Threats to On-line Privacy

Prathiba Mahanamahewa

Attorney-at-Law
mahanamahewa@yahoo.com

Abstract - *The further development of the World Wide Web is threatened by the lack of online privacy and efforts to destroy net neutrality, says the father of the Web, Sir Tim Berners-Lee. He believed the world had to think about privacy "from a completely different point of view" in future, because the threat to personal privacy will be so great. Consumer awareness about privacy is increasing, particularly among Internet users. Sooner or later, if it is not happening, consumers will demand that their privacy be respected by business. This may require some modification to business practices and customer service and may involve costs not previously incurred. Even American big business has accepted that privacy is a concern, which must be addressed. All the public surveys conducted by and for big business in America showed a lack of confidence that consumer's personal information would be protected if they entered into transactions on the Internet. Privacy concerns have been clearly identified as a barrier to the development of e-business. This paper discusses the barriers to effective E-business and the legal protection for data Privacy in Sri Lanka.*

Keywords: Privacy, E-Business, Surveillance

I. DEFINITION OF PRIVACY

Nonetheless an agreed definition of Privacy remains elusive. Ever since the seminal article of Warren and Brandies (1890 cited Rowland and Macdonald 2000) at the end of the 19th century academic writers have been analysing the multi-faceted concept of privacy. Westin (1967 cited Rowland and Macdonald 2000) suggested that 'privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others', a definition based on the right of self determination that maybe placed at particular risk by the practice of data matching. This notion was supported by Miller (1971) in the specific context of this technology, who considered privacy as 'the individuals ability to control the circulation of information relating to him' Gavison (1980 cited Rowland and Macdonald 2000) on the other hand, is critical of the ability to control personal information as being a determinant of the definition of privacy precisely because a dependence on subjective choice makes both a realization of the scope of the concept and the provision of legal protection problematic. In the quest for a more neutral approach, Gavison attempts to deconstruct privacy into three components: secrecy, anonymity and solitude. The differential difficulties are exacerbated by the fact that whether or not privacy is considered to have been invaded is a very subjective issue, which will hinge not only on the view of the person whose privacy is being invaded, but also on who is the invader and what information they are uncovering.

The link between data protection and privacy has increasingly been recognized in the UK as well as internationally. In 1994, the Data protection registrar (cited Rowland and Macdonald 1997) stated in his final report 'data protection legislation is about the protection of individuals rather than the regulation of the industry' (Tenth annual Report of the Data protection registrar, 1994) the judgment given in *British Gas Trading Ltd. V. Data Protection Registrar* gives a increased recognition to the concept; 'an underlying purpose of the data protection principals is to protect privacy with respect to the processing of personal data.'

II. DATA PROTECTION AND PRIVACY

The relationship between the terms 'data protection' and 'data privacy' have not been easy to reconcile. Data protection is often viewed as a technical term relating to specific information management practices (Rowland and Macdonald 2000) this is a preferred stance for those who would see data protection as a primary aspect of business regulation. In contrast Privacy is more likely to be considered as a fundamental human

right or convenor of constitutions. It is however possible to discuss privacy issues in the terminology of risk and risk assessment, concepts which are more familiar in the business environment. Three risk factors can be identified which could be considered to be elements of privacy (Rowland and Macdonald 2000) the first of these risks would be the risk of injustice due to significant inaccuracy in personal data. The second risk is to one potential control over the collection of personal information as a result of excessive and unjustified surveillance, collection of data without the data subjects consent and also the prohibition or active discouragement of that means to remedy these risks (Such as the use of encryption and anonymising software). Finally there is a risk to dignity as a result of exposure and embarrassment due to an absence of transparency in information procedures, physical intrusion into private spacers, unnecessary identification or absence of anonymity, or unjustified disclosure of personal information without consent.

