Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility

Mauricio S. Featherman
College of Business, Washington State University, Pullman, Washington, USA

Anthony D. Miyazaki
College of Business Administration, Florida International University, Miami, Florida, USA, and

David E. Sprott
College of Business, Washington State University, Pullman, Washington, USA

Abstract
Purpose – The paper aims to examine ways to reduce privacy risk and its effects so that adoption of e-services can be enhanced.
Design/methodology/approach – Consumers that form a viable target market for an e-service are presented with the task of experiencing the e-service and expressing their attitudes and intentions toward it. Structural equation modeling is used to analyze the responses.
Findings – The paper finds that consumer beliefs that the e-service will be easy to use and that the e-service provider is credible and capable reduce privacy risk and its effects, thus enhancing adoption likelihood.
Research limitations/implications – The focus on a financial services product (online bill paying) suggests that similar research should be conducted with other high-risk e-services (such as those dealing with healthcare) and lower-risk e-services (such as subscription services and social networks).
Practical implications – In addition to addressing consumers’ privacy risk directly, e-service providers can also reduce privacy risk and its effects by enhancing corporate credibility and perceived ease of use of the service. Increased assessments of privacy risk perceptions and efforts to reduce those perceptions will likely yield higher usage rates for e-services.
Originality/value – The use of the technology acceptance model from information systems research, combined with a multi-faceted conceptualization of privacy risk, moves the examination of privacy risk to a higher level, particularly in light of the examination of the additional factors of perceived ease of use and corporate credibility.

Keywords Privacy, Risk management, Internet, Banking

Paper type Research paper

An executive summary for managers and executive readers can be found at the end of this article.

The decision to make online purchases and perform online service transactions includes an assessment of the risks involved. The array of risks, however, varies with the nature of the purchase. For instance, a different set of risks (or differentially weighted risks) may be considered for the decision to purchase a tangible good online, versus the decision to purchase a traditional service online (e.g., booking an airline flight), or the online subscription to an e-service (e.g., an electronic bill paying service). Furthermore, consumers patronizing an online service which requires the regular transmission and remote storage of confidential information may perceive elevated concerns regarding threats to the privacy of their personal and confidential information.

The purchase of online e-services is fundamentally different from the online purchase of goods or traditional services since e-services typically create a type of long-term relationship between the customer and online retailer that involves ongoing transmission and remote storage of the consumer’s confidential information. This increased transmission of confidential information (such as with financial or health-related services) suggests a greater consumer focus on privacy risk (Milne, 2000; Phelps et al., 2000; Sheehan and Hoy, 2000). While privacy risk in an online setting has been studied from a variety of perspectives including legal and regulatory issues (e.g., Caudill and Murphy, 2000; Milne et al., 2004; Miyazaki and Fernandez, 2000) and consumer risk perception (e.g., Featherman and Pavlou, 2003; Miyazaki and Fernandez, 2001; Miyazaki and Krishnamurthy, 2002; Wolfinbarger and Gilly, 2003), privacy risk perceptions in the context of e-service evaluations and usage has not been
investigated, nor have factors that may serve to mitigate those risk perceptions.

To remedy the lack of research in this area, we present two studies that examine consumer assessments of privacy risk (as well as related security and reliability concerns) involved in the online adoption and usage of an e-service. Each study examines a different factor proposed to reduce privacy risk and/or its effects, and thus enhance the likelihood of e-service adoption. The first study tests whether ease-of-use perceptions reduce perceived privacy risk while the second examines the risk-reducing impact of retailer credibility. In general, the research is a step toward encouraging the development of theory about, and methods for, reducing the effects of privacy risk in e-commerce, and specifically for e-service evaluations and adoption.

We now present a brief discussion of consumer security and privacy concerns regarding e-commerce. We then present our research model, which is followed by the two empirical studies mentioned above. We conclude with a discussion of our findings and their implications.

**E-commerce security, privacy, and risk**

Security and privacy in e-commerce settings is of considerable importance to consumers, businesses, and regulators. Security breaches of internet transmissions and databases enable the unauthorized use of consumers’ confidential information (e.g., name, address, password, social security and credit card numbers) and often result in identity theft (Milne et al., 2004). Prior research acknowledges the risks to consumer information privacy and of information misuse in the e-commerce setting (Culnan and Armstrong, 1999; Lwin et al., 2008; Miyazaki, 2008; Sprott, 2008; Wolfinbarger and Gilly, 2003). In reality, the prospect of privacy losses and information misuse in e-commerce settings may offset any convenience, time, and/or financial savings afforded to consumers. Unfortunately, security breaches are occurring at a growing rate. For example, the sophistication of phishing and pharming scams has increased and affects more unsuspecting web surfers each year (Shin, 2007). Moreover, banks, credit agencies, and payment processors continue to suffer losses of consumers’ confidential personal information (Associated Press, 2005).

New corporate disclosure laws, as well as the high profile coverage of data losses, ensures that privacy and security breaches do not go unnoticed. Indeed, Miyazaki and Fernandez (2001) found that internet users’ top-three concerns with regard to online shopping were privacy, system security breaches from third parties (due to faulty technological security), and security breaches in the form of fraudulent online retailer behavior. More recently, Litan (2005) reported that 42 percent of respondents stated that concerns about online attacks to their confidential information adversely affect their shopping behavior.

