Modelling Online Security and Privacy to Increase Consumer Purchasing Intent

Michael Milloy, Dieter Fink and Robyn Morris
Edith Cowan University, Perth, Western Australia

gtrock@iinet.net.au d.fink@ecu.edu.au r.morris@ecu.edu.au

Abstract

This paper investigates the concerns consumers have with respect to security and privacy when determining purchasing intent in the Web environment. The online retailing environment (e-retailing) is examined and various issues relating to security and privacy are identified as potential inhibitors for e-retailing. The paper then presents a model of the interaction between online security and online privacy taking into account the online experience levels of consumers and the role that symbols and statements have on security and privacy considerations. Based on the theoretical foundations of the paper, a number of research propositions are developed which can be tested by subsequent empirical research. The paper concludes that security and privacy are evolving issues both requiring continuing research. It can however be postulated that consumers will, albeit slowly, come to terms with online security and privacy, possibly due to different reasons. An improved understanding of how these issues impact on consumer purchasing intent will enhance e-retailers' ability to formulate strategies to overcome inhibitors and incorporate promoters of trust with respect to security and privacy issues into their website designs. This may well speed up the process of consumers coming to terms online security and privacy and can only serve to foster the growth of e-retailing in the future.

Keywords: e-retailing, online security, online privacy, consumer trust

Introduction

Although the expectations and possibilities are high for the new medium of the World Wide Web (Web) to be a major economic contributor to the world's economy there are an abundance of issues cited in the literature as inhibitors to its uptake for retailing (also referred to as e-retailing). There are various inhibitors contributing to online consumers distrusting the Web environment when considering a purchase which have attracted the attention of researchers in recent years (e.g. Archetype/Sapient, 1999; Auger, 1997; Doney and Cannon, 1997; George, 1999; Treasury, 2000).

The exponential growth of *online users* doesn't translate directly to *online consumers.* This is supported by statistics (Skinner, November, 1999; February, 2000; December, 2000) that show online users are slow to adopt online purchasing habits. An important issue in e-tailing research therefore is determining how factors impact on online consumers' purchasing intent. Intent to purchase is largely related to the amount of trust that the potential consumer has when engaging with a retailer in the e-environment. Trust must be established as soon as interaction with a Web site begins (Fink, 1999). In the virtual environment of the Web trust is important because the parties are not in physical proximity. There are no handshakes or body language to be observed when

closing a deal to enable to enable the consumer to evaluate the trustworthiness of the e-retailer.

To-date, there has been little research establishing factors and the relationship between them that increase potential consumers' willingness to purchase on the Web. Amongst the notable concerns identified by consumers when making purchasing decisions on the Web are security, especially in relation to the integrity of financial transactions (Archetype/Sapient, 1999), and privacy, mainly for credit card and other personal information (Archetype/Sapient, 1999; Hoffman, 1999). When researching these issues, the question arises whether or not security and privacy should be considered together or whether these two issues in themselves are umbrella terms comprised of many facets.

This paper seeks to establish the importance of security and privacy to purchasing intent in the online environment. The discussion leads to the development of a theoretical model in which research constructs are identified and various propositions are formulated for empirical testing. The objective of the study is to identify issues regarding security and privacy that, if properly managed, will impact positively on online consumers' purchasing intent.

Trust in the Online Environment

Generally the trust relationship between online consumers and e-retailers presents as a new area for research. While this purchasing medium has been available for almost a decade - since 1992, the advent of the Web – little research has been undertaken to establish the nature and significance of this relationship in affecting the online consumer's purchasing intent. It may be suggested that existing techniques for establishing trust in similar areas like telemarketing and mail order could be used to solve the trust problem in the online environment because they share similar characteristics i.e. the buyer and seller are not in the same physical proximity. However, while some concerns are similar to those in telemarketing and mail ordering, they take on new meanings in the e-environment.

Similarity exist for payments since in telemarketing/mail ordering consumers give their credit card information to someone on the telephone or send it by post. However for the latter, exponential growth occurred. Between 1972 and 1983 mail ordering grew tenfold from $4.5billion to $45billion (Festervand, 1986). This growth suggests a greater acceptance by consumers of the risk over time. This view is supported by Sitkin (1995) who found that risk propensity can change as a result of experience (risk propensity being the current tendency of an individual to take or avoid risks). It can therefore be reasonably argued that should online risks be downscaled over time, the Web should become a serious stakeholder in the multi-trillion dollar global retail economy.