III. LEGAL PROTECTION OF PRIVACY

A. International Conventions

Regulators and legislators have addressed the controversial online privacy issue quite differently across the world. The USA, the world's biggest financial and Internet market, has not yet adopted a national, standard-setting privacy law akin to the European Union's Data Protection Directive. US privacy statutes have primarily focused on protecting consumers' financial data, health information, and their children's personal information (Rombel, 2001). In many situations, entire industries in the USA are failing to comply with laws regarding privacy policies. According to a recent survey by Price waterhouse Cooper's Better Web program, (cited Nakra, 2001) two-thirds of all US banks' online privacy notices do not meet the requirements of the Gramm-Leach-Bliley Act (US) because they do not disclose the personal information that they collect from consumers. The European Union (EU) has already passed tough privacy measures too tough, say some multinational businesses. A warning shot has already sounded from Europe, as the European Union has criticized the largely self-regulatory stance championed by the USA. The European Union's privacy directive compels companies to disclose to individuals, upon request, the information being stored about them. The European Union's controversial Safe Harbor data-sharing agreement with the US Department of Commerce went into effect in year 2000 (cited Nakra 2001) in November. Under the accord, US companies have to agree to the European Union's more stringent privacy requirements or risk losing remote access to data about their European clients, employees, and business partners. By entering the Safe Harbor agreement, US companies will in effect be promising their European customers more privacy protection than they give their domestic clients (Rombel, 2001).

B. Regional Conventions

There are currently no regional agreements in the SAARC region or with any other SAARC country dealing with data protection legislation. However a reference to e-commerce is made in the Economic Partnership Agreement of India and Sri Lanka; joint study report (2003), the report mentions that the two countries markets must facilitate E-commerce, however no mention of data privacy methods or cross border data transfer protocols.

III. DATA PROTECTION LEGISLATIONS IN SRI LANKA

There are currently no legal or legislative documents that support data privacy in Sri Lanka, thus a key purpose of this research is to provide recommendations as to any progressive privacy legislation in Srilanka.

The lack of a framework on data protection prevents the free flow of personal data and information from the European Union (EU) for data centre and call centre operations in Sri Lanka. Therefore, the Government recognizing the need to have legislative measures or other measures such as the adoption of a "Codes of Practice" embodying principles that would ensure protection of personal information to benefit from Call centre / Data Centre operations and BPO operations. In this context ICTA has been directed finalise appropriate Codes of practice embodying Data Protection principles and measures, in consultation with the private sector. ICTA is taking into consideration the Private Sector Model Data protection Code adopted by Singapore in 2002.

V. PRIVACY POLICIES

There is an agreement at least in the industrialized world that privacy policies are essential in an e-

commerce environment regardless of country-imposed legislation. The IBM Multi-National Consumer Privacy Study found that nearly half of the respondents in the USA and the UK, and one quarter of the German respondents look for a privacy statement on Web sites. Sixty-three percent of the respondents who use the Internet have refused to give information to Web sites when they perceive that the information will be compromised when privacy policies are unclear (Pescovitz, 2000). Three years ago, the FTC startled the Internet business community by undertaking a sweep of Web sites and finding that only 14 percent posted policies that explained what they do with the personal information they gather. An industry-sponsored study found that 66 percent now have such policies (Wasserman, 2000). Privacy policies must begin with "fair information practices" with an "opt out" option, whereby the customer or visitor may forbid usage of their personally identifiable data and give them a right to review and correct their data. Consumers need unambiguous, plain-English statements explaining what information is collected, for what purpose it is used, and with whom it is shared. The disclosures should also provide a simple way for consumers to opt not to have their personal data used for marketing purposes.

