Journal of Organizational and End User Computing, 18(1), 1-22, January-March 2006 1

Privacy, Risk Perception, and Expert Online Behavior:
An Exploratory Study of Household End Users

Judy Drennan, Queensland University of Technology, Australia
Gillian Sullivan Mort, Griffith University, Australia
Josephine Previte, The University of Queensland, Australia

ABSTRACT

Advances in online technologies have raised new concerns about privacy. A sample of expert household end users was surveyed concerning privacy, risk perceptions, and online behavior intentions. A new e-privacy typology consisting of privacy-aware, privacy-suspicious, and privacy-active types was developed from a principal component factor analysis. Results suggest the presence of a privacy hierarchy of effects where awareness leads to suspicion, which subsequently leads to active behavior. An important finding was that privacy-active behavior that was hypothesized to increase the likelihood of online subscription and purchasing was not found to be significant. A further finding was that perceived risk had a strong negative influence on the extent to which respondents participated in online subscription and purchasing. Based on these results, a number of implications for managers and directions for future research are discussed.

Keywords: e-privacy; expert; household end user; perceived risk; privacy typology

INTRODUCTION

The number of Internet users has continued to grow, with a worldwide population of 934 million as of the final quarter of 2002 (Nua Internet Surveys, 2003). In addition, household users of the Internet are increasing rapidly with 136.6 million Americans and 8.79 million Australians having online access at home (Greenspan, 2004). As this burgeoning number of household end users of the Internet embarks on new activities online,

the issue of privacy and security becomes a major concern for consumers (Milne & Rohm, 2000; Sheehan & Hoy, 2000), governments, and consumer organizations (Consumer Reports Org, 2002; Federal Trade Commission, 1996, 2000a, 2000b; Office of the Federal Privacy Commissioner, 2001a). As a result, specific calls have emerged for end-user research on security and privacy to be extended to household end users (Troutt, 2002). Businesses also recognize privacy as an important positioning tool with, for example, the ISP EarthLink positioning itself on privacy in its competition against the dominant company AOL (Sweat, 2001). Thus, as more users move to the online environment and become more expert in that environment, privacy in the electronic domain (e-privacy) needs specific research attention (Perri 6, 2002). Given the growing number of competent experienced Internet users, e-privacy issues need to be reframed and investigated in the context of their online expertise.

This article focuses on the expert household end user, defined as highly competent experienced Internet users who consistently spend time online, are likely to have subscribed to commercial and/or government Web sites, to have purchased online, and to have Internet access via a home computer. The article proceeds as follows. First, privacy conceptualizations and typologies are examined. Second, theoretical approaches to consumers' online privacy and risk perceptions are addressed, together with the argument that privacy issues from the perspective of the expert online household user need to be considered. Third, the methodology is explained, and results of the two studies undertaken are provided. Finally, findings are discussed, management implications are drawn, and future research directions are identified.

CONCEPTUALIZATION OF PRIVACY AND TYPOLOGIES

The protection of privacy has received growing attention in the literature (Buchholz & Rosenthal, 2002; Charters, 2002; Cook & Coupey, 1998; Hoy & Phelps, 2003; Milne & Rohm, 2000; Miyazaki & Fernandez, 2001) in conjunction with the advances in technology and its applications to the Internet (Sappington & Silk, 2003). There are a number of conceptualizations of privacy, but fundamentally, privacy has been viewed as the right to be left alone (Warren & Brandeis, 1890), manifesting in the definition that other people, groups, or entities should not intrude on an individual's seclusion or solitude (McCloskey, 1980). For many people, there is now an expectation of privacy as a basic consumer right (Goodwin, 1991). However, privacy is not enshrined in constitutional rights nor is it grounded as essential to the operation of a democracy, as free speech is held to be essential in countries like the United States of America. Privacy is, thus, a weak right (Charters, 2002) that may be overridden easily by other legislative rights. Privacy and anonymity also are associated for many with personal freedom and liberty. Specifically, privacy is considered to exist when consumers are able to control their personal information (McCloskey, 1980)

or restrict the use of their personal information (Culnan, 1995; Nowak & Phelps, 1995).

Some futurists, for example George Orwell in *1984* (Orwell, 1951), foreshadowed the interest of the state in observing the citizen. More recently, it is the motivation of business in monitoring and maintaining surveillance of customers, which is considered likely to undermine anonymity, privacy, and, thus, perhaps freedom, that has received the most attention (Retsky, 2001). Implicit in the conceptualization of privacy as the ability of individuals to restrict information is the recognition that there may emerge a community consensus regarding which type of personal information is not for public consumption (Charters, 2002).

It has been accepted (Westin for Federal Trade Commission, 1996) that consumers fall into three basic types with regard to privacy in the general sense: the privacy fundamentalists, who always tend to choose privacy controls over consumer benefits; the privacy unconcerned, who tend to forgo most privacy claims in exchange for service benefits; and the privacy pragmatists, who weigh the benefits of various consumer opportunities and services against the degree of personal information sought. Recently, the Westin typology has been tested and extended to apply specifically to the online consumer. The study (Sheenhan, 2002) found that online consumers in the U.S. are better represented by a four-part typology consisting of the Unconcerned, the Circumspect, the Wary, and the Alarmed Internet users. This four-part typology for online consumers was established as a result of the identification of the high percentage of pragmatists (81%) compared to the Westin study (50%). Pragmatists thus were divided into the Circumspect and the Wary groups. Fundamentalist were renamed Alarmed Internet users.

The Unconcerned Internet users rarely complain about privacy breaches and when registering at Web sites rarely provide inaccurate information. The next group, the Circumspect Internet users, have minimal concerns about privacy overall, although there are some situations that may cause them to have higher levels of concern about privacy. In addition, they give incomplete information quite often when registering for Web sites. The third group, the Wary Internet users, have a moderate level of concern with most online situations. They experience higher than average concern for Internet privacy, including clandestine data collection practices. They occasionally complain about privacy breaches and are likely to provide incomplete information when they sporadically register for Web sites. The final group, the Alarmed Internet users, are most likely to complain about privacy breaches, rarely register for Web sites, and when they do, they are likely to provide incomplete and inaccurate data.