Despite the recent security and privacy breaches, e-commerce activity continues to trend upwards. In fact, retail service providers (e.g., accountants, insurance agents, bankers, and brokers) continue to deploy new online self-service technologies (e-services) to reduce costs of providing their services (e.g., preparation and submission of tax forms, insurance and loan processing, online banking, brokerage, and mortgage services).

As an example of a particular online service, a recent report estimates that 38 percent of internet users use some type of online bill paying system (Fox and Beier, 2006), which might range from an automatic debit for a single bill to the monthly manual processing of numerous payments. Considering the potential for myriad privacy issues connected with the varying degrees of online bill paying, the two studies presented herein focus on that e-service. Indeed, we propose that further investigation of consumer security, reliability, and privacy concerns surrounding the adoption of e-services is necessary if online bill payment is to become as widely accepted as e-service providers would like.

**Privacy risk**

Prior research establishes that consumer evaluations and decisions to make online purchases of tangible goods, traditional services, or e-services are better explained when consumer assessments of various risks are considered (De Ruyter et al., 2001; Featherman and Pavlou, 2003; Jarvenpaa et al., 2000; Pavlou, 2003). As mentioned previously, the two concerns most salient to online consumers are those related to privacy and security (Miyazaki and Fernandez, 2001).

Information privacy has been defined as “the claim of individuals … to determine for themselves when, how, and to what extent information about us is communicated to others” (Westin, 1967), and has become a key consumer issue as indicated by the US Federal Trade Commission’s establishment of the Division of Privacy and Identity Protection in 2006 (Federal Trade Commission, 2007). Research suggests that consumer privacy concerns are deep-rooted and growing and may actually increase as consumers gain internet shopping experience (Miyazaki and Fernandez, 2001). Indeed, consumer concern for information privacy is considered one of the most important issues of the information age (Caudill and Murphy, 2000; Sheehan and Hoy, 2000).

Although several marketing and policy studies examine online privacy concerns or risks in a general fashion (e.g., Milne and Culnan, 2004; Miyazaki and Krishnamurthy, 2002; Phelps et al., 2000; Wolfinbarger and Gilly, 2003), none focus specifically on privacy risk for e-services adoption. Within information systems research, risks to privacy are discussed, but they are not conceptualized based on perceived risk theory. For example, Malhotra et al. (2004) reiterate that consumers take high risks in the submission of personally identifying information while Suh and Han (2003) mention the risk of information theft, theft of service, and corruption of data. In general, privacy risk typically receives only a brief mention (Featherman and Pavlou, 2003) or is considered as an overall general measure of perceived risk (Pavlou, 2003; Malhotra et al., 2004).

Drawing from work on information privacy (e.g., Goodwin, 1991; Westin, 1967) and perceived risk (e.g., Taylor, 1974; Dowling and Staelin, 1994; Mitchell, 1999), we frame privacy risk as an assessment of potential losses. Specifically, privacy risk is a consumer’s subjective evaluative assessment of potential losses to the privacy of confidential personally identifying information, including the assessment of potential misuse of that information that may result in identity theft. As such, this subjective evaluative assessment can, when reinforced over time, predispose consumers to believe that an entire e-service category (e.g., online tax preparation services) or a brand within that category (e.g., TurboTax) has a certain level of privacy risk.
In the present research, we frame privacy concerns as a risk assessment which allows better measurement of the phenomenon and its consequences. Extending previous research on the effects of perceived risk in e-services adoption (De Ruyter et al., 2001; Featherman and Pavlou, 2003), we center attention on the contributors to and effects of privacy risk during consumer evaluations and decisions to use an e-service.

Consumer security and reliability concerns
In addition to privacy risk, another factor suggested to affect consumer evaluations and decisions regarding online purchases involves consumer concerns about the security and reliability of company processes in an online setting (Miyazaki and Fernandez, 2001; Suh and Han, 2003; Wolfinbarger and Gilly, 2003). These security and reliability concerns have also been suggested to influence consumer risk perceptions (Olivero and Lunt, 2004).

Consumers have been found to distrust internet shopping because they are concerned about both unscrupulous or ineffective merchants and the dubious security of the internet (Hoffman et al., 1999; Lee and Turban, 2001). Pavlou (2003) labels these two consumer concerns behavioral uncertainty and environmental uncertainty, respectively. In light of our focus on online retail services, we examine two types each of behavioral uncertainty (e-service security and e-service reliability) and environmental uncertainty (internet security and internet reliability).

The first dimension, e-service security, captures consumer evaluations of an online retailer’s security effectiveness (Lee and Turban, 2001) and perceived security control (Koufaris and Hampton-Sosa, 2004). This dimension is intended to elicit a consumer’s summary assessment of the security protection afforded by an e-service provider, based on the provider’s usage of, for example, encryption, firewall, and anti-spyware technologies. The second dimension, e-service reliability, measures the degree to which consumers believe that the e-service provider will accurately and reliably provide their service (Pitt et al., 1995).

The third and fourth dimensions, security and reliability of the internet, tap consumers’ environmental concerns (such as those regarding internet infrastructure) as they relate to the e-service in question. These concerns typically are based on subjective experience, word-of-mouth, and news reports, and thus represent an imperfect subjective assessment. Together, the dimensions are designed to gauge consumers’ security and reliability concerns regarding the particular e-service usage.