On the other hand, the Web and telemarketing/mail order environments have characteristics that are not shared and subsequently techniques being used by the latter to deal with issues of security and privacy are not transposable to the Web environment. In particular, the Web is an open and largely unregulated environment where opportunities exist for any business or individual to develop a Web presence at a negligible cost that gives them a global audience (McKeown and Watson, 1996). These same opportunities have provided consumers with the necessary grounds to be cautious, and in some cases distrusting, of the Web when considering a purchase.

The development of a conceptual framework for addressing issues of security and privacy provides the basis for improving trust between online consumers and e-retailers. Trust is generally expected between online retailers and consumers. In the brick and mortar environment however, it is generally accepted that retailers don't place as much importance on building trust from consumers particularly when payment is in cash. If items are placed on credit, as is particularly the case on the Web, the level of trust required from the consumer is greater. Furthermore, the trust required by both parties increases substantially because e-retailers and consumers can't experience the same physical proximity as they do in the brick and mortar sense (Hoffman, 1999).

Risk is an essential component of trust; "one must take a risk in order to engage in trusting action" (Mayer et al, 1995, p. 724). Risk-taking takes into account the probability of the occurrence of an event between parties and the difference in the anticipated ratio of what Deutsch (1958) calls 'positive and negative emotional consequences' to the parties. The probability of negative consequences will depend on how risky the situation is and the existence of security measures to minimise the risk of negative events from happening or reduce their impact. However, what level of security is adequate is difficult to establish as organisations and individuals vary considerably in the degree of assurance they require before they will act in a situation that has the potentiality of danger or negative consequences. Axelrod (1984) goes so far as to state that regardless of the environment it is generally accepted that one entity is not responsible for the trust relationship; instead it is a cooperative process.

To facilitate the development of trust it is necessary to overcome consumers' concerns with the security and privacy of their personal details when making a purchase online (Berlin, 2000; McKenzie, 1997; Wang et al, 1998). Specific concerns are twofold: the security and privacy of personal data while it is in *transit* and its *usage and access* once it reaches its destination. Privacy and security can be considered individually as each topic in its fundamental form concerns the protection of financial and/or personal information. However both issues are also interwoven in that the personal data of a consumer needs to be protected for privacy purposes and to keep the financial data in its original form. Treasury (2000) considered privacy as an extension or part of the broader area of security. It is helpful to consider the interrelationships amongst these issues graphically as shown in Figure 1.