Sheehan and Hoy (2000) also conducted a survey using 15 privacy scenarios. Results from this study indicate that privacy dimensions first are related to control over and collection of information. The other two privacy dimensions refer to pri-

vacy within a short-term transactional relationship and an established long-term relationship.

The typologies of Sheehan and Hoy (2000) and Sheehan (2002) relate to early types of technology use, such as e-mail, and construct the end user in a passive role where he or she only becomes aware of privacy issues after a breach has occurred. The studies are descriptive and do not link privacy types overtly to consequent online behaviors. Moreover, the typologies do not focus on the issue of expert end users' privacy concerns.

THEORETICAL APPROACHES TO CONSUMERS' ONLINE PRIVACY, RISK PERCEPTION, AND THE EXPERT ONLINE CONSUMER

A recent literature review has criticized privacy typologies such as Sheehan (2002) based on the conventional segmentation of fundamentalist, unconcerned, and pragmatist on a number of grounds (Perri 6, 2002). These include criticisms that the typology bears no relationship to risk in other consumption practices and has no underlying theoretical rationale to explain the privacy types. Moreover, at a practical level, criticism has been raised that the most common type, the pragmatic type, is too vague and likely to lead to business complacency. A new way of understanding privacy risk perception has been proposed (Perri 6, 2002) based on neo-Durkheimian institutionalist theory, using the social group as the unit of analysis. Perri 6 (2002) did not undertake empirical research to test the validity of the typology, and, owing to unfamiliar theoretical framework in neo-Durkheimian institutionalist theory (rather than the more usual individual psychology paradigm), it has limited practical utility for online privacy research. However, the conceptualization appears to offer some ability to understand how consumers may move in their privacy risk perception and offers marketers some insight into how privacy communication may be framed.

Consistent with Perri 6 (2002) and others (Ho & Ng, 1994; Miyazaki & Fernandez, 2001; Hoy & Phelps, 2003) we argue that perceived risk is fundamental to understanding consumer concerns about privacy online and that the relationship among privacy, risk, and online purchase intentions is central to enhancing our understanding the behavior of expert online household end users.

The issue of perceived risk in consumer purchase has been addressed by a large number of studies over the years (see, for example, Mitchell, 1999). Perceived risk can be defined as an expectation of loss (Stone, 1987) or "consumer's subjective belief of suffering a loss in pursuit of a desired outcome" (Pavlou, 2003, p. 109). Viewed in this way, risk is strongly negatively correlated with intentions and behavior (Stone, 1987). Pavlou (2003) suggests that behavioral uncertainty is created as a result of Web retailers misrepresenting products, leaking private information, providing misleading advertising, using false identities, and denouncing warranties. Specifically, consumers may perceive risks in terms of monetary losses (economic risk), the purchase of unsafe

products and services (personal risk), imperfect monitoring of products (seller performance risk), and disclosure of private information (privacy risks). Environmental uncertainty is also an important issue, leading consumers to fear theft of personal information online. Consumer intentions to transact business online are thus "contingent upon beliefs about Web retailers that are partly determined by behavioral and environmental factors," and therefore, perceived risk is likely to negatively influence consumer's intentions to undertake transactions on Internet sites (Pavlou, 2003).

Risk has been studied in a number of contexts such as food technology (Frewer, 1994), banking (Ho & Ng, 1994), and retail patronage mode (e.g., mail order, catalogue, and in-home shopping) (Festerand, 1986; Schiffman, Schus, & Winer, 1976). Different types of perceived risk have been identified, including functional, physical, financial, social, and psychological risk (Kaplan, Szybillo, & Jacoby, 1974). Saythe (1999) studied the risk referred to as "the security and reliability of transactions over the Internet," a type of physical risk, and found that this type of risk was a significant barrier to diffusion of Internet banking. Bahatnagar, Misra, and Rao (2000) examined financial and product risk in purchasing on the Web, where financial risk is related to the possibility of credit card fraud. Product risk was not as important as financial risk in predicting the likelihood of online purchases.

Perceived risk generally produces wariness or risk aversion and leads to a variety of risk handling behaviors, which include buying well-known major brands, brand loyal behavior, seeking information, wider search, increased use of use of word-of-mouth information sources, a preference for congruent rather than incongruent products in a product category, or avoiding purchase altogether (Campbell & Goodstein, 2001; Dowling & Staelin, 1994; Roselius, 1971). Concerns about privacy were not found to affect online purchasing rates directly; neither was concern about online retailer fraud, such as non-delivery of goods or misrepresentation of goods (Miyazaki & Fernandez, 2001). Only the general perceived risk of online purchase and what was termed in the study "system security issues," such as unauthorized access to personal and credit card information, were found to directly affect rates of online purchase.

Empirical research examining privacy concerns and experienced online consumers is beginning to emerge. For example, Graeff and Harmon (2002) undertook a study of U.S. consumers and asked about their privacy concerns, use, and familiarity with loyalty cards and online purchase behavior. Those with online purchase experience were significantly more likely than non-purchasers to consider that customers should be informed and have a say in such information-gathering and selling practices. In addition, Koyuncu and Lien (2002) found that those with more online experience in a private and secure home environment were more likely to purchase on the Internet.

While there has been some attention to the experienced online consumer and

privacy concerns, no research to date has empirically developed a typology of experienced "expert" household end users nor sought to relate these typologies to online behavior. Expert end users are of particular interest because they are becoming the dominant group online. We are rapidly exiting the era when most online household end users were novices with low levels of knowledge and experience in the online environment. More often, a purposeful motivation has replaced random surfing of the Internet (Rodgers & Sheldon, 2002). Experts are an important population to sample in order to answer questions about consumer privacy protection strategies online, because they are better able to distinguish between relevant and irrelevant information and have more differentiated and organized knowledge (Larkin, McDermott, Simon, & Simon, 198●).