VI. THE RELATIONSHIP BETWEEN PERCEIVED PRIVACY AND SECURITY ON A WEB SITE

The analysis conducted above shows that although the privacy and security variables in internet relationships are related, they have particular characteristics that enable us to establish a clear distinction between them. Specifically, privacy is linked to a set of legal requirements and good practices with regard to the handling of personal data, such as the need to inform the consumer at the time of accepting the contract what data are going to be collected and how they will be used. Security refers to the technical guarantees that ensure that the legal requirements and good practices with regard to privacy will be effectively met. For example, the company may promise that the data will not be given to third parties without the consumer's consent. Yet hackers might get hold of the data and hand them over to malefactors. This invasion of privacy can only be prevented by the use of suitable security measures. The close relationship between the concepts of privacy and security may be seen in three clearly distinct areas. First, it should be emphasized that there is a close relationship between the two concepts in the mind of consumers. Indeed, at times consumers do not make a clear distinction as to where one concept ends and the other begins, and they may well confuse them. Usually, this distinction is not particularly relevant for consumers, since all they want is that their privacy be respected, either through the law, good practices, secure systems or a combination of the three. Second, it is worth pointing out that companies tend to handle both concepts jointly. In fact, the idea is widely spread in the business world that protection of privacy is an element that depends not only on the following of a series of behaviour guidelines or the law; it also depends on the reliability of information systems (Lyman, 2003). Third, we see that public bodies view both concepts as running side by side. Thus, legislative measures include, along with those of a procedural nature regarding the collection, use and transfer of private data, others of a purely technical nature (e.g. Directive 2002/58/EC of the European Parliament and of the Council, of 12th June 2002 (European Commission, 2002), concerning the processing of personal data and the protection of privacy in the electronic communications sector).

VII. RISK

Risk exists when there is a less than 100 per cent probability that things will turn out as expected. As Bauer (1967, p. 24) succinctly puts it:

"Consumer behaviour involves risk in the sense that any action of a consumer will produce consequences which he cannot anticipate with anything approximating certainty, and some of which are likely to be unpleasant."

Hence, risk implies that there is some degree of uncertainty about the outcome of an action which caries the possibility of physical harm or some other damage. The perception of riskiness may vary from person to person and from product to product, or service to service (Stone and Gronhaug, 1993): in short, a very personal thing, related to specific circumstances.

Consumers tend to use intuitive judgement to decide whether or not something is risky, which may be affected by previous experiences, the level of involvement, or the price of the purchase. Risk

has a moderating effect on consumers because they are often more inclined to try to avoid a mistake rather than benefit from utility in their buying decisions. For this reason, shoppers may "pre-select" brands for consideration to avoid risk (Mitchell, 1999).

A. Risk Online

Previous research has identified that customers can perceive risks in many purchase situations. Mail order has been considered to be more risky than in-store purchasing (Akaah and Korganonkar, 1988) and users of the internet encounter more risks than they do in face-to-face transactions (Riegelsberger et al., 2003). Not all users understand or perceive these risks, or wish to contemplate them. Some consumers may consider that just working with computers could be risky, let alone using them to make purchases. Online transactions involve a lack of control on the part of customers with anonymous trading partners and, consequently, the potential for opportunism. It may be that some risks are heightened or unique to the online purchasing environment. If customers think that they may be taken advantage of, they may not engage in online transactions at all. A typical online transaction necessitates giving the vendor access to personal data, such as address, telephone number a financial details (Tsiames and Siomkos, 2003). Such access may be the source of worry (or perceived risk) for some consumers, especially if they are concerned about fraud or losing money. This concern was highlighted as one of the dimensions of internet quality by Madu and Madu (2002). Customer concerns may also include worry about the honesty of the sales proposition, and immodest claims about products when customers are unable to physically check the quality of those products (Chaudhuri and Holbrook, 2001) could be visited, worries may be exacerbated because customers cannot rely on visual and physical clues to reassure themselves of the bona fides of the selling organisation. Such lack of reassurance may result in transactions being regarded as risky. Customers may also be anxious about bombardment with unwanted messages and service guarantees (Urban et al., 2000). Without confidence in these areas, any exchange between provider and customer may be limited (Subirana and Cavajal, 2000). Tan (1999) suggests that less risk-averse customers are more likely to use internet shopping services. Nevertheless, internet marketers must be able, long-term, to convince customers to shop online if they are to maximise the effectiveness of online channels.

