Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2011 Proceedings - All Submissions

8-5-2011

Consumer Risk: The Importance of Privacy and Security while Connected to Wi-Fi Hotspots: Does Location Matter?

Patrick Curry
Baylor University, pat_curry@baylor.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2011_submissions

Recommended Citation
Curry, Patrick, "Consumer Risk: The Importance of Privacy and Security while Connected to Wi-Fi Hotspots: Does Location Matter?" (2011). *AMCIS 2011 Proceedings - All Submissions*. 308.
http://aisel.aisnet.org/amcis2011_submissions/308

This material is brought to you by AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2011 Proceedings - All Submissions by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Consumer Risk: The Importance of Privacy and Security while Connected to Wi-Fi Hotspots: Does Location Matter?

Patrick Curry
Baylor University
pat_curry@baylor.edu

ABSTRACT

As the FCC begins releasing white space in the radio spectrum, the number of free Wi-Fi hotspots in the U.S. is expected to proliferate. However, organizations should not regard this service as a solution to drive new customers to their businesses. This study examines trust, privacy, security, risk and convenience related to users' intentions to use free Wi-Fi hotspots. Findings indicate that trust in the hotspot location is a significant antecedent of privacy and security beliefs, and reduces risk perceptions. Furthermore, a newly developed construct called social privacy is influential in risk reduction leading to greater Wi-Fi use. While this study shows that convenience is a major driver of free Wi-Fi use, businesses offering the service would be remiss in not maintaining high levels of user trust.

Keywords: Trust, Security, Social Privacy; Convenience; Risk; Wi-Fi Hotspots

INTRODUCTION

Wi-Fi hotspots have begun to proliferate at various types of businesses such as coffee shops, airports, hotels, and fast food restaurants. Hotspots are capable of providing a customer with unlimited access time, specialized web services (e.g., Starbucks Digital Network), no registration/account to create, data transfer rates up to 11 Mbps, and other benefits at more than 72,000 registered locations throughout the United States (Blog, 2010). In addition, on September 24, 2010 the Federal Communication Commission (FCC) approved rules for the development and deployment of radio equipment in the white space spectrum, which refers to the unused portions of the radio spectrum made available by the switch from analog to digital television. This ruling will increase access to the white space spectrum and enable companies to bring broadband to rural and other remote areas (FCC, 2010). Additionally, the ruling is likely to produce a new generation of wireless devices as well as greatly increase the number of free Wi-Fi locations.

However, risk affects individual decision-making when the decision may produce adverse consequences over which the individual has no control. Perceived risk is defined as an individual's beliefs about the severity of the adverse consequences of behavior (Koller, 1988), the chance of adverse consequences resulting from use (Dowling & Staelin, 1994), or the expectations of losses (Stone & Gronhaug, 1993). The consumer's perception of risk has been shown to rise with increasingly negative consequences or with the consumer's decreasing control over the consequences (Koller, 1988). Hence, users may be unwilling to use ubiquitous free Wi-Fi hotspots if they believe the risk of connecting to the network is excessive. This has implications for providers of Wi-Fi as they reach out to consumers to provide a service that is reliable, secure, trustworthy, and with minimal risk to consumers.

The focus of the present study is on identifying antecedents to consumers' perceptions of risk as it relates to free Wi-Fi hotspots. In this context, risk is the consumer's risk-related beliefs that form his subjective risk assessment of the potential dangers and losses that may occur as a consequence of using free Wi-Fi hotspots. Relationships between risk and trust, privacy beliefs, social privacy, and security are examined. A Wi-Fi hotspot is defined as a specific geographic location in which an access point provides public Wi-Fi broadband network services to mobile visitors through a Wi-Fi local area network. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers and hotels. Hotspots typically have a short range of access, but coverage could increase with the FCC ruling on white

space as new technological developments could take advantage of the new spectrum by increasing range and coverage to include rural and other remote locations (at sea and in the air).

This paper examines the following research questions:

RQ1: How do consumer risk perceptions affect the use of free Wi-Fi locations?

RQ2: How does trust in the location of the free Wi-Fi connection influence the user's intention?

RQ3: Is social privacy an important antecedent of the user's risk perceptions?

RQ4: What is the role of convenience on intentions to use free Wi-Fi hotspots?

Prior IS studies have examined the relationships between user attitudes, satisfaction and behavioral intentions as well as system usage on the basis of the Theory of Reasoned Action (TRA) (e.g., Gefen and Straub, 1997, 2000; Venkatesh, 2000; Venkatesh and Davis, 2000; Gefen, 2003; Hsu and Lu, 2004; Ong *et al*., 2004). Similarly, TRA is the basis for examining how social privacy, privacy beliefs, security beliefs, convenience, and trust influence risk and the user's intention to use free Wi-Fi hotspots. Partial Least Squares (PLS) is used to analyze the research model with the survey results of 168 respondents. Findings indicate that while risk is an important determinant of usage intentions, for this group of respondents convenience is the major driver of intentions to use free Wi-Fi hotspots. However, trust and privacy should not be dismissed especially if businesses intend to use free Wi-Fi to bring in new customers or maintain existing customers. The location of the hotspot does matter.

The present study has implications for companies that may soon consider providing free Wi-Fi services as well as those assessing the costs and benefits of this service. The use of organizational assets to provide a service that generates little return is imprudent, thus an understanding of the determinants of Wi-Fi use are important. Based on the results of this study, companies that choose to implement hotspots would do well to address users' risk perceptions, develop high levels of trust, and educate customers on measures to secure their device (i.e., laptop, Smartphone, IPAD) while attached to the Wi-Fi connection. If users believe that they and/or their information are not being protected, companies are likely to lose out to competitors that provide those assurances.