This research addresses the need to develop an e-privacy typology of expert household end users and relate these privacy types to online behavior. Perceived risk is used as a central theoretical foundation. Informed by typologies developed in earlier research (Perry 6, 2002; Sheehan, 2002; Sheehan & Hoy, 2000), we integrate government privacy guidelines (www.dcita.gov.au) for end users to ascertain the dimensions of privacy concerns. The next section presents the method undertaken for two studies: Study 1 empirically derives a typology of e-privacy dimensions for expert household end users; Study 2 tests the causal relationships among these derived e-privacy dimensions, perceived risk, and online subscription and purchasing behaviors.

METHODOLOGY

The Sample

A sample of 76 expert household end users was recruited for the present study by surveying an Internet marketing class of university e-commerce students who all had access to the Internet via their home computers. There was a 91% response rate to the survey. Sixty-three percent of respondents were male, and 37% were female. Ninety-four percent were in the age range of 18 to 25 years old, while 6% were over 25 years old. A convenience sample of college students was considered appropriate for the current study, because demographically, they share characteristic of the stereotypical user — young, university/college-educated males. Importantly, representation of women in the sample corresponds to the changing gender trend in user statistics over time that indicates a growing population of educated women online (Rainie & Kohut, 2000). It is argued, therefore, that university or college students are representative of a dominant cohort of online users for the following reasons: the tertiary student group is the most connected segment of the population in the United States, with 93% of American college students regularly using the Internet (Nua Internet Surveys, 2002); and a similar trend is evident in the Australian population (Australian Bureau of Statistics, 2004). In addition, their visits to online shopping sites are

growing dramatically (Nua Internet Surveys, 2002). Though no specific data were available for Australia, it has further been predicted that U.S. and European teenagers are likely to spend $10.6 billion U.S. online by 2005 (Nua Internet Surveys, 2002). Thus, a sample drawn from university students is appropriate, as it is drawn from an active and rapidly growing segment of experienced and frequent users of the Internet.

Additionally, this sample was considered to be illustrative of expert household end users, as it is descriptive of experiential behavior of Internet users based on the following criteria. First, survey respondents were second-year e-commerce students who had completed courses in introductory e-commerce business studies and Web-based design and development subjects. Therefore, they meet the criteria of competence and experience. Second, as e-commerce students, they were required by their studies to spend extensive time online (approximately 20 hours per week). They thus meet the criterion of consistent time spent online. Third, expert consumers also are more likely to have subscribed to a Web site and purchased online. Approximately 54% of the sample population had purchased goods or services over the Internet. This is well above the population average for online purchasing, where only 10% had done so (Australian Bureau of Statistics, 2001). In addition, 80% of the sample had subscribed to commercial or government Web sites by exchanging personal information for free services. Thus, the sample meets the criterion of having experience in subscribing to a Web page and purchasing online.

Collecting and interpreting data about Internet use is not straightforward because of inadequacies in the sampling frame. A number of factors compromise random sampling statistical measures in Internet research, such as users holding multiple e-mail accounts and maintaining different identities to log into different commercial and non-commercial Web sites. Therefore, while numerous Internet directories are available online, their reliability is questionable compared to a sampling frame such as the commercially controlled and updated telephone listings by telecommunication companies. Consequently, the Internet population typifies characteristics of a hidden population (Heckathorn, 1997). The defining characteristics of a hidden population are that no sample frame exists, as the size and boundaries of the population are unknown. Other researchers have identified similar problems in conducting Internet research (Aladwani, 2002; Wyatt, Thomas, & Terranova, 2002) and consider the appropriateness of university/college students a useful representative sample of Internet and computer users (Wierschem & Brodnax, 2003). Nevertheless, a convenience sample reduces the generalizability of the findings to the larger Internet population. However, this sample was considered adequate and useful for the current research to address expert Internet users' privacy concerns. Furthermore, it is argued that the expert online user will continue as the dominant Internet cohort in light of emergent research that indicates

that less educated, younger Internet users are logging off (Katz & Rice, 2002). Arguably, education is a significant demographic indicator in continued Internet usage, combined with other access factors (income, etc.). Finally, when it is borne in mind that response rate to sample surveys are often low and declining, the research differences between random and convenience samples in terms of their representativeness is not always as great as some researchers wish to imply (Bryman & Cramer, 2001).

Survey Measures

Expert users were surveyed using a self-administered instrument, including a participant's information sheet and instructions for participants. The survey instrument was developed from three main sources. First, questions relating to e-privacy issues were derived from the Australian Federal Government privacy fact sheet concerning consumers' shopping on the Internet (Department of Communications Information Technology and the Arts, 2002). This fact sheet was developed as a result of extensive research by the Australian Federal Government and reflects international best practice procedures for online consumer privacy. As such, it identifies key privacy protection indicators applicable to household online users when interacting and purchasing on the Internet. These privacy protection indicators were considered particularly appropriate for use in this study, as they encompass both attitudes and behaviors toward online privacy protection.

Second, a three-item perceived risk scale (Jarvenpaa & Tractinsky, 1999) was modified to reflect risk relating to online purchasing and subscription. Specifically, two items (the first pertaining to safety of using a credit card to purchase online and the second to risk online compared to other ways of purchasing) were slightly modified to reflect online purchasing risk. A new item pertaining to perceptions of risk in revealing personal details online, if requested, was included to tap concerns relating to Web site subscription. While the original scale had a Cronbach's alpha of 0.65, the modified scale had a Cronbach's alpha of 0.58, which was a little low (Nunnally, 1989) but was accepted as satisfactory for the purposes of this exploratory research. Third, two questions were developed to ascertain whether respondents had purchased online or had disclosed personal information to subscribe to a Web site. These items were aggregated into a single item termed "online subscription and purchasing" further discussed in subsequent paragraphs. The preliminary instrument was pilot tested and reviewed for clarity by postgraduate students and the article's authors and accepted without further revision.