B. Trust

Trust is a complex state that comes about because individuals do not know what the motives and intentions of others are (Kramer, 1999). Thus, trust is an expectation about others' behaviour within the society in which they live, or by which they are ruled (Barber, 1983), and so involves cultural mores as well as emotionally and socially based responses. Trust has been defined by Riegelsberger et al. (2003, p. 768) as:

". . . a device to reduce complexity, a shortcut to avoid complex decision processes when facing decisions that carry risk."

Thus, it is an especially important factor when there is some kind of choice to be made. Trust can be bestowed on a person, an object (product), an organisation (a business), an institution (the government) or a role (a professional of some kind). Trust may be acquired by a rational process based on what we know of the other party, and also the incentive of that other party to honour the trust bestowed upon him, her or it (Hardin, 1992). Alternatively, it can be an emotional and social response to others or to society as a whole (Kramer, 1999). People who consider themselves to be unlucky in life, for example, may be less likely to be trusting than others who have not had such bad experiences. If a person is "disposed to trust" he or she is less likely to see the potential for risk, as a consequence of assuming that people are honourable and will do what they say they will. A person's propensity to trust or disposition to trust has its roots in personality psychology (Grabner-Krauter and Kaluscha, 2003). It is for this reason that previous experience may be a mitigating factor in developing trust on a rational basis (Rotter, 1971). Trust may be easy to acquire but, if abused, can be easy to erode or destroy. Boyle and Bonacich (1970) suggest that individuals continuously update their expectations about trustworthy behaviour based on their experiences with individuals in whom they have placed their trust.

C. Trust Online

Online marketing transactions necessitate online customer trust (McCole and Palmer, 2001). According to Egger (2006), the number of people

purchasing online has grown at a slower rate than those who use the internet. Sufficient trust needs to exist to place an order online and, perhaps, for the customer to submit his or her financial information and other personal data in undertaking other financial transactions, such as online banking. Corritore et al. (2003, p. 740) define trust as:

". . . an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited."

Stell and Paden (2002) suggest that inexperience may lead to concern about, or avoidance of, using the internet and hence to a lack of trust. Houston (2001) suggests that organisations doing business online must forge trust swiftly in order to succeed. This opinion conflicts to some extent with the view of Ennew (2003, p. 16) who says:

"The continuing uncertainty and scepticism of consumers in regard to the internet means that acquiring their trust will be an incremental process . . . For the majority of internet users, trust in transactions online will be built up experientially over time."

Therefore, organisations utilising the internet should not hope for results too soon and abandon their attempts to woo the customers to purchasing online. Trust may be built incrementally following experience online, and customers may build trust by starting with small purchases and building up to bigger and more expensive ones as their trust in the medium or the organisation (or both) increases. Dimensions of trust online, as outlined by Camp (2001), include security, privacy and reliability.

In order to engage in online shopping, a customer must have trust in the mechanism itself (Lee and Turban, 2001). Whilst this may have been particularly important in the early stages of internet commerce, with more and more transactions taking place online, less concern needs to be focused on the mechanism today. There is an increasing need for customers to feel sufficient trust in the supplier, rather than the channel that the supplier has chosen to use.

VIII. CONSUMER TRUST IN A WEBSITE

The constant development of relationships over the internet is significantly affecting most commercial sectors (Gunasekaran and Love, 1999). However, this influence has not been translated into high sales figures via the internet since there is a lack of trust that means that consumers are reluctant to adopt e-commerce (Gefen, 2000). This distrust is a consequence of the particular features of the internet when set against transactions conducted via traditional channels (Yousafzai et al., 2003). Thus, when a consumer conducts a transaction with an online store that is characterized to be operating in an uncertain environment (Fung and Lee, 1999) such as the internet, the consumer is less likely to trust that everything about his transaction is assured and normal as compared to his transactions with an offline store.