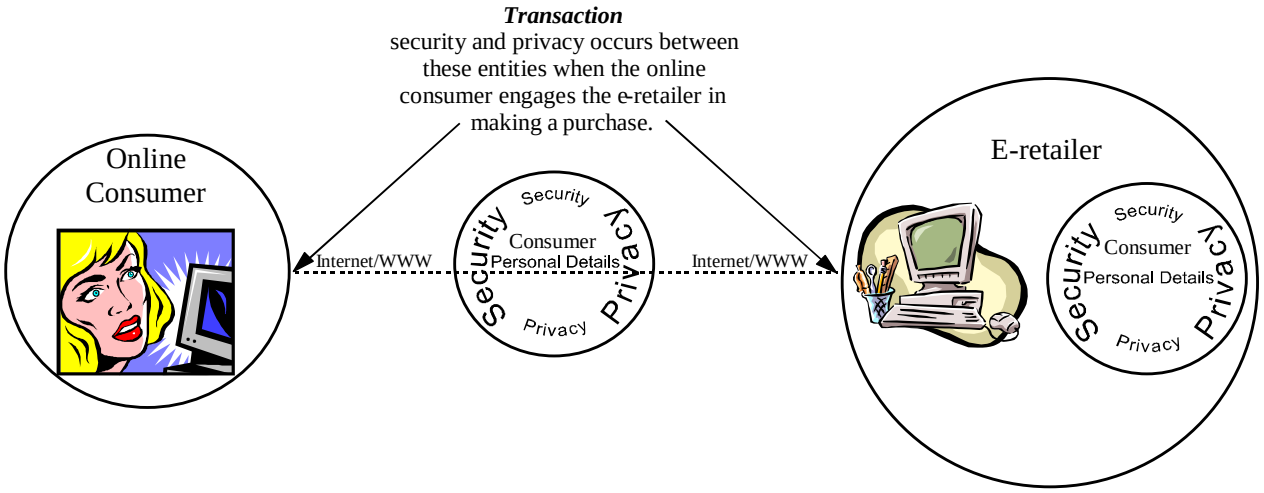

Figure 1: The Relationship between Security and Privacy in an Online Environment

Online Security

The concern consumers have regarding the security of online payment systems is cited by Treasury (2000), Berlin (2000) and George (1999) as a key reason for consumers not engaging in online purchasing and generally being distrusting of e-retailing. This is a frustrating situation for e-retailers given that the security of online payment systems can be better than brick and mortar credit card payment systems (a matter discussed in greater detail later in this paper). This begs the question, 'why are consumers concerned about online security given the Web environment can provide more secure transactions?' Consumers' security concerns relate principally to the protection of personal information contained in online credit card purchasing details (Archetype/Sapient, 1999; Auger, 1997; Hoffman, 1999; Jarvenpaa and

Todd, 1997a). It seems that online consumers are not well informed about the adequacy of security in relation to online credit card usage relative to comparable offline transactions.

Consumers appear to be specifically concerned with the security of their personal information when it is in transit and with how the information is protected after it reaches its destination. These issues have been dealt with in practical terms by employing encryption technology. The encryption technology used to protect consumers' personal information when making a purchase online is safer than the regular offline credit card system (Jarvenpaa and Todd, 1997a). Further, supporting this, Stewart (1995) cited in Auger (1997) states, "International versions of encryption schemes require a prohibitively massive amount of computing power to crack". The safety of the Web for purchasing is further supported by McKeown and Watson (1996) who argue that giving your credit card to a waiter or using it over the phone is riskier than using it on the Web as the details can be easily written down. This is supported by Forrester cited in Auger (1997) who states the Internet commercial fraud rate is $1 per $1000 in comparison to credit card fraud at $1.41 per $1000, cellular phone at $19.83 per $1000 and toll call fraud at $16 per $1000. These figures highlight the relatively high safety of online security in comparison to other forms of sale mediums.

Since encryption technology can protect consumers' personal details and given that consumers' security fears are still prevalent, the question begging is, 'what is it about online security that concerns consumers'? The question may be answered in part by McKenzie (1997) who suggested that the popular press is partly responsible for online consumer security fears through the release of media reports about online credit card theft, which are exaggerated. It seems that greater effort education of online consumers needs to occur for them to recognise where the risks actually lie (Treasury, 2000). To this end Archetype/Sapient (1999) explored the benefit of web sites using symbols (like Verisign) that convey a sense of security and trust. They found however that these only conveyed trust and security where online consumers were knowledgeable about the symbols.

Current research suggests that the security problem is evolving from concerns regarding the *transmission* of personal data to the e-retailers *storage* and *usage* of consumer personal data (Treasury, 2000). Organisations and specifically e-retailers need to protect data while it is in transit and being stored (McKeown and Watson, 1996). This isn't new to larger organisations that are accustomed to protecting information although new issues may present themselves in the Web environment. Large organisations, however, are in a good position to deal with them because of their expertise and experience in this area. This may however present a potential problem from small and medium sized enterprises. The issue for online consumers is that they are unaware of the internal protection mechanisms and policies that organisations may use because the organisation might not display these details on their Web site.

Although the majority of research indicates consumers don't trust online security (Archetype/Sapient, 1999; Jarvenpaa et al, 2000; Berlin, 2000), other research like Lyons (1995) and Kennedy and Dietsch (1995) cited in Auger (1997) has indicated some success by private networks like Compuserve and America Online as they have experienced more transactions than regular web-based sites. This suggested that consumers feel security is greater within private networks than in the public web-based networks resulting in a higher rate of online consumer spending. The importance of private networks however may not be high because the majority of the population only has access to the publicly-based Web environment.