The survey instructions informed participants that the aim of the research was to assess awareness of online privacy issues regarding requested personal information when subscribing to Web sites or purchasing over the Internet and their perception of any risks involved in sharing information online. All privacy and risk items were measured using five-point Likert

scales, and questions relating to online subscription and purchase behavior were dichotomous.

A construct representing online subscription and purchasing transactions that involve disclosure of personal information was developed. Online subscription is a form of consumer transaction that can be described as a secondary exchange, where there is a non-monetary exchange of personal information for perceived value from the online organization in terms of quality service, prize incentives, or relationship building (Culnan & Bies, 2003). Online purchasing, on the other hand, is the first exchange, whereby money or other goods is given in exchange for goods or services (Culnan & Bies, 2003). Nonetheless, in the online environment, personal information also must be disclosed in the first exchange. Two dichotomous variables — *online subscriptions* and *online purchasing* — which provided data relating to whether respondents actually subscribed and purchased online, were combined to form a construct with ordinal properties representing no online subscriptions or purchases, online subscriptions only, online purchases only, and online subscriptions and purchases.

STUDY RESULTS

Study 1: Dimensionality of E-Privacy

Privacy dimensions were developed by submitting 12 privacy items to a principal components procedure with a varimax rotation. This analysis yielded three orthogonal factors with eigen values greater than 1.0, explaining 52.21% of the variance within these data. Factor loadings of less than 0.3 were omitted from the privacy factors, as illustrated in Table 1. The final analysis, therefore, included 11 items, as one did not load above 0.3 on any of the factors.

The grouping of statements provided insights into the interpretation of the three privacy factors. As shown in Table 1, four items loaded on Factor I, which explains 21.3% of total variance. Factor I, labeled *privacy aware*, is reflective of consumer knowledge and sensitivity regarding the risks of sharing selected personal information online. It consists of four items: selective about information provision, awareness of sensitivity of tax file number, awareness of sensitivity of mother's maiden name, and perception that companies require excessive personal information. The privacy aware factor is illustrative of users who guard information such as their mother's maiden name and are selective about the information they provide during online exchanges because they are aware of the risks involved. Significantly, these users feel that companies in the current marketplace require excessive or unnecessary information to complete an online exchange.

Factor II, labeled *privacy active*, illustrates active behaviors that users undertake relating to privacy. This factor explains 16.4% of the variance within the sample (Table 1). Four items load onto this factor: seeking detailed information about privacy policies, demanding detailed information before purchasing online, requesting that firms do not share personal details provided by the consumer, and

Table 1. Dimensionality of e-privacy factors

Privacy Statements	Mean*	S.D	Privacy Factors: Factor Loadings I	II	III
Privacy Aware					
Selective about providing information requested for transactions	3.54	1.10	**0.786**		0.303
Aware of sensitivity of tax file number	3.39	1.61	**0.743**		
Aware of sensitivity of mother's maiden name	2.38	1.62	**0.713**		
Feel online companies require excessive personal information	3.34	1.15	**0.538**		
Privacy Active					
Ask for detailed privacy policy information before purchasing online	2.41	1.44		**0.740**	
Look for privacy policies	2.04	1.26		**0.646**	0.419
Request firms do not share personal information and details with other organizations	2.91	1.51		**0.578**	
Do not regularly use the same password	3.03	1.18		**0.425**	
Privacy Suspicious					
Aware companies plan to share consumer's personal information with other companies	3.64	1.20		-0.339	**0.693**
Believe companies' privacy policies are difficult to find	3.00	0.99	-0.415		**0.673**
Before transacting with businesses online, they check to ensure e-mail and phone numbers are provided	3.40	1.52			**0.570**
Eigen values					
% Variance–Factor			21.332	16.421	14.457
% Variance–Cumulative			21.332	37.7543	52.210

*All item means display pro-dimension agreement. Factor loadings of less than 0.3 have been omitted, and those judged to constitute a factor -- the dominant loadings -- are in boldface.

regularly changing passwords to guard their privacy. Those users who take action to guard their privacy are more likely to perceive reduced risk. If the benefits of disclosing information outweigh the risks, it is likely that they will divulge the personal information required for online subscription or purchasing transactions (Culnan & Bies, 2003). However, as Graeff and Harmon (2002) found, experienced online purchasers demand to be informed and/or have a say in the sharing between organizations of their personal information.

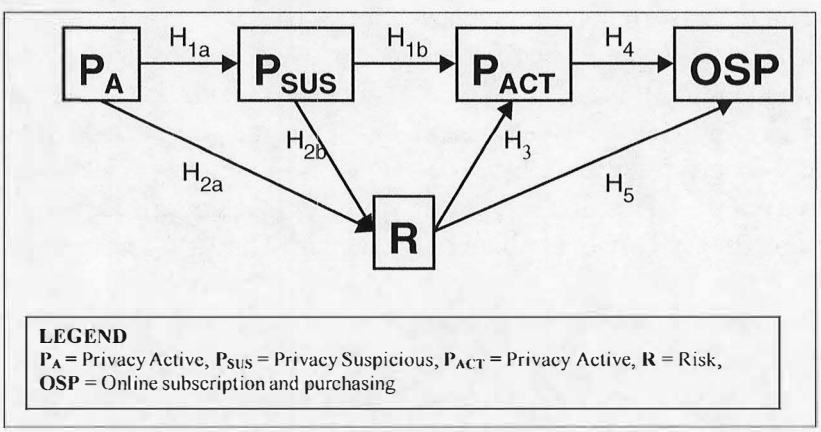
Factor III, labeled *privacy suspicious*, highlights consumer concerns about company behavior and explains 14.45% of the total variance (Table 1). For example, these online household end users are concerned about how companies use personal information and potentially divulge users' details. Three items load onto this factor: awareness of companies' plans to share personal information, belief that company privacy policies are hard to find, and checking to ensure that e-mail and online phone numbers are provided before transacting with a company. The privacy suspicious construct highlights the point that users' privacy concerns also extend to suspicions that commercial organizations may fail to guard consumer data and privacy. Previous privacy research (Sheehan & Hoy, 2000) found that users' concerns about privacy increased because of company management behavior, such as disclosing a consumer's personal information without permission. In contrast, users' beliefs that firms use fair information practices will ease privacy concerns (Culnan & Bies, 2003) and should reduce perceived risk.