RESEARCH MODEL AND HYPOTHESES

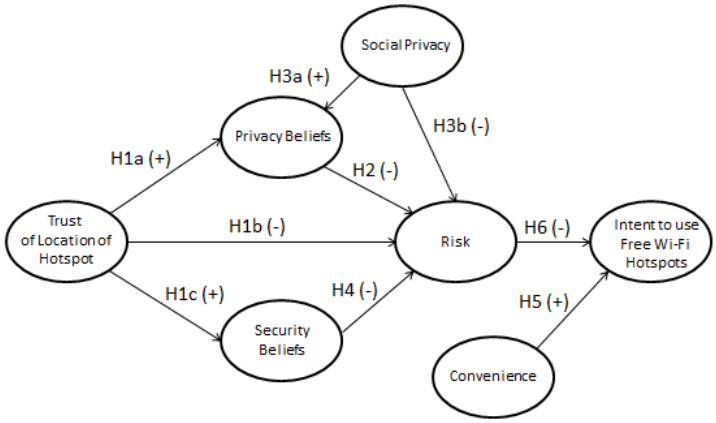

Figure 1: Research Model

The Effect of Trust on Privacy Beliefs, Risk and Security Beliefs

Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other

party" (Mayer, *et al*., 1995). This reasoning can be extend to Wi-Fi relationships, where lack of trust can be an obstacle to the expansion of free Wi-Fi hotspots due to a high degree of mistrust a user could feel (Truste, 2003). In the Wi-Fi hotspot context, trust refers to the belief that the user of the hotspot will not be taken advantage of by the provider of the hotspot. If trust perceptions are not positive, then a potential user is not likely to utilize the Wi-Fi service because the user feels vulnerable. This vulnerability may be related to feelings about a lack of privacy if the user is unsure how confidential his communications actually are if he uses the hotspot.

Thus, a user's trust in a Wi-Fi location is likely to carry over into a confidence that the provider will protect the user's privacy while conducting personal business over the Wi-Fi connection, which is imperative to ensure users continue to utilize that location. Therefore, the following hypothesis is examined:

H1a: Trust in the location of Wi-Fi hotspots will be positively related to privacy beliefs.

Yousafzai (2003) states that trust is related to risk, because trust reduces the risk of falling victim to opportunistic behavior. If there was no risk and actions could be taken with complete certainty no trust would be needed (Yousafzai *et al*. 2003). Trust is essentially needed only in uncertain situations since trust effectively means to assume risks and become vulnerable to trusted parties (Hosmer 1995).

In this study, Wi-Fi user risk includes the idea that the user is open to the opportunism of the Wi-Fi provider. In some respects, the user is at the mercy of the provider but the perceptions of vulnerability may be mitigated when the user trusts the provider. It is likely that the more the user trusts the provider the less his perception of the risk of falling prey to opportunistic behaviors of the provider. In general, users are assumed to differ in terms of their propensity to trust or their disposition to trust (Lee and Turban, 2001; McKnight and Chervany, 2001). The propensity to trust is likely influenced by users' awareness of Wi-Fi hacking and their past experience regarding situations involving risk (Tan and Theon, 2001). If a provider of Wi-Fi fails to secure the connection with adequate safe guards and a customer's laptop is compromised, trust in the provider will be negatively impacted and the level of risk is likely to increase. Therefore, when a user's trust of a specific location is optimized he will likely perceive using the Wi-Fi as less risky, leading to the following hypothesis:

H1b: Trust in the location of Wi-Fi hotspots will be negatively related to perceived risk.

Kolsaker and Payne (2002) stated that in a network environment, perception is as important as reality and there is a general consensus that the success of business is largely dependent upon the emergence of guaranteed security. Network reliability is an important factor for consumers as it relates to the transmission of data over the network infrastructure (i.e. Wi-Fi). There are inherent security risks associated with each transmission that include unauthorized third party interception of the information (Clay and Strauss 2000).

Security risk in this paper includes the belief that providers have mechanisms to ensure the safe transmission of users' information, whereby the information is not susceptible to third party interception or modification. Users need technical guarantees that improve their perception of trust in the provider of Wi-Fi hotspots. It is likely that as a user's trust of the Wi-Fi location increases, his security beliefs also increase because the user feels his information will be less exposed and more secure in a trust-worthy situation or trusted location, leading to the following hypothesis:

H1c: Trust in the location of Wi-Fi hotspots will be positively related to perceived security risk.

Privacy continues to be an issue with internet usage. Whether it is giving personal information to a website to process a transaction, information to gain access to a site or information to obtain a connection to the network, consumer's personal information is at risk (Rust *et al.*, 2002). Privacy belief is defined as individual's ability to control the terms by which personal information is acquired and used (Galanxhi-Janaqi and Fui-Hoon Nah, 2004). Privacy as it relates to consumer activities via electronic means (i.e. Wi-Fi connection) refers to "personal information and the invasion of privacy which relates to the unauthorized collection, disclosure, or other use of personal information as a direct result of the electronic connection" (Wang *et al* 1998). Users' privacy is often compromised due to network bleed when user information is provided to connect to the network, and that information is often collected by web sites the consumer accesses (Hoffman *et al.* 1999).

New technologies' growing capacity for information processing, plus its complexity, have made privacy an increasingly important issue (Kelly and Erickson, 2004, 2005). Companies that provide Wi-Fi hotspots should view protection of users' private information with great importance since privacy is likely a major factor in decisions to use Wi-Fi services. Wi-Fi hotspots have an inherent risk associated with utilization and reducing privacy concerns may help mitigate the risk factors.

Therefore, the following hypothesis is presented:

H2: Privacy beliefs will be negatively related to perceived risk.

The Effect of Social Privacy on Privacy Beliefs and Risk

Social privacy is a concept not yet demonstrated in the literature. Socialness is defined as pertaining to the life, welfare, and relations of human beings in a community (Merriam-Webster's, 2008). Privacy as stated previously refers to the confidentiality of personal information and the invasion of privacy is the unauthorized collection, disclosure, or other use of personal information as a direct result of the electronic transaction (Wang *et al* 1998). One need not be alone to have privacy. Even in community, individuals expect a certain amount of privacy. For example, a student typing on his laptop in the library expects that others would respect his privacy and would not stop and read over his shoulder. Social privacy is a new construct that includes the notion of the expectations of privacy one has concerning his personal information or communications when he is surrounded by others. Social privacy also includes the user's perception of how others behave to maintain the privacy of a Wi-Fi user who may be conducting business in a public venue (i.e. coffee shop, restaurant, hotel lobby).