Reducing online privacy risk to facilitate e-service adoption
Basic risk research suggests that reducing risk, or reducing risk’s influence, can be beneficial in facilitating adoption or purchase behavior. Thus, our investigation is carried out in two studies that begin by examining the effects of consumer reliability and security concerns and e-service privacy risk on consumer evaluations and intended usage of an e-service. Study 1 then explores e-service ease-of-use as a potential privacy risk reduction factor. Study 2 provides further indications of the risk and security effects, but also examines whether initial evaluations of an e-service provider’s credibility and capability reduce those effects in terms of consumer assessments of an e-service and the likelihood of adopting it.

Study 1
Culnan and Armstrong (1999) propose that individuals perform a simple risk-benefit calculation when deciding whether to disclose confidential information, and when the risks outweigh the benefits, they do not disclose such information. Strader and Shaw (1997) likewise contend that consumers will not participate in e-commerce activities if they feel the risk level is unacceptable. Survey results cited by Hoffman et al. (1999) and Belanger et al. (2002) support these contentions in that consumers’ most cited reasons for rejecting online transactions were their concerns about the lack of information privacy and the potential loss of control over confidential information. Because e-services are based on the continual transmission, processing, and storage of often very sensitive financial or health-related personally identifiable information, many consumers may reject using an e-service, not because it lacks utility, but due to privacy risk. If the risks of disclosing confidential information are too high, they will not be sufficiently offset by the perceived benefits of patronizing the e-service provider.

E-commerce research finds that higher assessed usage risks reduce consumer intention to perform online purchases of goods (Pavlou, 2003) and services (De Ruyter et al., 2001), adopt an e-service (Featherman and Pavlou, 2003), and reveal personal information (Sheehan and Hoy, 1999; Malhotra et al., 2004). Such research does not, however, typically discuss privacy risk in particular. A notable exception is Sheehan and Hoy (1999), who found that privacy concerns were negatively related to the likelihood of registering for a web site that was requesting private information. The above suggests the following hypothesis:

H1. Privacy risk decreases consumer intent to use an e-service.

Perceived risk has been found to lower consumer evaluations of many different types of goods and services (Dowling and Staelin, 1994; Mitchell, 1999). Within the e-commerce context, consumers’ overall risk assessments have been found to reduce the perceived usefulness of an e-service (Featherman and Pavlou, 2003). E-services that require the transmission and storage of sensitive information are likely to be deemed less useful by consumers who consider possible exposure to security breaches, potential privacy losses, and the misuse of personally identifiable information. This suggests the following:

H2. Privacy risk decreases the perceived usefulness of an e-service.

Prior research has viewed perceived security control as a separate antecedent to consumer trust, which acts to increase trust of an e-commerce vendor (Koufaris and Hampton-Sosa, 2004; Suh and Han, 2003). Because perceived risk and trust are found to be negatively correlated (Pavlou, 2003; Pavlou and Gefen, 2004), it follows that a perceived lack of e-service security and reliability (e.g., derived from the lack of environmental structures) increases assessed levels of privacy risk. Indeed, Olivero and Lunt (2004) theorize but do not test a related relationship between a lack of environmental control and consumer perceptions of risk. Thus:

H3. Consumers’ security and reliability concerns increase assessments of privacy risk.
Risk-reducing effects of an e-service’s ease of use

Because e-services are, in essence, transaction-oriented information systems, it is practical to examine privacy risk and consumer security and reliability concerns within the parsimonious version of the technology acceptance model. The technology acceptance model is an evaluation and intentions model specified initially for information systems research. It theorizes that consumer intention to adopt a technology is based primarily on the rational assessment of outcomes of technology usage, based on beliefs of the technology’s usefulness and ease of use (Davis, 1989). Previous research suggests that a general measure of perceived risk improves the explanatory power of this model (Featherman and Pavlou, 2003).

Perceived ease of use (PEOU), a key factor in the technology acceptance model, is the degree to which an individual believes that using a particular technology would be free of cognitive effort (Davis, 1989). During pre-purchase evaluations, an e-service that appears to be easy to learn, understand, and use should alleviate consumer uncertainty and overall risk. Although initial support for this general risk-reducing effect has been found in the context of e-services (Featherman et al., 2006), it remains unknown if PEOU acts to reduce assessed levels of privacy risk in particular.

A related line of research suggests that a well-explained and easy to understand web site (i.e., one likely to be given a high rating of PEOU) increases consumer trust in an e-commerce vendor (Gefen et al., 2003). Because subsequent research indicates that trust and risk (as well as trust and security/reliability concerns) are inversely related (Pavlou and Gefen, 2004), this line of research suggests that, in addition to increasing consumer trust levels, PEOU also acts to reduce consumer perceived risk levels, as well as security and reliability concerns. Thus:

**H4.** Ease of use reduces (a) the assessed privacy risk and (b) the security and reliability concerns of using an e-service.

Method

Study 1 was conducted as an online task consisting of a pre-purchase evaluation of a little known financial bill payment e-service. A relatively unknown provider was chosen so that initial assessments of e-service reliability and security, privacy risk, and other factors were based to a large extent on respondents’ evaluations of the web site content rather than prior knowledge or experience.