Online Privacy

Online privacy concerns, similar to security concerns, have the potential to reduce the intent of a consumer making an online purchase (Treasury, 2000; George, 1999; Hoffman, 1999; Wang et al, 1998; McKenzie, 1997). Privacy is a vast area, however this paper considers only the issues of privacy that directly affect the transaction and storage of consumer personal information. Once consumer personal information is received by the e-retailer, the concern is the information may be sold to or swapped with

other organisations by e-retailers (McKenzie, 1997; Wang et al, 1998). Furthermore, improper storage may result in consumer data being readily accessed from inside and outside the organisation, via computer networks such as the Web (George, 1999; Wang et al, 1998).

The importance of privacy in the literature is apparent in the strong meanings applied to it. Katsh (1994) cited in Gattiker (1997) defined it as, "the right to be left alone", and "the right to control information about oneself". This presents an immediate dilemma for online consumers when sending their personal details to an e-retailer. The consumer, although unwillingly, is potentially relinquishing control and responsibility for the control of their information to an unknown entity.

Although privacy statements may say the information won't be given to other organizations there appears to be no system or structure in place to stop e-retailers selling or swapping consumer details with other organisations. Consumers would be unaware of such an occurrence unless they began receiving unsolicited junk mail. Even then, the consumer wouldn't know exactly how the organisation sending the junk mail received their personal details. Therefore, the value and usefulness of displaying privacy statements on web sites, or more specifically, the confidence consumers have in the presence of these privacy statements needs to be determined.

Consumers can view organisations' privacy statements as the organisation's moral responsibility to their consumers. However, even if this is the case, how reliable are privacy statements? Gattiker (1997) discusses morals as a component of privacy in that they offer constraints to individuals when interacting with society. Application of Gattiker's (1997) morality concept to e-retailers would, in a perfect world, mean e-retailers would consider the sale of consumer transaction information to other organizations as an unacceptable practice. However given the financial gain from selling consumer transaction information (Wang et al, 1998) it may be difficult to convince consumers that their personal details are safe, irrespective of assurances offered by e-retailers.

Various approaches have and are being used by e-retailers to convey privacy policies to online consumers. One approach available to e-retailers is the use of TRUSTe (www.truste.org). If the e-retailer is involved with this organisation it conveys a message to the consumer that the e-retailer's privacy practices can be trusted. Wang et al (1998, p.6) say, "TRUSTe can review and audit sites to ensure they correctly disclose their information practices". However, Archetype/Sapient (1999), as mentioned previously, found that sites displaying security symbols like VERISIGN only benefited when the consumer understood the symbol's meaning. The same may well apply for TRUSTe.

Another approach is the use of 'Digital Cash' which goes by names like Cyber Cash and Internet Cash. This approach aims to enable users to remain anonymous when making transactions (Wang et al, 1998), thereby promoting privacy. The benefit of this option however does not appear to have encouraged online buying given the small total of online users that actually make an online purchase (Skinner, November 1999; February 2000; November 2000).

Modelling Online Security and Privacy Issues

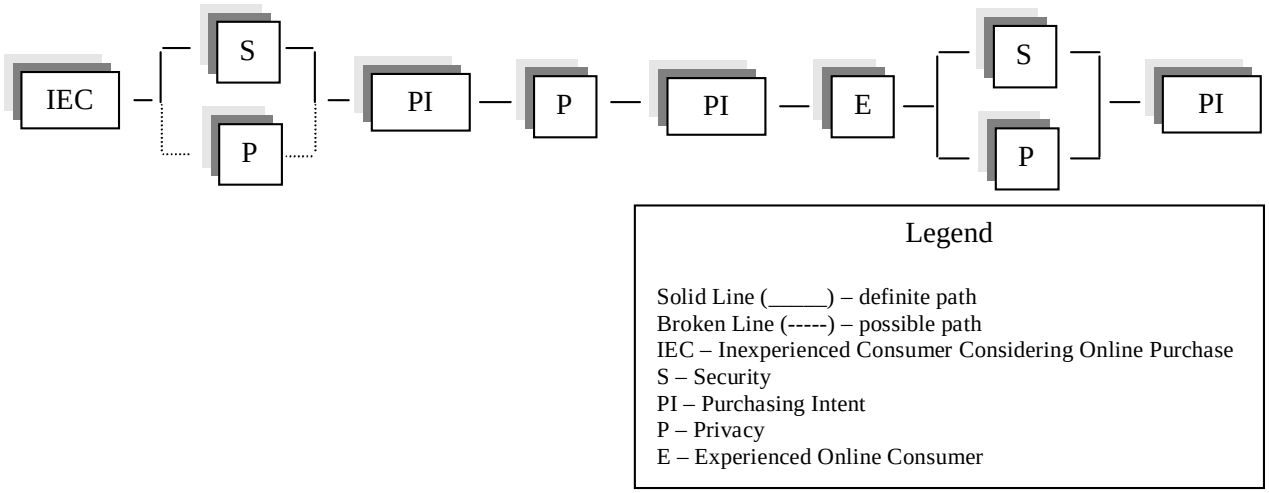

Figure 2: Effect of Experience with Security and Privacy on Purchasing Intent of Online Consumers