Social privacy as it relates to the use of free Wi-Fi hotspots is viewed as an antecedent of privacy beliefs. Hence, as a user's perception of social privacy increases his privacy beliefs will also be positively influenced leading to the following:

H3a: Social privacy will be positively related to privacy beliefs.

Similarly, Wi-Fi users whose perception of social privacy is affected by the physical and/or technical barriers erected by the provider are likely to believe that using that service is less risky. For example, a 3-sided individual laptop carousel that provides a certain amount of privacy within a social setting such as an airport is likely to lessen users' feelings of vulnerability. If the user believes the Wi-Fi provider cares about his social privacy needs, then the user may feel less at risk which leads to the following hypothesis:

H3b: Social privacy will be negatively related to perceived risk.

The Effect of Security Beliefs on Risk

Security beliefs may be defined as the subjective probability with which users believe that their personal information will not be viewed, stored, and/or manipulated during transit and storage by inappropriate parties in a manner inconsistent with their confidential expectations (Flavian and Guinaliu, 2006). In this respect, providers of Wi-Fi focus on the technical aspects of security that affords consumers integrity, confidentiality, authentication and non-repudiation in relationship to data transmission (Flavian, and Guinaliu 2006). The integrity of the connection is the trustworthiness of information resource, confidentiality refers to limiting information access and disclosure to authorized users and preventing access and disclosure to those unauthorized, availability is the accessibility of information resources and non-repudiation means that sending parties cannot deny they sent a communication. When users are afforded these technical security assurances, they are likely to believe their information is safe. Security of the network is of great concern to consumers and is believed to be frequent barriers to usage (Pitkow and Kehoe 1996). Han and Ho (1999) note that lower levels of security have a negative effect on the network usage.

Although consumers have some responsibility to secure their Wi-Fi connection (e.g., VPN connection, personal firewall), service providers may also reduce security risk perceptions with various technical solutions (e.g., firewall, Wired Equivalent Privacy). Hence, when the user believes the Wi-Fi provider is adequately attending to the security of electronic transmissions his perception of risk is likely to decrease. This leads to the following hypothesis:

H4: Security beliefs will be negatively related to perceived risk.

The Effect of Convenience on Intent to Use

One of the major advantages for the use of free Wi-Fi hotspots is the convenience of service locations. There are already thousands of locations for users to connect online and with the FCC opening the white space spectrum that number is bound to increase exponentially. As of March 22, 2010 there were more than 72,000 registered Wi-Fi hotspots (Aaron, 2010). Various news blogs suggest that as many as 100,000 Wi-Fi hotspots could be available by 2015 with the extension of the white space spectrum. Consumers have indicated that convenience is a major reason to connect online (Chang et al., 2005) and with a proliferation of service providers, hotspots will be ubiquitous.

Convenience is defined by (Brown 1990) as having five dimensions: time, place, acquisition, use and execution. Cheolho and Sanghoon (2007) reduced the dimensions of convenience to time, place and execution when referring to technology. In this study, convenience is defined within the parameters of 1) time: Wi-Fi hotspots can be used to accomplish tasks at a convenient time, 2) place: Wi-Fi hotspots can be used to accomplish tasks at a convenient place, and 3) execution: Wi-Fi hotspots are convenient in the process of accomplishing a task. Elliot and Fowell (2000) note that convenience is a major reason consumers use internet connections, but argued that difficulties with web site navigation is a factor for dissatisfaction and reduced usage.

One of the major advantages of free Wi-Fi hotspots is convenience with thousands of locations for a consumer to connect.

Thus, when hotspots provide time, place and execution conveniences, users are more likely to use the hotspots, resulting in the following:

H5: Convenience will be positively related to intent to use free Wi-Fi hotspots.

The Effect of Risk on Intent of Use

As previously noted, Wi-Fi hotspots are on an upward trend and could continue to grow as new technology takes advantage of the white space spectrum. However, the expanding Wi-Fi network can create a heightened level of risk for users. Riskiness can be conceptualized as the amount of uncertainty surrounding the outcome of innovation (Dearing et al., 1994; Johnson et al., 1998). The perception of risk has been found to significantly impact technology adoption (Johnson et al., 1998) and risk toward a product category is negatively associated with usage intentions toward that product category (Westland 2002). Comparable reasoning can be used to assess a user's perception of risk and his likelihood of using free Wi-Fi hotspots.

If overall perceptions of vulnerability and opportunities for loss are high, then users a less likely to use a hotspot, which leads to the following hypothesis:

H6: Perceived risk will be negatively related to intent to use free Wi-Fi hotspots.

RESEARCH METHOD

The research model was tested with a 39 item survey preceded by a narrative to mentally place the respondent at one of two chosen locations prior to completing the survey.

Scenario one, positioned the respondent in a coffee shop: *When taking this part of the survey imagine you are entering the LOCAL COFFEE SHOP with your laptop to utilize their free Wi-Fi connection, then answer the following questions.*

Scenario two, positioned the respondent traveling on a major highway: *Prior to answering the following questions, imagine you are driving on I-35. You stop for gasoline and notice that the gas station has free Wi-Fi service. You enter the station and open your laptop on the counter provided for customers.*

The study was conducted using both an online and a paper survey. E-mails were sent to 60 students and faculty associated with a large southwestern university in the U.S. Additionally, paper surveys where administer to 145 undergraduate students in a classroom setting. The data for this study was collected over a ten day period, resulting in 168 completed, usable surveys out of a possible 205 surveys issued for a response rate of about 82 percent.