Respondents were drawn from a sampling population of university students. This is an appropriate sample in that this segment is familiar with many online services and represents to a large degree the primary target market of many growing e-service providers. Since the investigation concerned initial consumer evaluations of an e-service provider, the sample was screened for prior knowledge of the service provider. Respondents were asked to read information posted on the web site of a financial e-service provider until they felt they had a good sense of how the e-service worked, could provide an evaluation, and make a usage decision. Following this was a test of the e-service wherein respondents used the online provider’s computer simulated demonstration software. Respondents then completed an evaluation of the e-service by answering the measurement items (shown in Table 1). Overall, the research session averaged approximately 30 minutes in length.

Results

A sample of 434 respondents yielded 409 usable responses. In total 97 percent of the sample reported that they currently paid monthly bills (at least partially) by mailing paper checks, thus representing a target market of the e-service. The scale psychometrics, research model, and hypothesized relationships were analyzed with structural equations modeling (maximum likelihood estimation using Mplus version 3.11). Model statistics showed that the scales exhibited strong construct validity and high scale reliability (standardized Cronbach’s alpha scores above 0.80). There was also evidence that the research model provided an excellent fit to the data (see Figure 1).

**H1,** that privacy risk would directly decrease consumer intention to use the e-service, was supported ($\beta = -0.225, p < 0.001$), as was **H2,** that privacy risk decreases perceived usefulness of the e-service ($\beta = -0.346, p < 0.001$). A significant indirect path ($\beta = -0.175, p < 0.001$) through perceived usefulness also suggests that privacy risk reduces intention to use the e-service by reducing usefulness beliefs.

**H3** was supported by finding that security and reliability concerns increase privacy risk ($\beta = 0.846 p < 0.001$). A more granular model used to measure the unique (individual) effects of each first-order facet of security and reliability concerns revealed that privacy risk was most increased by concerns for the security and reliability of the internet ($\beta = 0.372$) and concerns about the security systems of the e-service provider ($\beta = 0.326$). Reliability concerns contributed less to privacy risk ($\beta = 0.189$, all paths were significant at $p < 0.001$).

Finally, with respect to **H4,** although perceived ease-of-use did not have the hypothesized direct negative effect on privacy risk, it did have a direct negative effect on SRC ($\beta = -0.274, p < 0.001$) and thus indirectly reduced privacy risk ($\beta = -0.232, p < 0.001$).

Summary

Consumer concerns about the e-service’s security and reliability and risk to information privacy were operationalized and tested within a technology evaluation and acceptance model. For this sample and the online bill payment service context, consumer assessments of privacy risk were increased by related security and reliability concerns. Consumer beliefs that they may suffer a privacy loss reduced the perceived usefulness of the e-service as well as consumer intentions to use it. The e-service’s ease-of-use operated as an indirect privacy risk-reduction factor via its effects on reducing security and reliability concerns.

Study 2

Study 2 further tests the viability of the technology acceptance model for studying privacy risk, and also examines another privacy risk reducing factor. De Ruyter et al. (2001) found that a vendor’s good reputation reduced consumers’ overall perceptions of risk in the online purchase of a traditional service. However, the more specific privacy risk-reducing effect of vendor reputation has not been investigated. Study 2 thus focuses on consumer evaluations of a firm’s credibility (a facet of vendor reputation) and tests whether it reduces consumer assessments of an e-service’s security and reliability concerns, as well as privacy risk.
Corporate credibility refers to the degree to which consumers believe a firm can deliver the products and services the customer desires (Keller, 1998) and is composed of the perceived expertise and perceived trustworthiness of the firm (Goldsmith et al., 2000). In terms of online service provision, such expertise refers to perceptions of a vendor’s skills, competencies, and capability to deliver on service promises while trustworthiness refers to perceptions of a vendor’s sincerity, reliability, truthfulness, and dependability with respect to carrying through on service promises.

Corporate credibility can be seen as a key element in creating trust online and reducing both privacy risk and consumer security and reliability concerns. A merchant’s good reputation has been shown to increase consumer trust in an e-commerce store (Jarvenpaa et al., 2000), reduce general perceptions of risk (Mitchell and Greatorex, 1993), and reduce the effect of perceived risk on consumer intent to purchase a traditional service online (De Ruyter et al., 2001).

It remains to be tested whether consumer beliefs that an online retail service provider is reputable or credible acts to reduce privacy risk assessments and the effects of perceptions of privacy risk on consumer intention to adopt.

Many e-service providers are small, relatively unknown, and have no local physical presence. Moreover, consumers generally perceive services to be riskier purchases than

