the real Slim Shady", June 10, 2002, [http://www.salon.com/tech/feature/2002/06/10/eminem\\_mp3/?x](http://www.salon.com/tech/feature/2002/06/10/eminem_mp3/?x)
  28. 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 (ed.s), Jossey- Bass, San Francisco, 1995, pp. 133-173.
  29. Luhmann, N. *Trust and Power*, John Wiley & Sons, Chichester, England, 1979.
  30. Mayer, R.C., Davis, J.H., and Schoorman, F.D. "An Integration Model of Organizational Trust," *Academy of Management Review* (20:3), 1995, pp.709-734.
  31. McGuire, D. "Lawmakers push prison for online pirates", *Washingtonpost.com*, March 31, 2004 <http://www.washingtonpost.com/wp-dyn/articles/A40145-2004Mar31.html>
  32. 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 473-490.
  33. McKnight, D.H., Choudhury, V., and Kacmar C. "Developing and Validating Trust Measurers for e-Commerce: An Integrative Typology", *Information Systems Research* (13:3), 2002, pp 334-359.
  34. 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.
  35. Nunnally, J. C. *Psychometric Theory* (2nd ed.). New York: McGraw-Hill, 1978.
  36. Oram, A., Ed. *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. O'Reilly & Associates, Cambridge, MA, 2001.
  37. P2P United, <http://www.p2punitd.org>.
  38. 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.
  39. Pavlov, V. O., and Saeed, K. "A Resource-Based Assessment of the Gnutella File-Sharing Network", In *Proceedings of 24th Annual International Conference on Information Systems (ICIS)*, Seattle, Washington, United States, December 2003, pp 85-95.
  40. PEW Internet & American Life Project, "The state of music downloading and file-sharing online," April 2004, [http://www.pewinternet.org/reports/pdfs/PIP\\_Filesharing\\_April\\_04.pdf](http://www.pewinternet.org/reports/pdfs/PIP_Filesharing_April_04.pdf)
  41. Reiter, M. K. and Rubin, A.D. "Anonymous Web Transactions with Crowds," *Communications of the ACM* (42:2), 1999, pp. 32-38.
  42. Rotter, J. B. "Generalized Expectancies for Interpersonal Trust," *American Psychologist* (26), May 1971, pp. 443-450.
  43. Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. "Not So Different After All: A Cross-Discipline View of Trust," *Academy of Management Review* (23:3), 1998, pp. 393- 404.
  44. Samant, K. "Free Riding, Altruism, and Cooperation on Peer-to-Peer File-sharing Networks", In *Proceedings of 24th Annual International Conference on Information Systems (ICIS)*, Seattle, Washington, United States, December 2003, pp 914-920.

45. Shapiro, D. L., Sheppard, B. H., and Cheraskin, L. "Business on a Handshake," *Negotiation Journal* (3), 1992, pp. 365-377.

46. Shimp, A. T. and Preston, L. I., "Warranty and Other Extrinsic Cue Effects on Consumers' Risk Perceptions," *Journal of Consumer Research*, 9 (June), 1982, pp 38-46.

47. Sitkin, S.B. and Weingart, L. R. "Determinants of risky decision-making behavior: a test of the mediating role of risk perceptions and propensity," *Academy of Management Journal* (38:6), 1995, pp. 1573-1592.

48. Snir, M. E "The Record Industry in an Era of File Sharing: Lessons from Vertical Differentiation", In *Proceedings of 24th Annual International Conference on Information Systems (ICIS)*, Seattle, Washington, United States, December 2003, pp 72-84.

49. Song, J. and Walden, A. E. "Consumer Behavior in the Adoption of Peer-to-Peer Technologies: An Empirical Examination of Information Cascades Network Externalities", *Proceedings of Ninth Americas Conference on Information Systems (AMCIS)*, Tampa, Florida, August 2003, pp 1801-1810.

50. Sprigman, C. "Why Grokster and Morpheus Won, Why Napster Lost, and What the Future of Peer-to-Peer File Sharing Looks Like Now," *FindLaw's*, May 8, 2003, [http://writ.news.findlaw.com/commentary/20030508\\_sprigman.html](http://writ.news.findlaw.com/commentary/20030508_sprigman.html)

51. Stewart, K.J. "Trust Transference on the World Wide Web," *Organ. Sci.* (14:1), 2003, pp 5-17.

52. Tsvivos, P., Whitley, A. E. and Hosein, I. An exploration of the emergence, development and evolution of regulatory characteristics of information systems, In *Proceedings of the Twentieth International Conference on Information Systems (ICIS)*, Charlotte, North Carolina, USA. December 1999, pp 813-816.