MEASUREMENT

A questionnaire was employed to collect data for the constructs of the research model. Of the 39 items used in the survey, six were developed specifically for this study. The remaining 33 measures were adapted from various extant literature and adjusted to fit the context of the Wi-Fi study. All items were measured using a seven-point Likert-type response format extending the scale from "strongly disagree" to "strongly agree". All variables were modeled as reflective constructs. The measurement items and their sources are detailed in Appendix A.

The measures for perceptions of social privacy were newly developed for this study. First, a pilot survey was conducted that consisted of eight measures of various aspects of privacy from extant literature (Rust, 2002; Dinev and Hart, 2006; Lo, 2010). Privacy has many dimensions such as privacy of the person, patient privacy (health care) and client privacy (legal field) (Raghupathi, 2002). Social privacy as defined by the measurement items considered individual's beliefs about how evasive people are when it comes to viewing what a user is doing online. The measurement items inquired about whether individual users believe that others are watching over their shoulder as they use electronic devices in social settings, if they are aware of others viewing their laptop screen, if users believe that others want to know what they are doing on their device, of if they notice others trying to look at what they are doing on their laptop.

A scenario used presented which situated the respondent in a coffee shop with their laptop to utilize the free Wi-Fi connection. Respondents in the pilot test were undergraduate and graduate students majoring in MIS. Respondents were asked to respond to the statements based on a seven-point Likert-type scale of strongly disagree to strongly agree. As a result of the factor analysis, five potential measures of social privacy were dropped due to low factor loadings below .40, and three were retained with a Cronbach's alpha of 0.73.

PARTICIPANTS

Based on a survey response group, 55 percent of the participants were male and 45 percent female, 94 percent of the respondents were between 18 – 24 years old, and more than 87 percent of the respondents owned two or more Wi-Fi enabled devices. Seventy-three percent of the respondents accessed free Wi-Fi in the past month, of which forty-six percent accessed free Wi-Fi more than 4 times in the past month. Overall, the respondents represented a group accustomed to using free Wi-Fi with more than 87 percent owning two or more Wi-Fi enabled devices with nearly half reporting more than occasional monthly use. Interestingly, 55 percent indicated the main reason for using free Wi-Fi was for social networking purposes, followed by 23 percent for academic uses, 11 percent for gaming and only 7 percent for conducting personal business. Detailed descriptive statistics related to the survey respondents and the data are in Table 1 and Table 2.

	Survey Demographics
Number of Subjects	N=168
Average Age	18 - 24 years old = 94%
Gender	Male = 55%; Female = 45%
Primary reason for using free Wi-Fi:	
Academic	23%
Gaming	11%
Social Networking	55%
Personal Business	7%
Other	4%
How many Wi-Fi enabled devices do you own:	
0	0%
1	13%
2	55%
3	21%
>3	11%
How often have you used free Wi-Fi in the past month:	
0	27%
1-3 times	39%
4-6 times	17%
7-9 times	4%
> 9 times	13%

Table 1. Descriptive statistics of respondents' characteristics

Construct	Mean	Standard Deviation
Convenience	5.18	1.53
Intent	4.17	1.76
Privacy Beliefs	3.72	1.50
Risk	4.82	1.51
Security	3.40	1.47
Social Privacy	4.63	1.52
Trust	3.98	1.61

Table 2. Descriptive Statistics of Data

MEASUREMENT MODEL

The research model was tested using partial least squares (PLS), a structural modeling technique that is well suited for highly complex predictive models (Barclay et al. 1995, Chin 1998, Lohmoller 1989, Wold and Joreskog 1982). PLS was most appropriate given the number of constructs (seven) in the model and the exploratory nature of the research. SmartPLS version 2.0 (M3) Beta (Ringle, Christian Marc/Wende, Sven/Will, Alexander 2005) was used for the analysis and the bootstrap method using 500 re-samples was used to determine the significance of the paths within the structural model. Through its confirmatory factor analytical capability, PLS tested both the psychometric properties of the scales and the hypothesized structural relationships (Gefen et al, 2003).

The test of the measurement model includes the estimation of internal consistency, reliability, and discriminant validity of the instrument items. Generally, items loading greater than 0.60 on their related factor are considered acceptable (Barclay et al, 1995). As shown in the table of loadings and cross-loadings (Table 3), all items loaded above the threshold value on their corresponding factors. The correlation table is shown in Table 4 and reliability in Table 5. The recommended threshold for Cronbach's alpha is .70 (Nunnally, 1978) and average variance extracted (AVE) measures are acceptable above .50 (Hair et al., 1998). Each construct demonstrated an acceptable level of internal consistency as measured by the Cronbach's alpha and AVE. Additionally, the inter-item correlations of the constructs were all below the .90 threshold (Bagozzi *et al*., 1991) indicating the distinctness of each construct.

Discriminant validity indicates that each construct shares more variance with its measurement items than with other constructs in the model. Discriminant validity is demonstrated in PLS when indicators load higher on their corresponding construct than on other constructs in the model and when the square root of the average variance extracted (AVE) is larger than the inter-construct correlation (Chin, 1998). As shown in Table 3, all indicators loaded more highly on their own construct than on other constructs, and the square root of the AVE in bold on the diagonal in Table 4 are sufficiently larger than the construct correlations. In sum, these results suggest that the scales exhibited discriminate validity as well as acceptable psychometric properties.