IX. CONCLUSION

Unlike the European Union, the United States traditionally has adopted a different approach to data protection. The European Union embraces privacy as a fundamental right and thus considers comprehensive legislation as the most appropriate means to protect personal information. Such an approach requires the creation of government data protection agency and approval before the processing of persona data. By contrast, many Americans believe in the free market and are constantly suspicious of government intrusions. Therefore U.S approach relies on a mix of legislation, administrative regulation and industry self-regulation through code of conducts developed by industries as an alternative to government regulation. In my opinion, I firmly believe that, If Sri Lanka really willing to accept the benefits of the globalization and absorbing into the International trade still we are not late therefore any proposed data protection law should be definitely based on European model of the EU directive and the data privacy principles because U.S data protection model is an ad hoc one and therefore no independent authority to protect and implement data users rights. Finally we should recognize data privacy as one of our fundamental right and we need more laws in this emerging new area to attract more E-business from the western world.

REFERENCES

AKAAH, I.P. AND KORGANONKAR, M.G. (1988), "A cojoint investigation of the relative importance of risk relievers in direct marketing", *Journal of Advertising Research*, Vol. 13, pp. 36-47.

ALADWANI, A.M. (2001), "Online banking: a field study of drivers, development challenges and expectations", *International Journal of Information Management*, Vol. 21, pp. 213-25.

ALJIFRI H.A., PONS A., COLLINS D., (2003), "Global E-commerce: a framework for understanding and overcoming the trust barrier", Information Management & computer security, 11/3, pp130-138

ATTARAN M., VANLAAR I., (1999), "Privacy and security on the Internet: how to secure your personal information and company data", Information Management & Computer Security 7/5 pp241-246

BAINBRIDGE D., (2000), Introduction to computer Law, 4th Edition, Pearson Education Limited, Harrow, England

BARBER, B. (1983), The Logic and Limits of Trust, J.J. Rutgers University Press, New Brunswick.

BAUER, R.A. (1967), "Consumer behaviour as risk taking", in Cox, D.F. (Ed.), Risk Taking and Information Handling in Consumer Behaviour, Division of Research, Graduate School of Business Administration, Harvard University, Boston, MA, pp. 23-33.

BHATNAGAR, A, MISRA, S., AND RAO, H. R. (2000), Online risk, convenience, and Internet shopping behavior,. Communications of the ACM (43:11), pp. 98-105.s

BORCHERS, A. (2001), Trust in Internet shopping: A test of a measurement instrument,. Proceedings of the 7th Americas Conference on Information Systems, pp. 799-803

BOTT F., *et al*, Professional issues in software engineering, 3rd edition, Taylor and Francis, London

BOYLE, R. AND BONACICH, P. (1970), "The development of trust and mistrust in mixed-motives games", Sociometry, Vol. 33, pp. 123-39.

BRAMALL, C., SCHOEFER, K. AND MCKECHNIE, S. (2004), "The determinants and consequences of consumer trust in e-retailing: a conceptual framework", *Irish Marketing Review*, Vol. 17 Nos 1/2, pp. 13-22.

BRINSON J., ABRAMS B.D., ABRAMS D.D., MASEK J., MC DUNN R., WHITE B., (2001), Analysing E-commerce and Internet law, Pretence Hall Inc., Upper Saddle River, United States of America.

CAMP, L.J. (2001), Trust and Risk in Internet Commerce, MIT Press, Cambridge, MA.

CHAUDHURI, A. AND HOLBROOK, M.B. (2001), "The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty", *Journal of Marketing*, Vol. 65, pp. 81-93.

CHOU D C., YEN D C., LIN **.,** HONG P., CHENG L., (1999) "Cyberspace security management" *Industrial Management & Data Systems* 99/8 353-361

CONSTANTINIDES E., 2004, "Influencing the online consumer's behavior: the Web experience" Internet Research Volume 14 · Number 2, pp. 111-126

CORRITORE, C.L., KRACHER, B. AND WIEDENBECK, S. (2003), "On-line trust: concepts, evolving themes, a model", *International Journal of Human-Computer Studies*, Vol. 58, pp. 737-58.

CURRAN C.M., RICHARDS I., (2004), "Misplaced Marketing: Public Privacy and Politics", Journal of consumer marketing, Vol 21, No. 1, pp 7-9.

CYBER ATLAS NEWS (1999a), "Consumers to e-tailers: don't kiss and tell", Internet.com Corp, August, p. 16.