Solid Line (_____) – definite path , Broken Line (-----) – possible path, IEC – Inexperienced Consumer Considering Online Purchase

S – Security, PI – Purchasing Intent, P – Privacy, E – Experienced Online Consumer

The literature review established various aspects about consumer concerns regarding security and privacy. Little empirical evidence exists however to establish exactly how important these consumer concerns are in the formulation of a consumer's purchasing intent. Online security and privacy's role in a consumer's purchasing decision needs to be understood to determine whether or not they are significant considerations in the purchasing decision, hence important issues to be addressed by e-retailers. For example, if the consumer's first thought in making a purchasing decision is 'privacy', then having a great product or a well-designed site may count for little if the consumer lacks confidence in the privacy of their personal information. Figure 2 shows how security and privacy may impact on purchasing intent of inexperienced and experienced online consumers.

Figure 2 is based on the application of Sitkin's (1995) risk propensity theory to online consumer purchasing intent. Initially consumers entering into online purchasing are more concerned, if not solely concerned, with online security although some consumers consider privacy at this point. Purchasing intent is affected. After the consumer becomes comfortable with online security, they then consider privacy, perhaps in more detail if they have considered it already. Purchasing intent will change again and the user becomes an experienced user who considers both security and privacy simultaneously in determining his/her purchasing intent.

Figure 2 shows that online consumers, depending on experience, may have differing requirements, although ultimately security and privacy will play an equal/combined role in determining purchasing intent. As indicated by the model, education about online security and privacy needs to occur. The optimum timing for this education is at the point where the adequacy of online security and privacy is being considered as it will be of greatest relevance to the consumer. This timing will ensure a greater propensity for the consumer to be receptive to the information being communicated as it will coincide with the information gathering and evaluation stages of the purchase decision making process. To this end Archetype/Sapient (1999) explored the benefit of web sites using symbols (like Verisign) that convey security and trust. Under this so-called identification-based trust, trading partners establish common desires and intentions based on empathy and common values (Lewicki and Bunker, 1996) identified by symbols and statements. There is an emotional connection between them and one can act as an 'agent' for the other. This leads to the following model which illustrates how the utilisation of appropriate symbols and statements can redress security and privacy concerns of online consumers.

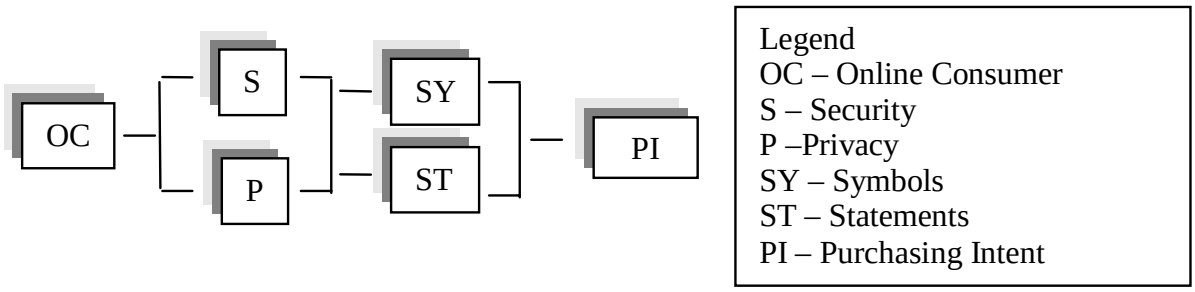

Figure 3: The Role of Security and Privacy Symbols and Statements in Purchasing Intent

Figure 3 shows a model for online security and privacy in which online consumers purchasing intent is affected equally/simultaneously by the security and privacy implications and is subsequently influenced by the display of security and privacy symbols and security and privacy statements on the web site.