	Convenience	Intent	Privacy Beliefs	Risk	Security	Social Privacy	Trust
Conv1	**0.811**	0.536	0.326	-0.191	0.310	0.079	0.375
Conv2	**0.903**	0.549	0.375	-0.017	0.266	0.171	0.298
Conv3	**0.912**	0.540	0.341	-0.026	0.224	0.195	0.305
Conv4	**0.884**	0.541	0.375	-0.043	0.278	0.160	0.262
Conv5	**0.755**	0.682	0.555	-0.247	0.498	0.044	0.531
Int1	0.521	**0.791**	0.403	-0.335	0.335	0.097	0.381
Int2	0.587	**0.756**	0.499	-0.277	0.422	0.126	0.432
Int3	0.592	**0.872**	0.590	-0.433	0.417	-0.067	0.626
Int4	0.450	**0.758**	0.531	-0.336	0.439	0.195	0.539
Int5	0.517	**0.768**	0.600	-0.259	0.515	0.064	0.539
PriBel1	0.155	0.257	**0.672**	-0.219	0.343	-0.013	0.314
PriBel2	0.214	0.372	**0.819**	-0.363	0.473	0.045	0.582
PriBel3	0.546	0.681	**0.843**	-0.294	0.571	0.141	0.647
PriBel4	0.484	0.668	**0.762**	-0.358	0.496	0.104	0.525
Risk1	-0.042	-0.340	-0.352	**0.882**	-0.295	0.058	-0.420
Risk2	-0.115	-0.380	-0.345	**0.905**	-0.416	0.243	-0.402
Risk3	-0.190	-0.423	-0.409	**0.952**	-0.447	0.054	-0.462
Sec1	0.360	0.486	0.535	-0.385	**0.894**	0.137	0.606
Sec2	0.390	0.499	0.579	-0.354	**0.925**	0.020	0.664
Sec3	0.267	0.451	0.513	-0.321	**0.836**	0.025	0.541
Sec4	0.359	0.465	0.560	-0.442	**0.868**	-0.082	0.623
Sec5	0.297	0.454	0.536	-0.376	**0.882**	-0.085	0.595
SocPri1	-0.299	-0.196	-0.145	-0.101	-0.013	**0.877**	-0.159
SocPri2	-0.238	-0.143	-0.018	-0.043	0.041	**0.854**	-0.065
SocPri3	0.193	0.124	-0.012	-0.136	-0.003	**0.664**	0.037
Trust1	0.329	0.543	0.553	-0.466	0.554	0.017	**0.856**
Trust2	0.313	0.472	0.485	-0.320	0.503	0.030	**0.770**
Trust3	0.282	0.356	0.478	-0.210	0.492	0.109	**0.746**
Trust4	0.435	0.640	0.715	-0.522	0.637	0.107	**0.924**
Trust5	0.390	0.592	0.593	-0.368	0.654	0.135	**0.842**

Table 3. Table of Loadings and Cross-Loadings

	Convenience	Intent	Privacy Beliefs	Risk	Security	Social Privacy	Trust
Convenience	**0.855**						
Intent	0.678	**0.790**					
Privacy Beliefs	0.474	0.664	**0.777**				
Risk	-0.131	-0.419	-0.404	**0.913**			
Security	0.382	0.535	0.619	-0.428	**0.881**		
Social Privacy	-0.148	-0.096	-0.101	-0.132	-0.002	**0.804**	
Trust	0.427	0.639	0.690	-0.469	0.689	0.097	**0.830**

* Values highlighted on the diagonal are SQRT of the average variance extracted (AVE).

Table 4: Correlations of Latent Variables

	AVE	Composite Reliability	Cronbach's Alpha
Convenience	0.731	0.931	0.907
Intent	0.625	0.892	0.849
Privacy Beliefs	0.604	0.858	0.783
Risk	0.834	0.938	0.901
Security	0.777	0.946	0.928
Social Privacy	0.646	0.844	0.734
Trust	0.689	0.917	0.886

Table 5: Reliability Measures

STRUCTURAL MODEL

PLS also tests the structural model which includes estimates of the path coefficients, which indicate the strengths of the relationships between the dependent and independent variables, and the coefficient of determination (R^2), which represents the amount of variance explained by the independent variables. Together, the path coefficients and the coefficient of determination indicate how well the data support the hypothesized model. Path coefficients in PLS are similar to standardized beta weights in regression analysis (Chin, 1998; Lohmoller, 1989).

Figure 2 shows the results of the test of the hypothesized structural model. Various demographic variables were included as control variables in the initial analysis. These included age, gender, education, reason for using free Wi-Fi, number of Wi-Fi devices owned, and frequency of access to Wi-Fi in the past month. Two of the variables were significant and retained in the PLS analysis. These included the number of devices owned (β = -0.132, p <.01) and level of education (β = -0.137, p <.01).

The results of the structural model analysis show support for six of nine hypothesized relationships. Trust perceptions have a significant positive influence on privacy beliefs (H1a: β = 0.687, p < .01) and security beliefs (H1c: β = 0.689, p < .01), and a significant negative influence on risk perceptions (H1b: β = -0.299, p < .01). Social privacy has a significant negative influence on (H3b: β = -0.174, p< .05), although the path to privacy (H3a) was not significant. As expected, convenience has a significant positive effect on intent to use (H5: β = 0.579, p < .01) and risk was significantly related to intent to use (H6: β = -0.312, p < .01). The remaining two hypothesized relationships not supported were between privacy beliefs and risk (H2), and security beliefs and risk (H4).