### Table 1 Psychometric properties for measurement scales

<table>
<thead>
<tr>
<th>Item loading</th>
<th>Study 1</th>
<th>Study 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and reliability concerns&lt;sup&gt;a&lt;/sup&gt;</td>
<td>E-service security</td>
<td>The security systems built into the e-billpayment service can’t assure my checking account is 100 percent protected.</td>
</tr>
<tr>
<td></td>
<td>E-service security</td>
<td>The security systems built into the e-billpayment service can’t fully protect against internet hackers (cyber-criminals).</td>
</tr>
<tr>
<td></td>
<td>Factor loading for first order factor</td>
<td>0.537</td>
</tr>
<tr>
<td>E-service reliability</td>
<td>The e-billpay service may have problems executing transactions</td>
<td>0.870&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>The e-billpay service may make mistakes and process my payments incorrectly</td>
<td>0.811</td>
</tr>
<tr>
<td></td>
<td>Factor loading for first order factor</td>
<td>0.722</td>
</tr>
<tr>
<td>Internet security and reliability</td>
<td>The internet is not secure enough to enable the e-billpay service to perform well.</td>
<td>0.868&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>The internet is not reliable enough to enable the e-billpay service to perform correctly.</td>
<td>0.865</td>
</tr>
<tr>
<td></td>
<td>Factor loading for first order factor</td>
<td>0.836&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td>Privacy risk&lt;sup&gt;b&lt;/sup&gt;</td>
<td>If you use an e-billpayment service you will lose control over the privacy of your payment information</td>
<td>0.834&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>My payment information would be less confidential if I were to use an e-billpay</td>
<td>0.901</td>
</tr>
<tr>
<td></td>
<td>Using an e-billpayment service would lead to a loss of privacy for me because my personal information would be used without my knowledge</td>
<td>0.866</td>
</tr>
<tr>
<td></td>
<td>If I used e-billpay internet hackers (criminals might access my account and steal my personal information (potential identity theft)</td>
<td>0.752</td>
</tr>
<tr>
<td>Corporate credibility&lt;sup&gt;c&lt;/sup&gt;</td>
<td>Vendor trustworthiness</td>
<td>The e-service provider is (undependable/dependable</td>
</tr>
<tr>
<td></td>
<td>Vendor trustworthiness</td>
<td>The e-service provider is (dishonest/honest</td>
</tr>
<tr>
<td></td>
<td>Vendor trustworthiness</td>
<td>The e-service provider is (unreliable/reliable</td>
</tr>
<tr>
<td></td>
<td>Vendor trustworthiness</td>
<td>The e-service provider is (insincere/sincere</td>
</tr>
<tr>
<td></td>
<td>Vendor trustworthiness</td>
<td>The e-service provider is (untrustworthy/trustworthy</td>
</tr>
<tr>
<td></td>
<td>Factor loading for first order factor</td>
<td>0.883</td>
</tr>
<tr>
<td></td>
<td>Vendor expertise</td>
<td>The e-service provider is (not an expert/an expert</td>
</tr>
<tr>
<td></td>
<td>Vendor expertise</td>
<td>The e-service provider is (inexperienced/experienced</td>
</tr>
<tr>
<td></td>
<td>Vendor expertise</td>
<td>The e-service provider is (unknowledgeable/knowledgeable</td>
</tr>
<tr>
<td></td>
<td>Vendor expertise</td>
<td>The e-service provider is (unqualified/qualified</td>
</tr>
<tr>
<td></td>
<td>Vendor expertise</td>
<td>The e-service provider is (unskilled/skilled</td>
</tr>
<tr>
<td></td>
<td>Factor loading for first order factor</td>
<td>0.824</td>
</tr>
</tbody>
</table>

Notes: <sup>a</sup> Study 1 GFI = 0.989, RMSEA = 0.066, χ²/df = 2.97. Study 2 GFI = 0.958, RMSEA = 0.067, χ²/df = 3.17; <sup>b</sup> Study 1 GFI = 0.981, RMSEA = 0.00, χ²/df = 0.53. Study 2 GFI = 0.987, RMSEA = 0.00, χ²/df = 0.78; <sup>c</sup> Study 2 CFI = 0.976, RMSEA = 0.80(0.060 – 0.101), SRMR = 0.029, χ²/df = 2.63; <sup>d</sup> Indicates a parameter fixed at 1.0; t-values for item factor loadings and factor structural coefficients in parentheses.
tangible goods (Mitchell and Greatorex, 1993). In this context, what strategies can less-known vendors use to allay consumer assessments of privacy risk and reliability and security concerns?

Drawing on Doney and Cannon’s (1997) capability process method of trust development, it appears that consumers’ initial determination of an e-service provider’s credibility and technical capability is facilitated when they read about the security technologies in force and its privacy practices. It can be argued that the prominent posting of this type of capability information on vendor web sites can send strong quality signals of the e-service provider’s capabilities and technical skill level and, ultimately, credibility (Clow et al., 1998; Kirmani and Rao, 2000).

E-service consumers (perhaps unconsciously) must often make an initial decision of “surface credibility” (Tseng and Fogg, 1999) to assess whether the service provider has the capability and credibility to continuously deliver the promised service benefits. If the vendor appears to lack credibility, then promotional messages will be unpersuasive and unsuccessful (LaBarbera, 1982). In the current study, the focal e-service provider posted claims about its strong privacy and security protections and safeguards (SSL-based 128-bit encryption and firewall technologies) on its web site. Recent research examining consumer reactions to privacy policy information (Milne and Culnan, 2004; Miyazaki, 2008) and third-party online seals of approval (Miyazaki and Krishnamurthy, 2002) suggests that many consumers will welcome these claims (even if they are not fully understood) and perhaps perceive them as signals of service performance efficacy, reliability, and expertise. Consumers who believe the service provider has the requisite expertise to provide their desired service are more likely to internalize these service claims resulting in increased trustworthiness and overall credibility.

For many consumers, beliefs that an e-service provider is capable and credible are likely to reduce consumer security and reliability concerns, and subsequently consumer assessments of privacy risk. Prior research has shown corporate credibility to reduce consumers’ general risk assessments in the context of offline purchases (Goldsmith et al., 2000). In an online context, Jarvenpaa et al. (2000) found that perceived reputation of an e-commerce merchant increases consumer beliefs of the trustworthiness of an internet store, which in turn reduces consumers’ overall perceived risk. Similarly De Ruyter et al. (2001) found that service providers’ good reputation increases consumer trust in the service provider. Because consumer trust and risk are inversely related (Pavlou, 2003; Pavlou and Gefen, 2004), these findings suggest that the perceived reputation or credibility of an e-service provider would also reduce consumer security and reliability concerns and privacy risk assessments. This suggests the following:

**H5.** Corporate credibility reduces (a) consumer security and reliability concerns and (b) consumer assessments of privacy risk.