Research Propositions

This preliminary research provided insight into the role of security and privacy in determining intent to purchase in the e-tailing environment and the potential effects of consumer experience and security and privacy symbols/statements on this intent. The reviewed literature enabled the development of a theoretical model aimed at providing a statement of the relationships between units observed or approximated and answers the questions of *how, when* and *why* (Bacharach, 1989).

Theory is useful in that it can both explain and predict what is and will be happening to purchasing intent. A theory is a collection of constructs which are related to each other by research propositions. Based on the foregoing discussions, the following propositions have been identified for testing in future research.

Proposition 1: From a purchasing intent perspective, inexperienced online consumers treat online security and online privacy as separate issues by considering security before privacy.

As stated by Treasury (2000), security is the broad umbrella and includes privacy considerations. Furthermore, security in the online environment has so far received greater attention than privacy. For these reasons it is reasonable to argue that consumers new to the online environment want to have their security concerns satisfied before they consider privacy concerns.

Proposition 2: From a purchasing intent perspective, experienced online consumers treat privacy and security with equal importance and simultaneously, i.e. security does not come before privacy.

Those consumers that have used the online environment more regularly and over a longer period thereby having undergone learning, would have become aware of the shift from security to privacy. For example, in Australia, the Privacy Act has just been released under which privacy obligations have been extended from the government sector to the private sector. This has attracted much attention in the press. It is therefore reasonable to assume that experienced online users would consider privacy and security aspects of equal importance and simultaneously in arriving at a purchasing decision.

Proposition 3: The display of security and privacy symbols and statements increases the intent to purchase for both inexperienced and experienced online consumers.

Symbols and statements can provide powerful assurances provided they are perceived to be independent and reputable and are recognisable by consumers. A good example is the service provided by WebTrust which was set up by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants with the aim of providing third party assurance for customers and businesses using the Web. WebTrust provides the framework and the methodology to assure online consumers of the integrity and security of the site, as well as the disclosures of business practices of a firm doing business on the

Web. The WebTrust seal on a Web site provides assurance in three areas (Muysken, 1998): business practices, transaction integrity and information protection.

Proposition 4: The more knowledgeable an online consumer becomes about security and privacy the more knowledgeable an online consumer becomes about the concerns relating to security and privacy.

As the volume of e-retailing increases, consumers will become more knowledgeable about security and privacy. This increased understanding is brought about by education, media and even by retailers themselves in the way they seek to assure consumers. This should enable consumers to judge how valid their concerns are. For example, they may realise that encryption of data provides a high degree of security over transactions and personal data.

Proposition 5: The more knowledgeable an online consumer becomes about security and privacy the greater is the intent to purchase.

With increased confidence that e-retailers are meeting security and privacy concerns, consumers will take advantage of the benefits that online purchasing provides. These benefits are well known and include convenience for grocery purchasers shopping from home and better selection of goods because of the variety of goods from which to choose.

Initially, a survey approach is the best way to test this model because a survey will produce quantitative data, which is lacking in this area. In selecting a consumer sample, considerations need to be given to the type of participant. For example should only existing online consumers be tested? Or should only non-online consumers be tested or both? This dilemma arises because a large percentage of the population don't currently purchase online but is expected do so in future. The survey should include a diversity of online consumers by selecting subjects from various demographics and backgrounds such as age, gender, online experience and so forth.

Conclusion

Security and privacy are evolving issues both requiring ongoing research. It can however be postulated that consumers will, albeit slowly, come to terms with online security and privacy, possibly due to different reasons. For example, the use of cryptography, symbols and statements may meet their concerns head on. Furthermore, as Sitkin (1995) argues, risk propensity (i.e. an individual's tendency to take risk) increases with experience. In future online consumers may be more aware of risks and, if avoidance strategies exist, will be aware of them and use them.

On the other hand, McKenzie (1997) argued that although security mechanisms may be adequate to protect consumer information, this isn't enough to assure consumers as they are equally concerned about the legitimacy of the business in which the personal information is being sent to. In this regard, it is important to point out that security and privacy considerations won't by itself be an ultimate solution to the advancement of e-retailing because there are other areas to consider like branding and business reputation.