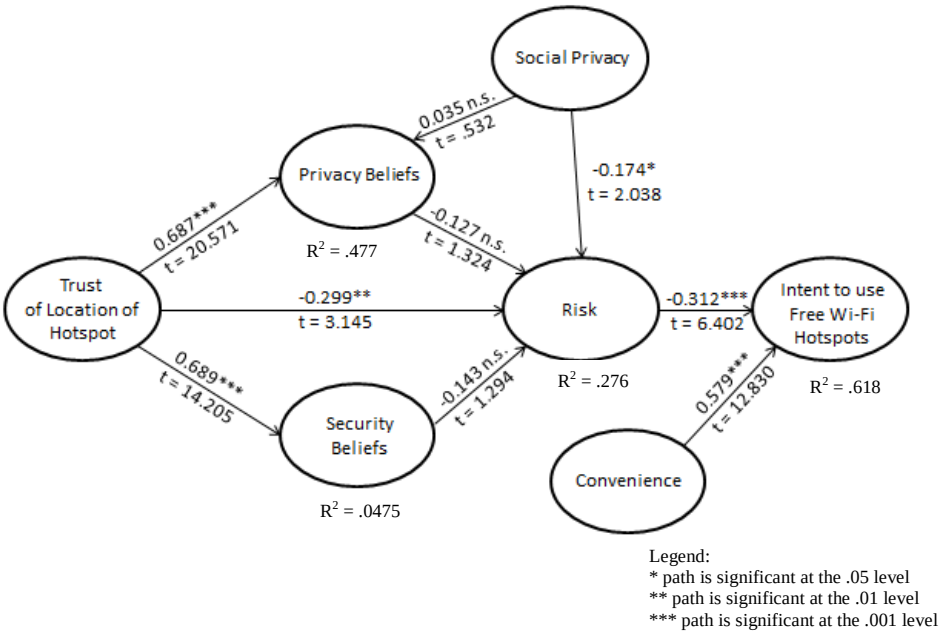

Figure 2: Structural Model

DISCUSSION

The results of the analysis provide several important insights into users of free Wi-Fi hotspots. First, when users have a greater level of trust in the location or provider of the Wi-Fi service they believe that their personal information is adequately safeguarded from the provider as well as from unauthorized third parties. As trust increases, perceptions of personal risk decrease and users are more likely to patronize the hotspot. Users hold high levels of expectations regarding their personal information and data transmissions that providers must be vigilant to maintain. One of the main drivers of consumer distrust in the internet is related to the fraudulent use of personal information (Harris Interactive, 2002), which may be especially important in a Wi-Fi context (Casalo, 2007) since the user can specifically pinpoint *where* or through *what provider* a fraud or cybercrime originated. Although Wi-Fi may be regarded as a nuance of the internet, trust may take on an expanded role with potential positive or negative consequences for the service provider. For example, if hotspots become ubiquitous trust may be the sole indicator of which hotspots are patronized, with consequential effects on the establishments providing *untrustworthy* hotspots. Consumers use free Wi-Fi for various reasons to include social networking, academic research, personal business (banking, purchases), collaboration, etc. Hence, providers that fail to understand the level of trust they are expected to maintain may regret providing the free connection if their users become victims of fraud, or worse.

It is also important for Wi-Fi locations to manage the risk perceptions of users. Users that perceive a likelihood of loss related to using the service will not use the service. This may mean that the user in need of a connection goes to a competitor whose Wi-Fi is viewed as less risky. About 28 percent of the variation in risk is explained by trust, security and privacy considerations. Interestingly, social privacy is related to overall risk indicating that for some users a physical barrier that enables private communication will reduce their risk perceptions and motivate them to use the hotspot. To increase social privacy perceptions, businesses could provide an area where consumers can access Wi-Fi in private. For example, many public libraries offer study rooms or partitions between tables to provide their patrons a sense of privacy within a social environment. Even a small 'sense' of segregation might help reduce perceptions of risk when using a hotspot.

Additionally, convenience is a strongest indicator of intentions to use a free hotspot. Convenience is a major reason why consumers use Wi-Fi to access the internet (Elliot and Fowell, 2000) and may mitigate negative factors related to connecting to Wi-Fi (Chang *et al.*,2005). However, future research should consider how trust might moderate the convenience factor. A user with a low level of trust in a certain location that is very convenient might be less likely to use that Wi-Fi provider. Providers should not over-emphasize convenience without maintaining high levels of trust. Similarly, future research should investigate the interplay between risk and convenience. Users want convenience and if denied to them, either by lack of insight or by lack of design, they will find it even at the cost risk (Gerck, 2007). The extent to which some users may ignore risk for the sake of convenience would be an interesting extension of this study.

Overall the model accounted for about 62 percent of the variance in intentions to use a free Wi-Fi hotspot. Potential users of hotspots are primarily influenced by their trust in the provider, their perceived level of risk, as well as the convenience of the hotspot location. Trust and risk are important components of user cynicism with this type of connection that could impede usage and the rapid expansion of Wi-Fi hotspots. A number of studies have analyzed trust and risk concepts related to internet use; however, the examination of user perceptions related to free Wi-Fi connections is limited but is warranted given the potential to negatively (or positively) impact the economic health of the organization offering the service.

LIMITATIONS AND FUTURE RESEARCH

Several limitations were identified in this study. The model was tested with undergraduate and graduate students which may limit the generalizability of the results to other age groups and users. Since the respondents indicated prior familiarity and use of Wi-Fi, their perceptions have likely been tempered by past experiences with the service. Thus, potential users without Wi-Fi experience are likely to express greater, not less, trepidation when considering using the service. In that regard, managing trust and risk perceptions takes on even greater significance and convenience may be a non-factor. Future research might consider the perceptions of non-users and factors that would motivate their use of free hotspots.

The construct of social privacy was newly developed for this study. It was found to be a significant antecedent of risk perceptions and researchers might further develop the construct to better understand user behavior in other contexts. Likewise, convenience is a significant determinant of use in the present study that may yield different outcomes in other contexts with different technologies. As technology, in general, becomes ubiquitous the convenience factor may achieve a prominent role in use. Will users give up safety for convenience? This seems a fruitful avenue for future study.

CONCLUSION

Businesses may offer free Wi-Fi as an incentive for customers to patronize their place of business. Whether it is a coffee shop, book store, hotel, or fast food restaurant, owners are considering ways to get consumers in their establishments, stay for an extended period of time and return on a future date. The free Wi-Fi connection is a medium through which businesses can develop long-term trust with current customers and relationships with new customers (Casalo et al. 2007). Yet, organizations that violate users' trust or who are the channel through which users' trust is violated may rue the day they implemented a free Wi-Fi hotspot. Thus, the management of consumer trust and risk are fundamental tasks for Wi-Fi providers since they are two key variables that are required in order to achieve long-term relationships (Morgan and Hunt, 1994).

In this study, user intent to use a hotspot was found to be directly influenced by convenience, a result which lends support to the findings of previous researchers (Rowley, 2006; Sanchez-Franco & Roldan, 2005). Essentially, the goal is to provide the user with a Wi-Fi connection and increase the probability of a user repatronizing the provider's establishment. Yet, a logical tension exists between the convenience of the hotspot and perceptions of risk in using the hotspot. No matter how convenient a hotspot may be, if the user feels his information or transmission is 'unsafe' in that location he is not likely to use it – and that has obvious implications for the user as a consumer of the business in general.