Fombrun’s (1996) assertion that consumer perceptions of the trustworthiness and expertise of a company are used to judge the quality of a company’s products suggests that, given the potential a priori unknown nature of e-service attributes, corporate credibility may be useful in influencing consumers perceived usefulness of, and thus intention to use, an e-service. Indeed, the positive effects of corporate credibility have been established in terms of brand evaluations and purchase intent of goods (e.g., De Ruyter et al., 2001; Goldsmith et al., 2000; Keller, 1998), but have yet to be tested with respect to e-services. In the e-services context, initial assessments of the usefulness of an e-service, and consumer decisions to use it, may be improved by initial beliefs that the e-service provider is trustworthy, delivers what it promises, and has the expertise to securely and reliably perform service transactions as promised. Thus:
Reducing online privacy risk to facilitate e-service adoption

Mauricio S. Featherman et al.

H6. Corporate credibility increases (a) the perceived usefulness of an e-service and (b) consumer intention to use the e-service.

In addition to direct and indirect effects on privacy risk, there is evidence that corporate credibility may impact the effect of privacy risk on intention to use an e-service. Prior work by De Ruyter et al. (2001) suggests that a vendor’s reputation can reduce the negative effects of general perceived risk on intention to book a traditional service online. In terms of privacy risk, this suggests the following:

H7. Corporate credibility reduces the effect of privacy risk on consumer intention to use the e-service.

Method

The method for Study 2 was the same as for Study 1, except that respondents also read vendor capability information describing the vendor’s privacy statement and security protections (e.g., usage of SSL-based 128-bit encryption and firewalls). To measure corporate credibility, we adopt Newell and Goldsmith’s (2001) operational definition of corporate credibility (see Table 1). As in Study 1, the research model and hypothesized relationships were analyzed using a maximum likelihood structural equation modeling approach.

Results

A second sample (n = 266) drawn from a similar sampling population yielded 253 usable responses. General model testing results suggest strong evidence of the research model’s nomological validity (see Figure 2).

Perceived usefulness was found to increase consumer intent to use the e-service (β = 0.766, p < 0.001). Privacy risk negatively affected perceived usefulness (β = −0.180, p = 0.018) and consumer intent to use the e-service (direct effect, β = −0.126, p = 0.013; indirect effect β = −0.138, p = 0.019). Security and reliability concerns also led to increased privacy risk (β = 0.790, p < 0.001). These findings offer additional support for H1-H3.

Specific to Study 2, corporate credibility decreased security and reliability concerns and thus H5a was supported (β = −0.692, p < 0.001). At a more component level of analysis, this effect was found to be driven by trustworthiness (β = −0.691, p < 0.001), rather than expertise (β = 0.016, p = 0.863). Corporate credibility did not have a direct reducing effect on privacy risk (β = 0.039, p = 0.672), yet the results supported a significant indirect effect via SRC (β = −0.547, p < 0.001), providing support for H5b.

Corporate credibility was also found to increase the perceived usefulness of the e-service, supporting H6a (β = 0.390, p < 0.001). With respect to H6b, although corporate credibility did not increase consumer intention to use an e-service directly (β = 0.033, p = 0.531), evidence of an indirect effect via perceived usefulness (β = 0.299, p < 0.001) provided some support.

To test H7, the sample was median-split into high and low levels of corporate credibility. The median split analysis found that privacy risk affected usage intentions when corporate credibility was low (β = −0.159, p = 0.019), but not when it was high (β = 0.027, p = 0.873). The median split analysis revealed other examples of corporate credibility’s favorable effects as well. First, it was found that privacy risk did not reduce the e-service’s perceived usefulness when corporate credibility was high (β = 0.044, p = 0.876), but did when corporate credibility was low (β = −0.441, p < 0.001). Also, consumer security and reliability concerns did not serve to raise perceived privacy risk when corporate credibility was high (β = 0.441, p = 0.177), but did have an inflating effect when corporate credibility was low (β = 0.840, p < 0.001).

Figure 2 Research model and SEM results for Study 2
Reducing online privacy risk to facilitate e-service adoption

Mauricio S. Featherman et al.

Summary
Study 2 provided further support for the validity of using the technology acceptance model to examine online privacy risk in the context of the adoption of an e-service. It also provided evidence of an additional privacy risk-reducing factor, that of initial perceptions of corporate credibility, which were found to reduce privacy risk indirectly via a reduction in consumer security and reliability concerns, as well as by reducing the effect of security and reliability concerns on consumer perceptions of privacy risk. In addition, corporate credibility limited the negative impact of privacy risk by reducing its effects on the perceived usefulness and the intended usage of the e-service. Corporate credibility was also found to have direct positive effects on perceived usefulness of the e-service, as well as indirect positive effects on intention to use the e-service.