Study 2: Relationship Between E-Privacy Dimensions, Perceived Risk, and Online Subscription and Purchasing Behavior

Development of Hypotheses

Figure 1 illustrates a number of inferred causal relationships between the expert end-user privacy dimensions empirically derived in Study 1: perceived risk and online subscription and purchasing behaviors. These were tested in the second stage of this exploratory research using a probabilistic approach to causation. De Vaus (2001) defines probabilistic approaches to causation as the argument that a given factor increases (or decreases) the probability of a particular outcome. We

Figure 1. A model depicting the relationships among privacy dimension, perceived risk, and online subscription and purchasing



now develop the hypotheses that drive Study 2 and discuss the relationship between privacy concerns, risk, and outcome behavior in terms of the e-privacy dimensions of privacy awareness, privacy suspicion, and privacy active derived in Study 1. We present two lines of argument. In the first, we adopt a hierarchy of effects model of expert household end users' privacy concerns, relating awareness to suspicious to active. The hierarchy of effects is a well-recognized marketing model (Lavidge & Steiner, 1961) that proposes that consumers move through subsequent stages of awareness (think), affection (feel), and conation (do). Moreover, this model has been used specifically in Internet-related research (Huizingh & Hoekstra, 2003) to describe attitudinal changes of online consumers leading to behavioral changes after visiting a Web site. In the second line of argument, the relationships among the stages in the privacy hierarchy and perceived risk are proposed. We then propose a relationship among the end stage of the privacy hierarchy, privacy active, and online subscription and purchasing intentions. We conclude with a proposed relationship among perceived risk, and online subscription and purchasing behavior. The proposed relationships are shown in Figure 1.

Privacy awareness and the extent of knowledge about privacy issues have been raised by a number of researchers (Graeff & Harmon, 2002). However, there has been little research to examine the impact of this awareness on subsequent privacy attitudes and protective behaviors. Dhillon and Moore's (2001) research suggests that as consumers become more aware of privacy issues, they question how firms use the information that is collected about them. These authors suggest that the provision by consumers of such information should be made discretionary. This questioning and apparent suspicion aroused in consumers leads us to hypothesize that higher levels of privacy awareness are related positively to increased levels of privacy suspicion (Hypothesis 1a).

In proposing the next stage of the privacy hierarchy, a relationship between privacy suspicious attitudes and privacy active behaviors, we adopt a hierarchy of effects argument. We argue that privacy suspicion of company online behavior may lead to proactive behavior by expert household end users to protect their privacy; that higher levels of privacy suspicion lead to privacy active behavior (Hypothesis 1b). Moreover, consistent with our hierarchy of effects approach whereby awareness leads to affect before action, we propose that there will be no direct link between privacy awareness and privacy active behavior. This leads to Hypothesis 1c that privacy awareness does not directly affect privacy active behavior.

We now consider the relationships between the stages of the privacy hierarchy and perceived risk. Research by Novak and Phelps (1995) suggests that privacy awareness leads to a greater perception of threat to consumer privacy. We thus hypothesize that higher levels of end user privacy awareness lead to heightened perceived risk (Hypothesis 2a). Culnan and Bies (2003) argue that consumers will

perceive disclosure of personal information to be low risk, if they believe the company to be open and honest about their information practices. Conversely, it can be argued that if end users are suspicious of a company's honesty, their perceived risk is likely to be heightened. Therefore, we hypothesize that the extent of end-user suspicion of a company will be related positively to perceived risk (Hypothesis 2b).

We have argued that a hierarchy of effects exists for privacy and that privacy awareness leads to privacy suspicion, which subsequently leads to privacy active behavior. It is further argued that privacy active behavior by expert end users is also influenced by perception of risk. Thus, a relationship between higher levels of perceived risk and privacy active behavior is proposed (Hypothesis 3).

Returning to the end stage of the privacy hierarchy, we suggest that privacy active behavior influences online subscription and purchasing. We argue that expert household end users who take action to protect their privacy are then more likely to subscribe to Web sites and to make online purchases. This leads us to hypothesize that high levels of privacy active behavior are related positively to online purchase and subscription (Hypothesis 4).

Finally, relying on research by Miyazaki and Fernandez (2001) and Pavlou (2003), which suggests that risk perceptions of Internet privacy relate to online purchasing behavior, we propose that higher levels of perceived risk negatively influence online subscription and purchasing (Hypothesis 5).

H1a: The extent of end users' awareness of threats to privacy in the online environment will be related positively to their privacy suspicious attitudes.

H1b: The extent of end users' privacy suspicious attitudes will be related positively to their online privacy active behavior.

H1c: No direct relationship will be found between privacy awareness and online privacy active behavior.

H2a: The extent of end users' awareness of threats to privacy in the online environment will be related positively to perceived risk.

H2b: The extent of end users' suspicious attitudes toward company online behavior will be related positively to perceived risk.

H3: The extent of end users' perceived risk will be related positively to active online privacy protection behavior.

H4: The extent of end users' active online privacy protection behavior will be related positively to online subscription and purchasing behavior.

H5: The extent of end users' perceived risk will be related negatively to online subscription and purchasing behavior.