CYBER ATLAS NEWS (1999b), "Consumers fear for their online privacy", Internet.com Corp, November, p. 1.

DESAI M.S., RICHARDS T.C., DESAI K.J., (2003) "E-commerce and customer Privacy", *Information management and computer security*, 11/1, pp 19-27

EGGER, A. (2006), "Intangibility and perceived risk in online environments", paper presented at the Academy of Marketing, University of Middlesex, London, July.

ELOVICI Y., GLEZER C., SHAPIRA B., (2005), " Enhancing customer privacy while searching for products and services on the world wide web", Internet Research Vol. 15 No. 4, pp. 378-399

ENNEW, C. (2003), "Just tryin' to keep the customer satisfied? Delivering service through direct and indirect channels", *Interactive Marketing*, Vol. 5 No. 2, pp. 131-43.

EUROPEAN COMMISSION (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, European Commission.

EUROPEAN COMMISSION (2004), Issues relating to Business and Consumer E-commerce, Special Eurobarometer 60.0/ Wave 201, European Opinion Research Group.

FEDERAL TRADE COMMISSION (1998), FTC Releases Report on Consumers' Online Privacy, FTC File No. 954-4807, FTC, press release, June 4.

FEDERAL TRADE COMMISSION (1999), "Self-regulation and privacy online: a report to congress", available at: www.ftc.gov/reports/privacy99/privacy99.pdf

FEDERAL TRADE COMMISSION (2000), "Privacy online: fair information practices in the electronic marketplace; a report to congress", available at: www.ftc.gov/reports/privacy2000/privacy2000.pdf

FITZGERALD, K. (2000), "Poll: consumers sharply divided on privacy issue", Advertising Age, Midwest region ed., Vol. 71 No. 47, November 13 , pp. 80 and 88.

FITZGERALD, K. (2000), "Poll: consumers sharply divided on privacy issue", Advertising Age, Midwest region ed., Vol. 71 No. 47, November 13 , pp. 80 and 88.

FLAVIA´N C., GUINALI´U M., (2006) "Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site", Industrial Management & Data Systems Vol. 106 No. 5, pp. 601-620

FRANZAK F., PITTA D., FRITSCHE S., 2001 "online relationships and consumers right to privacy", Journal of consumer marketing, Journal of consumer marketing, Vol 18, No. 7, pp 631-641

FUNG, R. AND LEE, M. (1999), "EC-trust (trust in electronic commerce): exploring the antecedent factors", paper presented at the Americas Conference on Information Systems.

FURNELL, S.M. AND KARWENI, T. (1999), "Security implications of electronic commerce: a survey of consumers and business", *Electronic Networking Applications and Policy*, Vol. 9 No. 5, pp. 372-82.

GEFEN, D. (2000), "E-commerce: the role of familiarity and trust", OMEGA: The International Journal of Management Science, Vol. 28, pp. 725-37.

GRABNER-KRAUTER, S.G. AND KALUSCHA, E.A. (2003), "Empirical research in on-line trust: a review and critical assessment", *International Journal of Human-Computer Studies*, Vol. 58, pp. 783-812.

GRITZALIS S., 2004, "Enhancing Web privacy and anonymity in the digital era", Information Management & Computer Security, Vol. 12 No. 3, pp. 255-288

HAMMER, B. (2000), "DoubleClick beats a retreat on privacy", The Standard.com, March, p. 6.

HAMMER, B. and Anderson, D. (2000), "DoubleClick strikes back", The Standard.com, March.

HARDIN, R. (1992), Trust, Russell Sage, New York, NY.

HARRIDGE S, (2006), "Can the building of trust overcome consumer perceived risk online?" *Marketing Intelligence & Planning* Vol. 24 No. 7, pp. 746-76

HOUSTON, D.A. (2001), "Trust in the networked economy: doing business on web time", *Business Horizons*, March/April, pp. 38-44.

INTERNET.COM (2000) "Security keeps women from shopping online", Cyber Dialogue's American Internet User Survey (AIUS), December, p. 2.