General discussion
Both Studies 1 and 2 found that security and reliability concerns influence privacy risk, which in turn, influenced the perceived usefulness of the e-service and the intentions to use it. Additionally, Study 1 found e-service ease-of-use to serve as a risk reduction factor and Study 2 found corporate credibility to reduce both perceived privacy risk and its effects on usage intentions. Jointly, the two studies also show that framing privacy concern as a risk assessment is useful in examining how privacy risk influences e-service evaluation and usage decisions. Overall, the studies integrate research on online privacy and security with that of perceived risk to refocus the determinants of consumer e-service evaluations to include a potential risk of adoption (here privacy risk) in addition to a potential benefit of adoption (here usefulness). The results provide evidence for the hypothesized negative effects of assessed privacy risk on consumers’ e-service usefulness evaluations and usage intentions.

The merger of the information privacy/security and perceived risk literatures to explain intended usage of information-sensitive e-services is an important step forward. Framing consumer privacy concerns in a specific, identifiable manner may better tap consumer uncertainties regarding their information privacy in online retail transactions. Furthermore, casting consumer adoption decisions to include both potential benefits and risks mirrors the current reality of online transacting. Analysis of the data shows that consumers chose to use or not use the online service after considering both potential benefits (usefulness) and costs (privacy risk).

Unlike purchases of tangible goods that require less personal information, e-service providers require a great deal of sensitive information for personalized service provision. This suggests that, like Mitchell and Greatorex’s (1993) finding that services make riskier purchases than tangible goods, consumer assessments of privacy risk are higher for the online purchase of e-services than for the online purchase of goods or of traditional services. High privacy risk may affect consumer evaluations and usage of many types of online retail financial services (e.g., tax preparation, banking, investment management, and bill paying) where the threat to finances accompanies, and may exacerbate, the threat to privacy. However, we recognize that many e-services may not have the same level of risk perceptions. Nevertheless, we contend that, even in the case of e-services where financial risk may be less salient (e.g. government and medical services), taking into account consumer assessments of privacy risk will better explain consumer usage of any e-services where the information transmitted and stored is sensitive and compromising such information would be harmful.

Practical implications
Online bill payment has become popular primarily due to the afforded convenience and time savings. Although many early adopters are already using this type of online retail service, further growth and deeper usage of these e-services may prove difficult, in part, because the majority of consumers do not understand the security practices of web sites where they are about to make a purchase or provide personal information (AOL/NCSA, 2005). With a lack of understanding of privacy practices and security technologies, many consumers are easily influenced by news reports of security breaches and identity theft, which can cause a quick backlash as measured by reduced e-service usage (Litan, 2005).

The findings reaffirm the importance of enhancing perceived corporate credibility regarding the use of sensitive consumer information in order to reduce perceived privacy risk and/or reduce its impact on usage intentions. Findings here and elsewhere suggest that e-service usage is dependent on online security and privacy. Many consumers, however, do not understand how to use security systems. For example, AOL/NCSA’s (2005) online safety study reports that 81 percent of respondents’ computers did not have core security protections in place although many understood the presence of security risks. In this context of overconfident, under-protected, and unknowledgeable online consumers, e-service adoption and usage will not directly increase simply by improving provider security systems. Rather, to allay consumer fears of privacy risk in using an e-service, providers must display to consumers their capability, trustworthiness, and expertise using clearer explanations and visualizations of privacy and security protection.

Interestingly, many of the consumers studied in this research failed to be persuaded by the e-service provider’s claims of information privacy, system security, and e-service performance reliability, suggesting that a clearer statement of these assurances is needed. Vendors are encouraged to improve the noticeability and readability of these assurances, with the specific goal of reducing consumer apprehension and uncertainties.

The use of the technology acceptance model from information systems research also sheds light on the ability of perceived ease of use of an e-service to influence how consumers view the security, reliability, and ultimately the privacy of their personal information when dealing with the e-service provider. E-service providers should consider the benefits of creating more user-friendly platforms, as well as training consumers in how to use them so that risks decrease and intentions to adopt the e-service increase.

Finally, e-service providers should spend more effort assessing the risk perceptions of their current and potential customers. While post-usage satisfaction scores may communicate post-adoption attitudes, word-of-mouth potential, and repeat patronage intentions, the evaluation of privacy risk can be useful in understanding why consumers do not adopt an e-service. The present research suggests that decreasing such privacy risks will likely result in higher adoption intentions.
Future research

Analyzing consumer survey data with structural equations modeling techniques represents a first step toward understanding the antecedents and consequences of privacy risk in the online retail service environment. The testing of the relationships proposed in this research, however, can be extended by using an experimental methodology, and perhaps by examining a variety of online retail service contexts. Further investigation into other costs and benefits associated with e-service adoption would also be fruitful and should assist in understanding how and when privacy and security risks affect patronage choices. Finally, there are questions as to whether the perceptions that consumers feel regarding privacy risks are indeed valid. That is, are they justified by the level of privacy protection provided by the online retailers?

Another positive aspect of the results of these two studies is the success of using privacy risk as a specific risk perception rather than using a more general approach. In fact, the results suggest that future studies of determinants of e-service adoption (and other online retail patronage), may be improved by including a specific measure of privacy risk. For example, prior work that did not find privacy and security statements to reduce general perceived risk of a web site (Miyazaki and Fernandez, 2000) may have benefited by including a more specific measure of privacy risk in lieu of a more general risk measure. The use of the specific privacy risk perception measure could benefit related research investigating third-party privacy/security seals of approval (e.g. CPA WebTrust or WebTrust Privacy seal) as well.