Regression Analyses

To test these hypotheses, simple and multiple regression analyses were employed to examine relationships among the privacy awareness, privacy suspicious, privacy active, and perceived risk constructs. Multinomial logistic regression

Table 2. Results of regression analysis of e-privacy dimensions influencing perceived risk and privacy active behavior

(a) Effect of privacy awareness on privacy suspiciousness			
			Sig
Adj R Square = 0.162	F= 14.549		0.000
Variable	β	t	
Privacy Aware (H1a)	0.417	3.814	0.000
(b) Effect of privacy awareness and privacy suspiciousness on privacy active behavior			
			Sig
Adj R Square = 0.217	F= 10.406**		0.000
Variable	β	t	
Privacy Suspicious (H1b)	0.353	3.001	0.004
Privacy Aware (H1c)	0.225	1.912	0.060
(c) Effect of privacy awareness and privacy suspiciousness on perceived risk			
			Sig
Adj R Square = 0.286	F= 15.039		0.000
Variable	β	t	
Privacy Aware (H2a)	0.041	0.369	0.713
Privacy Suspicious (H2b)	0.535	4.819	0.000
(d) Effect of perceived risk on privacy active behavior			
			Sig
Adj R Square = 0.264	F= 27.148		0.000
Variable	β	t	
Perceived risk (H3)	0.523	5.210	0.000

analyses were used to examine the effect of these constructs on online subscription and purchasing.

Results of simple and multiple regression analyses are reported in Table 2. Simple regression was used to examine the influence of privacy awareness on privacy suspicious (H1a) and findings show that 16% of privacy suspicious is explained by privacy awareness (Beta = 0.417, p < 01). Thus, Hypothesis 1a is supported. The influence of privacy awareness and privacy suspicious on privacy active behavior also was tested (H1b) and showed that 24% of privacy active behavior is explained with only privacy suspicious as statistically significant (Beta = 0.353, p < 01). Thus, Hypothesis 1b is supported, and there is also support for the hierarchy of privacy effects model, as there is no direct relationship between privacy aware and privacy active (H1c).

In the next step, multiple regression analysis was undertaken to test the influence of privacy awareness and privacy suspicious on perceived risk (H2a and H2b), and results show that 29% of variance is explained. However, only privacy suspicious (Beta = 0.535, p < 01) is statistically significant; thus, only Hypothesis 2b is supported.

To test whether privacy active behavior was influenced by perceived risk (H3), simple regression was used, and results show that a positive relationship exists with 27% of privacy active behav-

Table 3. Results of multinomial logistic regression of perceived risk and privacy active behavior on user subscription and consumer purchasing behavior online

(a) Effect of perceived risk and privacy active behavior on online subscription and purchasing behavior			
Variables	-2 Log Likelihood	Chi Square	Sig
Intercept	135.780	16.308	0.001
Privacy Active (H4)	122.114	2.642	0.450
Perceived Risk (H5)	150.515	31.043	0.000
(b) Effect of perceived risk, privacy active behavior, privacy suspiciousness, and privacy awareness on online subscription and purchasing behavior			
Variables	-2 Log Likelihood	Chi Square	Sig
Intercept	135.917	14.593*	0.002
Perceived Risk	145.856	24.532**	0.000
Privacy Active	123.510	2.186	0.535
Privacy Suspicious	123.941	2.618	0.454
Privacy Aware	122.090	0.767	0.857

ior being explained by perceived risk (Beta = 0.353, $p < 01$); thus, Hypothesis 3 is supported.

Multinomial logistic regression then was used to examine whether privacy active behavior was positively related to online subscription and purchasing (H4), and perceived risk was negatively related to online subscription and purchasing (H5). Results (refer to Table 3) show that only the negative influence of perceived risk is statistically significant. To establish that there were no influences on online subscription and purchasing from privacy awareness and privacy suspicious, multinomial logistic regression also was undertaken that included all four constructs. Only perceived risk was found to be a significant influence. Table 4 provides a summary of the results of the hypotheses.

DISCUSSION

The findings of this exploratory study reveal the dimensionality of e-privacy for a sample of expert online household end users: privacy aware, privacy suspicious, and privacy active. In addition, results suggest the presence of a privacy hierarchy of effects where awareness leads to suspicion, which subsequently leads to active behavior. An important finding was that privacy active behavior, which was hypothesized to increase the likelihood of online subscription and purchasing, was not found to be significant. This is consistent with Donmeyer and Gross (2003), who found that those who took action to protect their privacy were also less likely to subscribe and purchase online. It seems that expert household end users feel that any privacy active behaviors that they undertake may be necessary but not sufficient to lead them to be more likely to engage in

Table 4. Summary of results of hypotheses

H1a:	The extent of end users' awareness of threats to privacy in the online environment will be related positively to their privacy suspicious attitudes.	**Supported**
H1b:	The extent of end users' privacy suspicious attitudes will be related positively to their online privacy active behavior.	**Supported**
H1c:	No direct relationship will be found between privacy awareness and online privacy active behavior.	**Supported**
H2a:	The extent of end users' awareness of threats to privacy in the online environment will be related positively to perceived risk.	**Not Supported**
H2b:	The extent of end users' suspicious attitudes toward company online behavior will be related positively to perceived risk.	**Supported**
H3:	The extent of end users' perceived risk will be related positively to active online privacy protection behavior.	**Supported**
H4:	The extent of end users' active online privacy protection behavior will be related positively to online subscription and purchasing behavior.	**Not Supported**
H5:	The extent of end users' perceived risk will be related negatively to online subscription and purchasing behavior.	**Supported**

online subscription and purchasing. This is a possible explanation for the previous finding of Miyazaki and Fernandez's (2001) research on consumers. Perceived risk was heightened by privacy suspicion but not simply by privacy awareness. This finding indicates that there may be some threshold level that must be achieved in the privacy hierarchy of effects before risk is perceived. Perceived risk was found to increase levels of privacy active behavior and decrease online subscription and purchasing behavior. Thus, it appears that it is not sufficient to consider privacy concerns alone but rather the interrelationship between privacy concerns and perceived risk, if we are to understand the drivers of online subscription and purchasing for the expert online household end user.

As the explanatory power of privacy awareness on suspicion is relatively low, other factors, such as personal attributes (Dowling & Staelin, 1994) and specific experiences, also may need to be considered in future research as additional triggers of perceived risk.