The significance of this research rests in it being the initial stage in identifying how security and privacy concerns of online consumers impact on purchasing intent with a view to developing a broad based framework for redressing these concerns. Such a framework would present to e-retailers measures that can be adopted to build trust of online consumers thereby fostering the growth of online purchasing.

References

Archetype/Sapient. (1999), *eCommerce Trust Study*, Cheskin Research and Studio, January.

Auger, P. (1997), "Factors affecting the adoption of an internet based sales presence for small business" *The Information Society*, 13, 55-74.

Axelrod, R. (1984), *The evolution of co-operation*, Basic Books, New York.

Bacharach S.B. (1989), "Organizational Theories: Some Criteria for Evaluation", *Academy of Management Review*, 14(4), 496-515.

Berlin, M. (2000), "Global Online Retailing", *Ernest and Young*, 1(2), 1-165.

Deutsch M. (1958), "Trust and Suspicion", *Conflict Resolution*, 2(4), 265-279.

Doney, P. and Cannon J.P. (1997), "An Examination of the Nature of Trust in Buyer-Seller Relationships", *Journal of Marketing* 61, 35-51.

Festervand, T. (1986), "Influence of catalogue vs store shopping and prior satisfaction", *Academy of Marketing Science*, 14(4), 28-36.

Fink D. (2000), "Developing Trust for E-Commerce" in Janczewski L. (ed) *Internet and Intranet Security Management: Risks and Solutions*, Idea Group Publishing, London.

Gattiker, U. (1997), "The Internet Community and Ethics", *Proceedings of the Annual Meeting - Association of Administrative Science*s, Denmark.

George, J. (1999), "The Effects of Internet Experience and Attitudes Toward Privacy and Security on Internet Purchasing", 1053-1058.

Hoffman, D. (1999), "Building Consumer Trust Online", *Communications for the ACM*, 42(4), 80-85.

Jarvenpaa, S.and Todd P.A. (1997a), "Consumer reactions to electronic shopping on the World Wide Web", *International Journal of Electronic Commerce*, 1(2), 59-88.

Jarvenpaa, S.and Todd, P.A. (1997b), "Is there a future for e-retailing on the Internet?", *Electronic Marketing and the Consumer*, 139-154.

Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000), "Consumer Trust in an Internet Store", *Information Technology and Management*, 1, 45-71.

Katsh (1994), "Privacy and new information technologies", *Proceedings of the 18th Regional Conference on the History and Philosophy of Science*, University of Colorado, Boulder, 1994.

McKenzie, M. (1997), "Trust - the big issue in Internet marketing", *Marketing*, March, 37-40.

McKeown, P. and Watson, R. (1996), *Metamorphis: A Guide to the WWW and Electronic Commerce*.

Kennedy W. and Dietsch, Jr (1995), *Making Money Online*.

Lewicki R.J. and Bunker B.B. (1996) "Developing and Maintaining Trust in Work Relationships" in Kramer R.M. and Tyler T.R. (Eds.) *Trust in Organizations - Frontiers of Theory and Research*, Sage Publications, London.

Lyons D. (1995), "Case study sweet smell of success: 1-800-Flowers on the Iway", *Infoworld*, 17(25), 93.

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

Sitkin, S. (1995), "Determinants of Risky Decision-making behaviour", *Academy of Management Journal*, 1573-1592.

Skinner, T. (November, 1999), "Use of the Internet by Householders", *Australian Bureau of Statistics*.

Skinner, T. (February, 2000), "Use of the Internet by Householders", *Australian Bureau of Statistics*.

Skinner, T. (December, 2000), "Use of the Internet by Householders", *Australian Bureau of Statistics*.

Stewart L. (1995), "Recent Internet Security Problems", *Open Market Press Release*, October 5, available at http://www.openmarket.com.

Treasury (2000), "Drivers and Inhibitors to Consumer Uptake of Electronic Commerce", *Australian Treasury - Federal Government*.

Wang, H., Lee, M. and Wang C. (1998), "Consumer Privacy Concerns About Internet Marketing", *Communications for the ACM*, March, 63-70.

Biographies

Dieter Fink is an Associate Professor and **Robyn Morris** a Senior Lecture at Edith Cowan University in Perth, Western Australia. Both focus their research on SMEs especially how the Internet has affected them. **Michael Milloy** is a PhD student at the same university who is researching the adoption of the Internet by small and medium sized wine retailers.