Finally, it may be that although e-service reliability concerns subside with experience (rendering reliability an experience attribute), the privacy and security of an e-service may be difficult to evaluate (as credence attributes) on an ongoing basis. Methods of enabling buyers to properly assess privacy and security risks may be valuable in reducing such risks or in augmenting the correlation between some objective measure of risk and the perceptions felt by consumers.

Conclusion

The popular press, surveys of the general public, and research studies cite a common problem affecting information societies and service economies: some e-service providers’ lack of security control allows damaging privacy losses and the subsequent misuse of consumers’ confidential information, as in identity theft. This results in a variety of privacy risk assessments by consumers. To examine how such risks can be reduced, we drew upon research on perceived risk and information privacy and used the technology acceptance model from information systems research to propose that consumer assessments of privacy risk regarding an e-service activity are a function of their security and reliability concerns. Moreover, the findings provide evidence that privacy risk impedes e-service adoption, but can be diminished via more favorable perceptions regarding the ease of use of the e-service web site or by initial positive evaluations of corporate credibility. To further the expansion of e-service usage, online service providers must envision new strategies to counter consumers’ salient privacy risk and should measure that risk on a regular basis.

References


Further reading


Corresponding author

Anthony D. Miyazaki can be contacted at: miyazaki@fiu.edu

Executive summary and implications for managers and executives

This summary has been provided to allow managers and executives a rapid appreciation of the content of the article. Those with a particular interest in the topic covered may then read the article in toto to take advantage of the more comprehensive description of the research undertaken and its results to get the full benefit of the material present.

Asked how much he used the internet for purchases, a colleague replied: “Never! There’s no way I’m keying in my credit card number and other personal details on a web site.” The questioner was a bit taken aback, assuming that these days most people—especially younger ones who are more used to the technology than older people—buy goods or services on the internet, from time to time at least.

But many people just do not trust buying online and this is a big problem for those who offer their products and services via a web site. The wary ones are not just Luddites, determined to shun progress; often they have good reason to be skeptical. News reports of security breaches, bogus but realistic-looking web sites, and talk of identity theft do not help. Neither does the fact that many companies offering e-services are small, unknown and do not have a physical presence. It is not just the risk of criminals getting hold of your credit card details; it is also the worry of having all the other information you have to give about yourself exposed to those who should not have access.

Security breaches are growing with the sophistication of phishing and the potentially more-serious pharming scams affecting more unsuspecting users each year. Banks and credit agencies, too, have suffered losses of confidential personal information.

So what do e-service providers do to reassure the skeptics? Whatever they do, into the mix will be an enormous lexicon of words—which have to be meant and convincing. Words like reputation, sincerity, truthfulness, reliability, dependability, security, credibility, trustworthiness. Even then some will think the risk not worth taking, even though there are degrees of risk—subscribing to an online magazine or news service, for instance, will not involve you divulging as much about yourself as would a financial or healthcare service. There will continue to be risks—just as you take a risk driving to work, crossing the road or traveling by train or plane. But, as in those cases, an informed assessment of the risk has to be taken. Consumers choose to use or not use online services after considering both potential benefits (usefulness) and costs (privacy risk).

In “Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility” Mauricio S. Featherman et al. examine ways to reduce privacy risk, concluding that privacy risk which impedes e-service adoption can be diminished via favorable perceptions regarding the ease of use of the e-service web site or by initial positive evaluations of corporate credibility. To further the expansion of e-service usage, online service providers must envision new strategies to counter consumers’ salient privacy risk and should measure that risk on a regular basis.

Their findings reaffirm the importance of enhancing perceived corporate credibility regarding the use of sensitive consumer information in order to reduce perceived privacy risk and/or reduce its impact on usage intentions. Findings here and elsewhere suggest that e-service usage is dependent on online security and privacy. Many consumers, however, do not understand how to use security systems. For example an AOL/NCSC online safety study reported that 81 per cent of respondents’ computers did not have core security protections in place although many understood the presence of security risks.

In this context of overconfident, underprotected, and unknowledgeable online consumers, e-service adoption and usage will not directly increase simply by improving provider security systems. Rather, to allay consumer fears of privacy risk in using an e-service, providers must display to consumers their capability, trustworthiness, and expertise using clearer explanations and visualizations of privacy and security protection.

Interestingly, many of the consumers studied here failed to be persuaded by the e-service provider’s claims of information privacy, system security, and e-service performance reliability, suggesting that a clearer statement of these assurances is needed. Vendors are encouraged to improve the noticeability and readability of these assurances, with the specific goal of reducing consumer apprehension and uncertainties.

The use of the technology acceptance model from information systems research also sheds light on the ability of perceived ease of use of an e-service to influence how consumers view the security, reliability, and ultimately the privacy of their personal information when dealing with the e-service provider. E-service providers should consider the benefits of creating more user-friendly platforms, as well as training consumers in how to use them so that risks decrease and intentions to adopt the e-service increase.

Finally, e-service providers should spend more effort assessing the risk perceptions of their current and potential customers. While post-usage satisfaction scores may communicate post-adoptions attitudes, word-of-mouth potential, and repeat patronage intentions, the evaluation of privacy risk can be useful in understanding why consumers do not adopt an e-service. The present research suggests that decreasing such privacy risks will likely result in higher adoption intentions.

(*A précis of the article “Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility”. Supplied by Marketing Consultants for Emerald.*)