ACKNOWLEDGEMENT

I would like to thank Dr. Robin Wakefield, Baylor University for her guidance and encouragement throughout this research project.

REFERENCES

1. Aladwani, A. M. (2001) Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management,* 21, 4**,** 213-225.

2. Bagozzi, R., Yi, Y. and Phillips, L. (1991) Assessing construct validity in organizational research. *Administrative Science Quarterly* 36, 3, 421-458.

3. Barclay, D.C., Higgins, A., and Thompson, R. (1995) te partial least squares approach to causal modeling: Personal computer adoption and use as an illustration, *Technology Studies*, 2, 285-309.

4. Blog Reference, http://blog.foreignpolicy.com/posts/2010/03/24/quiz_how_many_wi_fi_hot_spots_are_there_in_the_world

5. Brown, L.G., (1990) Convenience in services marketing, *Journal of Services Marketing*, 4, 1, 53-59.

6. Casalo, L., Flavian, C., and Guinaliu, M. (2007) The role of security, privacy, usability and reputation in the development of online banking, *Online Information Review*, 31, 5, 583-603.

7. Chang, M. K., Cheung, W., and Lai, V. S. (2005) Literature derived reference models for the adoption of online shopping, *Information and Management*, 42, 4, 543-559.

8. Cheolho, Y., and Sanghoon, K. (2007) Convenience and Tam in a ubiquitous computing environment: The case of wireless LAN, *Electronic Commerce Research and Applications*, 6, 1, 102-112.

9. Chin, W.W. (1998) the partial least squares approach for structural equation modeling , in G.A. Marcoulides (Ed.), *Modern Methods for Business Research*, Lawrence Erlbaum Associates, Mahwah, NJ, 295-336.

10. Clay, K. and Strauss, R., (2000) Trust, risk and electronic commerce: nineteenth century lessons for the 21st century, *In: Proceedings of the 93rd Annual Conference on Taxation,* National Tax Association, Session on Taxation and E-commerce.

11. Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989) User acceptance of computer technology: a comparison of two theoretical models, *Management Science*, 35, 8, 982-1002.

12. Dearing, J., Meher, G., Kazmierczak, J., (1994) Portraying the new: communication between university innovators and potential users, *Science Communications* 16, 11-42.

13. Dinev, T., and Hart, H. (2006) An extended privacy calculus model for e-commerce transactions, *Information Systems Research*, 17, 1, 61-80.

14. Dowling, G.R., and Staelin, R., (1994) A model of perceived risk and intended risk-handling Activity, *Journal of Consumer Research* 21, June, 119-134.

15. Elliot, S. and Fowell, S., (2000) Expectations versus reality: a snapshot of consumer experience with Internet retailing, *International Journal of Information Management*, 20, 5, 323-326.

16. Federal Communication Commission, FCC adopts rules for unlicensed use of television white space www.fcc.gov accessed November 14, 2010.

17. Flavian, C. and Guinaliu, M. (2006) Consumer trust, perceived security and privacy policy, *Industrial Management and Data* 106, 5, 601-620.

18. Galanxhi-Jaanaqi, H. and Fui-Hoon Nah, F. (2004), U-commerce: emerging trends and research issues, *Industrial Management & Data Systems*, 104, 9, 744-755.

19. Gefen, D. (2003), TAM or just plain habit: a look at experienced online shoppers, *Journal of End User Computing*, 15, 3, 1-13.

20. Gefen, D. and Straub, D.W. (1997) Gender differences in the perception and use of e-mail: an extension to the technology acceptance model, *MIS Quarterly: Management Information Systems*, 21, 4, 389-400.

21. Gefen, D. and Straub, D.W. (2000) The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption, *Journal of the Association for Information Systems*, 1, 1-28.

22. Gerck, E. (2007), Convenience vs Risk – US public Elections by Email and Beyond, http://www.gather.com/viewArticle.action?articleId=281474976901451, [13 December 2010].

23. Hair, J., Anderson, R., Tatham, R., an Black, W., (1998) Multivariate Data Analysis (5th ed.) Prentice Hall, Englewood Cliffs, NJ.

24. Harris Interactive (2002) Privacy on and off the internet: what consumers want, www.aicpa.org/download/webtrust/pri_rpt_21mar02.pdf

25. Han, K.S. and Noh, M.H., (1999) Critical failure factors that discourage the growth of electronic commerce, *International Journal of Electronic Commerce*, 4, 2, 25-43.

26. Hoffman, D.L., Novak, T.P. and Peralta, M.A. (1999) Building consumer trust online, *Communications of the ACM*, 42, 4, 80-85.

27. Hosmer, L., (1995) Trust: The connecting link between organizational theory and philosophical ethics, *Academy of Management Review* 20, 379-403.

28. Hsu, C. and Lu, H. (2004), Why do people play on-line games? An extended Tam with social influences and flow experience, *Information & Management*, 41, 7, 853-68.

29. Johnson, J.D., Meyer, M. Woodsworth, M., Ethington, C., Stengle (1998), Information technologies within the cancer information service: factors related to innovation adoption, *Preventative Medicine*,1-12.

30. Kelly, E. and Erickson, S. (2005) RFID tags: commercial applications v. privacy rights, *Industrial Management and Data Systems*, 105, 6, 703-713.

31. Koller, M. (1998) Risk as a determinant of trust, *Basic and Applied Social Psychology* 9, 4, 265 – 276.

32. Kolsaker, A and Payne, C., (2002) Engendering trust in e-commerce: a study of gender-based concerns, *Marketing Intelligence and Planning*, 20, 4, 206-214.

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

34. Lo, Janice, (2010) Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites, *AMCIS 2010 Proceedings*, paper 110. http://aisel.aisnet.org/amcix2010/110.