53. Waldman, M., Cranor, F. L. and Rubin, A. "Trust", In: Oram A.(Ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. O'Reilly & Associates, Cambridge, MA, 2001, pp 242-270.

54. 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.

55. Zucker, L. G. "Production of Trust: Institutional Sources of Economic Structure, 1840-1920," in *Research in Organizational Behavior* (Volume 8), B. M. Staw and L. L. Cummings (eds.), JAI Press, Greenwich, CT, 1986, pp. 53-111.

## 8. Appendix A: Operationalization of Constructs

<p><b>Intention to Use (INT):</b> [23]</p> <p>I intend to use the software to search for, download or share resources in the next 12 months. (INT1)</p> <p>I predict I would use the software in the next 12 months. (INT2)</p> <p>I plan to use the software in the next 12 months. (INT3)</p>
<p><b>Perceived Risk in P2P Sharing (PR):</b> [46, 16]</p> <p>How confident are you of the software's ability to perform as expected? (1: Very confident; 7: Not confident at all) (PR1)</p> <p>What are the chances that the software or its accompanying third party advertisement software installed on your computer (if any) would cause you to lose control over your personal information? (1: Improbable; 7: Probable) (PR2)</p> <p>How confident are you of the peer's ability to perform as expected? (1: Very confident; 7: Not confident at all) (PR3)</p> <p>My use of the software would lead to a loss of privacy for me because a peer may access my personal information without my knowledge(1: Improbable; 7: Probable) (PR4)</p>
<p><b>Trust in P2P Vendor (TV):</b> [23]</p> <p>I believe the vendor is honest. (TV1)</p> <p>I believe the vendor cares about its users. (TV2)</p> <p>I believe the vendor is not opportunistic. (TV3)</p> <p>I believe the vendor is reliable. (TV4)</p> <p>I believe the vendor is predictable. (TV5)</p> <p>I believe the vendor is a capable and proficient provider of P2P sharing software. (TV6)</p>
<p><b>Structural Assurance (SA):</b> [23, 33]</p> <p>I feel assured that downloaded resources are legal because the vendor provides statements of guarantees of that all shared resources are legal. (SA1)</p> <p>I feel safe using the software because the vendor is in the list of P2P United. (SA2)</p> <p>I feel assured the legal and technological structures adequately protect me from problems on the Internet. (SA3)</p> <p>I feel assured that encryption and other technological advances on the Internet make it safe for me to transfer resources. (SA4)</p>
<p><b>Situational Normality (SN):</b> [23, 33]:</p> <p>The steps required to search for, download and share resources are typical of other similar software. (SN1)</p> <p>The approach used by the software to reduce resource free-riding is the type of approach most similar P2P sharing software employ. (SN2)</p> <p>The mechanisms built into the software to encourage peers to share their resources are typical of other similar software. (SN3)</p> <p>I feel good about how things go when I do resource searching, downloading, or sharing or other activities over the Internet. (SN4)</p>
<p><b>Peer Network Normality (PN):</b> Adapted from [23]</p> <p>How would you rate the peers on the network of the software based on your knowledge and experience?</p> <p>Most peers are honest. (PN1)</p> <p>Most peers care about other peers. (PN2)</p> <p>Most peers are reliable. (PN3)</p> <p>Most peers are predictable. (PN4)</p>
<p><b>Familiarity with P2P Vendor (FV):</b> [23]</p> <p>I am familiar with the vendor through resource searching and download by the software. (FV1)</p> <p>I am familiar with the vendor through sharing resources to other peers by the software.(FV2)</p> <p>I am familiar with the vendor through reading magazine/newspaper articles or ads. (FV3)</p>
<p><b>Risk Propensity (RP):</b> [14, 8]</p> <p>I sometimes do things I know are dangerous just for fun. (RP1)</p> <p>I am comfortable using software different from types I am accustomed to (RP2).</p> <p>I avoid risky things (reverse scale) (RP3).</p> <p>I would rather be safe than sorry (reverse scale) (RP4).</p>