JOHNSON, G F., THATCHER R. S., 2001, "B2C data privacy policies: current trends", *Management Decision* 39/4 pp262-271

JONES, S., WILIKENS, M., MORRIS, P. AND MASERA, M. (2000), "Trust requirements in e-business", *Communications of the ACM*, Vol. 43 No. 2, pp. 81-7.

KAREN A. FORCHT AND THOMAS D. S., (1994), "Information Compilation and Disbursement: Moral, Legal and Ethical Considerations", *Information Management & Computer Security*, Vol. 2 No. 2, pp. 23-28

KELLY E.P., ERICKSON G.S.,(2004), "Legal and privacy issues surrounding customer data bases and e-merchant bankruptcies: reflections on Toysmart.com", *Industrial Management & Data Systems,* Vol 104, No. 3, pp 209-217

KOLSAKER A., PAYNE C., (2002), "Engendering trust in E-commerce: a study a of gender based concerns", *Marketing Intelligence and Planning*, Vol.20/4, pp 206-214

KOLSAKER, A. AND PAYNE, C. (2002), "Engendering trust in e-commerce: a study of gender-based concerns", *Marketing Intelligence & Planning*, Vol. 20 No. 4, pp. 206-14.

KRAMER, R.M. (1999), "Trust and distrust in organizations: emerging perspectives, enduring questions", Annual Review of Psychology, available at: www.findarticles.com/cf0/m0961/1999 Annual/544423111 (accessed 13 June 2007)11.44.

KUCERA K., PLAISENT M., BERNARD P., MAGUIRAGA L., (2005), " An empirical investigation of the prevalence of spyware in internet shareware and freeware distributions", Journal of Enterprise Information Management, Vol. 18 No. 6, pp. 697-708

LEE, K.O. AND TURBAN, E. (2001), "A trust model for consumer internet shopping", *International Journal of Electronic Commerce*, Vol. 6 No. 1, pp. 75-91

LLOYD I.J.,(1997), Information Technology Law, 2nd Edition, Butterworth's, London, Great Briton.

LYMAN, J. (2003), "Symantec report puts corporations, consumers in crosshairs", Technewsworld, available at: http://www.technewsworld.com/perl/story/33142.html (accessed May 31 2007).

MADU, C.N. AND MADU, A.A. (2002), "Dimensions of e-quality", *International Journal of Quality & Reliability Management*, Vol. 19 No. 3, pp. 246-58.

MASCARENHAS O.A.J., KESAVAN R., BERNACCHI M.D.,(2003), "Co-managing online Privacy", Journal of consumer marketing, Vol 20, No. 7, pp 686-702

MCCOLE, P. AND PALMER, A. (2001), "A critical evaluation of the role of trust in direct marketing over the internet", paper presented at the World Marketing Congress, University of Cardiff, Wales, July.

MCROBB S., ROGERSON S., (2004), "Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium", Information Technology & People, Vol. 17 No. 4, pp. 442-46

MILLER A.R. 1971, The Assault on Privacy: computers data banks and Dossiers, Anne ArborMich, Michigan UP, USA

MITCHELL, V-W. (1999), "Consumer perceived risk: conceptualisations and models", *European Journal of Marketing*, Vol. 33 Nos 1/2, pp. 163-95.

MOSSBERG, W. (2000), "Five tests to see if AOL will still serve user needs", Wall Street Journal, January 21, p. A3.

MOULINOS K., ILIADIS J., TSOUMAS V., 2004, "Towards secure sealing of privacy policies" Information Management & Computer Security Vol. 12 No. 4, pp. 350-361

MUKHERJEE, A. AND NATH, P. (2003), "A model of trust in online relationship banking", *International Journal of Bank Marketing*, Vol. 21 No. 1, pp. 5-15.