The results of this study suggest that the task of building online confidence in

terms of privacy issues is a complex one. The results, which indicate that action by users to protect privacy do not positively impact online and purchase behavior, suggest that expert online household end users may feel that at this stage the options available to protect their privacy are not sufficient. This suggests that companies may need to provide more effective privacy protective options to all online users. It is also possible that governments may need to legislate more effectively in this area and make available legal recourse to assist and protect end users.

This research has advanced our understanding of e-privacy by putting forward a new typology of expert online household end users' privacy concerns. The existing typologies (Perry 6, 2002; Sheehan, 2002; Sheehan & Hoy, 2000) are more appropriate to the earlier types of technology, such as e-mail, while our typology is relevant to more sophisticated uses, such as e-commerce. Moreover, the existing typologies construct the end user in a passive role, where they only become aware of privacy issues after a breach has occurred (e.g., when they receive e-mail from an unknown company). Our research acknowledges and incorporates a heightened sensitivity to privacy on the part of the end user, resulting from expertise in the online environment. The previous studies also are largely descriptive and, unlike our study, do not conceptualize privacy in a hierarchy of effects, nor do they link privacy concerns specifically to online behaviors.

Management Implications and Future Research

The telephone, television, and now the Internet are just some of the technologies available to managers who are responsible for new considerations of issues related to privacy. Internet technologies are important for managers, because they transform the way in which goods and services are bought and sold and provide new opportunities for developing and maintaining longer-term relationships with household end users. However, if these relationships are to be sustained, household end users need to be reassured that organizational collection and use of personal data will not involve invasions of privacy.

As suggested by the results in the present study, expert household end users may be concerned about how personal information is collected, shared, and used by companies in today's marketplace. The important question for managers in the future is how to respond to these issues. Currently, management reactions to privacy concerns include a range of activities, such as adding privacy policies to Web sites, use of encryption methods, and security protocols to guard against misuse of sensitive and private information. Findings from this study suggest that managers need to consider whether technical security solutions are the answer to resolving consumer concerns about privacy online. As Katz (2002) states, a number of encryption methods are flawed, and anonymous remailer and other anonymity-guaranteeing services

have been compromised by browser software. It appears that expert users may have become aware of such weaknesses in current technical approaches to Internet security.

Expert household end users may respond to the provisions of detailed information and clarification about the steps a company will take to guard their personal information. For example, if companies wish to develop a long-term relationship with expert end users, they may need to provide, for example, details during a transaction of how the information is to be used and then discarded after each individual transaction. Research is needed to investigate expert household end users' information requirements and their desired level of control over their personal information. Ultimately, improved privacy protection strategies and procedures are likely to enhance a company's competitive position, because it will be able to retain customers who perceive lower levels of risk and are willing to enter longer-term partnerships.

While this exploratory research has gone some way toward elucidating the dimensionality of privacy concerns of expert household end users and understanding the relationships among privacy concerns, perceived risk, and online subscription and purchasing, a more comprehensive study needs to be undertaken to confirm these findings. In addition, research is required to test the cross-national validity of the model. As highlighted previously, research also is needed to understand expert household end users' information requirements and their desired level of control over the information provided during e-commerce and other transactions. Finally, the research agenda in this field also would benefit from a study on the perceived locus of risk and whether it is at the level of the vendor company, the product, or in the transaction medium itself. More specific information like this will allow management to direct its risk minimization strategies to the correct target and to have greater impact for the expert end user.

REFERENCES

Aladwani, A. M. (2002). Organizational actions, computer attitudes, and end-user satisfaction in public organizations: An empirical study: An empirical study. *Journal of End User Computing, 14*(1), 42-49.

Australian Bureau of Statistics. (2001). *Use of the Internet by householder: Australia* (Catalogue: 8147.0). Canberra, Australia: Government Printing Office.

Australian Bureau of Statistics. (2004). *Measures of a knowledge-based economy and society, Australia information and communications technology indicators*. Retrieved November 25, 2004, from http://www.abs.gov.au

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience and Internet shopping behaviour. *Communications of the ACM, 43*, 98-105.

Bryman, A., & Cramer, D. (2001). *Quantitative data analysis with SPSS Release 10 for windows: A guide for social scientists*. London: Routledge.

Buchholz, R. A., & Rosenthal, S. B. (2002). Internet privacy: Individual rights and the common good. *SAM Advanced Management Journal, 67*(1), 34-41.

Campbell, M. C., & Goodstein, R. C. (2001). The moderating effect of perceived risk on consumers' evaluations of product incongruity: Preference for the norm. *Journal of Consumer Research, 28*(3), 439-450.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the double click experience. *Journal of Business Ethics, 35*(4), 243-255.

Consumer Reports Org. (2002). *Big browser is watching you*. Retrieved July 10, 2003, from http://www.consumerreports.org/main/detailv2.jsp?CONTENT%3C%3Ecnt_id=18207&FOLDER%3C%3Efolder_id=18151&domUID=1057810848320

Cook, D. L., & Coupey, E. (1998). Consumer behavior and unresolved regulatory issues in electronic marketing. *Journal of Business Research, 41*, 231-238.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing, 9*(2), 10-20.

Culnan, M. J., & Bies, R. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342.

Department of Communications Information Technology and the Arts. (2002). *Consumer privacy fact sheet*. Retrieved from http://www.dcita.gov.au

De Vaus, D. (2001). *Research design in social research*. London: Sage Publication.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk handling activity. *Journal of Consumer Research, 21*(1), 119-154.

Federal Trade Commission. (1996). *Consumer information privacy hearings*. Retrieved July 10, 2003, from http://www.ftc.gov

Federal Trade Commission. (2000a). *FTC sues failed Website, Toysmart.Com, for deceptively offering for sale personal information of Website visitors*. Retrieved July 10, from http://ftc.gov/opa/2000/07/toysmart.htm

Federal Trade Commission. (2000b). *FTC announces settlement with bankrupt Website, Toysmart.Com, regarding alleged privacy violations*. Retrieved July 21, from http://www.ftc.gov/opa/2000/07/toysmart2.htm

Festerand, T. A., Snyder, D. R., & Tsalikis, J. D. (1986). Influence of catalog versus store shopping and prior satisfaction on perceived risk. *Journal of the Academy of Marketing Science, 14*(4), 28-36.