35. Lohmoller, J.B. (1989) *Latent variable path modeling with partial least squares*. New York: Spinger-Verlag

36. Mayer, R. C., J. H. Davis, and F. d. Schoorman (1995) An Integrated Model of Organizational Trust, *The Academy of Management Review* 20, 3, 709-734.

37. McKnight, D. and Chervany, N., (2001) What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology, *International Journal of Electronic Commerce*, 6, 2, 35-59.

38. Miyazaki, A.D. and Fernandez, A. (2001) Consumer perceptions of privacy and security risks online shopping, *J. Consumer Affairs*, 35, 1, 27-44.

39. Morgan, R.M. and Hunt, S.D. (1994) The commitment-trust theory of relationship marketing, *Journal of Marketing*, 58, 20-38.

40. Nunnally, J. (1978) *Psychometric Theory* (2nd ed.). McGraw-Hill, New York, NY.

41. Ong, C.-S., Lai, J.-Y. and wang, Y.-S (2004) Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies, *Information & Management, 41, 6,* 795-804.

42. Pitkow, J.E. and Kehoe, C.M. (1996) Emerging trends in the WWW user population, *Communications of the ACM*, 39, 6, 106-108.

43. Raghupathi, W. and Tan, J. (2005) Strategic IT applications in Health Care, *Communications of the ACO*, 45, 12, 56-61.

44. Ringle, C.M., Wendel, S., and Will, A. (2005) SmartPLS 2.0 M3 (beta), http://www.smartple.de. University of Hamburg, Hamburg, Germany.

45. Rowley, J. (2006) An analysis of the e-service literature: towards a research agenda. *Internet Research*, 16, 3, 339-359.

46. Rust, R., Kannan, P. K., and Peng, N (2002) The customer economics of internet privacy, *Journal of the Academy of Marketing Science*, 30, 4, 455-464.

47. Sanchez-Franco, M.J. & Roldan, J.L. (2005) Web acceptance and usage model. *Internet Research*, 15, 1, 21-48.

48. Stone, R., and Gronhaug, K. (1993) Perceived risk: Further considerations for the marketing discipline, *European Journal of Marketing* 27, 2, 39-50.

49. Truste (2003), Identity theft and spam will deter online shopping this holiday season, *press release of Trust 2003*, available www.trust.org/about/press_release/12_01_03.php

50. Venkatesh, V. (2000) Determinants of perceived ease of use: integrating control, *Intrinsic Motivation, and Emotion into the Technology Acceptance Model. Information Systems research*, 11, 4, 342-365.

51. Venkatesh, V. and Davis, F.D. (2000) "Theoretical extension of the technology acceptance model: four longitudinal field studies", *Management Science*, 46, 2, 186-204.

52. Wang, H.Q., Lee, M.K.O., and Wang, C., (1998) Consumer privacy concerns about internet marketing, iCommunications of the ACM, *41, 3, 63-70.*

53. Westland, J.C. (2002) Transaction risk in electronic commerce, *Decision Support Systems*, 33, 1, 87-103.

54. *Webster's 11th New Collegiate Dictionary*, Merriam-Webster Inc., Springfield, MA.

55. Wold, H. and Joreskog, K. (1982) Systems under indirect observation: causality, structure, prediction, *Contributions to economic analysis*, Amsterdam, New York and North Holland

56. Yousafzai, S., Pallister, J., and Foxall, G. (2003) A proposed model of e-trust for electronic banking, *Technovation*, 23, 11, 847-860.

Appendix A: Measurement Items and References

Construct	Items	Sources
Privacy Beliefs (4)	I believe this location shows concern for the privacy of its users.	Falvin and Guinaliu (2006), adapted
	I Believe this location abide by personal data protection laws.	
	I believe this location respects the user's rights when obtaining personal information	
	I feel safe when I send personal information over a free Wi-Fi connection.	
Perceived Risk (3)	There would be high potential for loss associated with sending personal information over this location's free Wi-Fi.	Malhotra et al. (2004), adapted
	Sending personal information over this location's free Wi-Fi could cause problems.	
	There is a high risk with sending personal information over this location's free Wi-Fi.	Dinev & Hart (2006), adapted
Intent to use Free Wi-Fi Hotspots (5)	I will use free Wi-Fi in the future.	Roca et al. (2009), adapted
	I will strongly recommend that others use free Wi-Fi hotspots.	
	I intend to use free Wi-Fi hotspots as often as needed.	
	I would the free Wi-Fi at this location again.	
	I would provide this location with the information it needs so I can access free Wi-Fi.	
Security Beliefs (5)	I believe this location would have mechanisms to ensure the safe transmission of its users' information.	Ranganathan & Ganapathy (2002), adapted
	I believe this location would show great concern for the security of any Wi-Fi transmission.	
	I believe this location would have sufficient technical capacity to ensure that the data I send cannot be modified by a third party.	
	When I send data from this location, I am sure that the data will not be intercepted by an unauthorized third party.	Falvin and Guinaliu (2006), adapted
	When I send data from this location, I am sure that the data cannot be modified by a third party.	
Convenience (5)	I believe it is convenient to use this location's free Wi-Fi.	Roca et al. (2009), adapted
	I find free Wi-Fi convenient to use.	
	Using free Wi-Fi gives me convenience in accessing the Internet.	
	Using free Wi-Fi enables me to accomplish tasks at a times that is convenient for me.	
	I will perform network tasks anyplace with the use of free Wi-Fi.	Loiacono, Chen and Goodhue (2002), adapted
Trust of location of hotspot (5)	I believe this vendor providing free Wi-Fi is honest.	
	I believe this vendor providing free Wi-Fi cares about customers.	
	I am quite certain what to expect from this vendor.	
	I feel safe in my transactions with this location's free Wi-Fi.	
	I trust this location's free Wi-Fi connection will keep my personal information safe.	
Social Privacy (3)	I believe that people can view my laptop screen by looking over my shoulder.	Developed for this study
	I believe that people view others' laptop screens by looking over their shoulder.	
	I am aware of others looking at my laptop screen.	