Frewer, L., Shepherd, R., & Sparks, P. (1994). The interrelationship between perceived knowledge, control and risk associated with a range of food related hazards targeted at the self, other people and society. *Journal of Food Safety, 14*, 19-40.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of*

Public Policy and Marketing, 10(1), 149-167.

Graeff, T., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318.

Greenspan, R. (2004). Three-quarters of Americans have access from home. *Click Z News Formerly Internet Advertising Report*. Retrieved October 18, 2004, from http://www.clickz.com/news/article.php/3328091

Ho, S. S. M., & Ng, V. (1994). A study of consumers risk perception of electronic payment systems. *International Journal of Bank Marketing, 12*(4), 26-38.

Hoy, M. G., & Phelps, J. (2003). Consumer privacy and security protection on church Web sites: Reasons for concern. *Journal of Public Policy & Marketing, 22*(1), 58-70.

Huizingh, E. K. R. E., & Hoekstra, J. C. (2003). Why do consumers like Websites? *Journal of Targeting, Measurement and Analysis for Marketing, 11*(4), 350.

Jarvenpaa, S., & Tractinsky, N. (1999). Consumer trust in an Internet store: A cross-cultural validation. *JCMC, 5*(2).

Kaplan, L., Szybillo, G.J., & Jacoby, J. (1974). Components of perceived risk in product purchase: A cross validation. *Journal of Applied Psychology, 59*, 287-291.

Katz, J. E., & Rice, R. E. (2002). *Social consequences of Internet use: Access, involvement, and interaction*. Cambridge, MA: MIT Press.

Larkin, J., McDermott, J., Simon, D. P., & Simon, H. A. (1980). Models of competence in solving physics problems. *Cognitive Science, 208*, 317-345.

Lavidge, R. J., & Steiner, G. A. (1961). A model for predictive measurements of advertising effectiveness. *Journal of Marketing, 25*, 59-62.

McCloskey, H. (1980). Privacy and the right to privacy. *Philosophy, 55*(211), 17-38.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19*(2), 238-249.

Mitchell, V.-W. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing, 33*(1/2), 163-195.

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

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual - Level consumer information: Determining how and why privacy matters. *Journal of Direct Marketing, 9*(3), 46-60.

Nua Internet Surveys. (2002). *How many online?* Retrieved April 1, 2003, from http://www.nua.com/surveys/how_many_online/index.html

Nua Internet Surveys. (2003). *Nielsen netratings: Global net population increases*. Retrieved October 18, 2004,

from http://www.Nua.Com/Surveys/Index

Office of the Federal Privacy Commissioner. (2001a). *Privacy and the community [Web].* Retrieved February 2, 2003, from http://www.privacy.gov.au/publications/rcommunity.pdf

Orwell, G. (1951). *1984.* London: Secker and Warburg.

Pavlou, P. (2003). Consumer acceptance of electronic commerce: Interating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Perri 6. (2002). Who wants privacy protection and what do they want? *Journal of Consumer Behaviour, 2*(1), 80-100.

Rainie, L., & Kohut, A. (2000). *Tracking online life: How women use the Internet to cultivate relationships with family and friends.*

Retsky, M. L. (2001). Just posting cookies agreement not enough. *Marketing News, 35*(20), 12-13.

Rodgers, S., & Sheldon, K. M. (2002). An improved way to characterize Internet users. *Journal of Advertising Research, 42*(5), 85-94.

Roselius, T. (1971, January). Consumer rankings of risk reduction methods. *Journal of Marketing, 35*, 56-61.

Sappington, D., & Silk, A. (2003). Marketing's information technology revolution: Implications for consumer welfare and economic performance: Overview of the special issue. *Journal of Public Policy and Marketing, 22*(1).

Saythe, M. (1999). Adoption of Internet banking by Australian consumers. *International Journal of Bank Marketing, 17*(7), 324-334.

Schiffman, L. G., Schus, S., & Winer, L. (1976). Risk perception as a determinant of in-home consumption. *Journal of the Academy of Marketing Science, 4*(4), 753-763.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing, 19*(1), 62-73.

Sheenhan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Age, 18*, 21-32.

Stone, R. N., & Winter, F. W. (1987). Risk: Is it still uncertainty times consequences? In Belk, R.W. et al. (Eds.), *Proceedings of the American Marketing Association*, 261-265.

Sweat, J. (2001). Earthlink: An ISP that customers can trust? *InformationWeek,* (851), 36.

Warren, S. D., & Brandeis, L. D. (1890, December). The right for privacy. *Harvard Law Review, 4*, 193-220.

Wyatt, S., Thomas, G., & Terranova, T. (2002). They came, they surfed, they went back to the beach: Conceptualizing use and new use of the Internet. In S. Woolgar (Ed.), *Virtual society? Technology, cyberbole, reality.* Oxford: Oxford University Press.

Judy Drennan is a senior lecturer in marketing in the Faculty of Business at Queensland University of Technology, Australia. Her qualifications include a PhD from Deakin University and a master's of education from Melbourne University. She researches in the areas of electronic marketing and entrepreneurship, and her work has been published in the Journal of Services Marketing, Journal of Database Marketing, *and the* International Journal of Innovation and Entrepreneurship.

Gillian Sullivan Mort is associate professor in marketing in the Griffith Business School, Griffith University, Gold Coast, Australia. Her qualifications include an earned doctorate in management and a master's of business administration. Her research interests include consumers and new technology, social entrepreneurship, and "born global" firms.

Josephine Previte is an associate lecturer in marketing in the UQ Business School at the University of Queensland, Australia. She is currently completing doctoral research examining the diffusion of social marketing strategy in online environments. Her other research interests include feminist theory and the social construction of new technologies.