NAKRA P., (2001) "Consumer privacy rights: CPR and the age of the Internet" *Management Decision* 39/4 pp272-278

PETROVIC-LAZAREVIC S. AND SOHAL A. S., 2004, "Nature of e-business ethical dilemmas" Information Management & Computer Security Vol. 12 No. 2, pp. 167-177

PRABHAKER P.R., 2000, “who owns the online consumer”, journal of consumer marketing, Vol 17, No.2, pp 158-171

RABB, C., 1993, The Governance of data Protection, Sage, London

REED C., ANGEL J., (2000), Computer Law, 4th Edition, Blackstone Press Limited, Aldine Place, London, Untied Kingdom.

RIEGELSBERGER, J., SASSE, M.A. AND MCCARTHY, J.D. (2003), “The researcher’s dilemma: evaluating trust in computer-mediated communication”, *International Journal of Human-Computer Studies*, Vol. 58, pp. 759-81.

RIEGELSBERGER, J., SASSE, M.A. AND MCCARTHY, J.D. (2003), “The researcher’s dilemma: evaluating trust in computer-mediated communication”, *International Journal of Human-Computer Studies*, Vol. 58, pp. 759-81.

ROMBEL, A. (2001), “The privacy law debate: navigating the privacy law divide”, Global Finance, Vol. 15 No. 1, January, New York, NY, p. 28.

ROTTER, J.B. (1971), “Generalized expectancies for interpersonal trust”, American Psychology, Vol. 26, pp. 443-52

ROWLAND D AND MACDONALD E., (1997), Information Technology Law, Cavendish Publishing Limited, London, Untied kingdom

ROWLAND D AND MACDONALD E., (2000), Information Technology Law, 2nd Edition, Cavendish Publishing Limited, London, Untied kingdom

SHALHOUB Z.K., 2006, "Trust, privacy, and security in electronic business: the case of the GCC countries", Information Management & Computer Security Vol. 14 No. 3, pp. 270-283

SIMMONS AND SIMMONS, (2001), E-commerce Law; Doing business online, Palladian Law Publishing, Bembridge, Great Britain.

SRINIVASAN, S. (2004), “Role of trust in e-business success”, *Information Management & Computer Security*, Vol. 12 No. 1, pp. 66-72.

STELL, R. AND PADEN, N. (2002), “Creating retail web sites for different consumer shopping orientations”, *Journal of Internet Commerce*, Vol. 1 No. 1, pp. 3-16.

STONE, R. AND GRONHAUG, K. (1993), “Perceived risk: further considerations for the marketing discipline”, *European Journal of Marketing*, Vol. 27 No. 3, pp. 39-50.

SUBIRANA, B. AND CAVAJAL, P. (2000), “Transaction streams: theory and examples related to confidence in internet-based electronic channels”, *Journal of Information Technology*, Vol. 15, pp. 3-16.

TAN, S.J. (1999), “Strategies for reducing consumers’ risk aversion in internet shopping”, *Journal of Consumer Marketing*, Vol. 16, pp. 163-80.

TSIAMES, I.S. AND SIOMKOS, G.J. (2003), “E:brands: the decision factors in creating a winning brand on the net”, *Journal of Internet Marketing*, February, available at: www.ARRAYdev.com/jim/current.htm

UDO G.J., (2001), “Privacy and security concerns as major barriers to e-commerce: a Survey Study” *Information management and computer security*, 9/4, pp165-174

URBAN, G.L., SULTAN, F. AND WUALLS, W.J. (2000), “Placing trust at the centre of your internet strategy”, *Sloan Management Review*, February, pp. 39-48.

WARREN A., 2002, “The right to Privacy? The Protection of personal data in UK public organizations”, New Library world, Vol 103, No. 1182/1183, pp 446-456

WASSERMANN, E. (2000), ``The FTC's unlikely enforcer'', The Standard.com, February, p.16.

WHYSALL P., (2000), "Retailing and the Internet: a review of ethical issues", International Journal of Retail & Distribution Management, Vol28 . No. 11. pp. 481-489

YOUSAFZAI, S.Y., PALLISTER, J.G. AND FOXALL, G.R. (2003), “A proposed model of e-trust for electronic banking”, Technovation, Vol. 23, pp. 847-60.

ZUGELDER M. T., (2000), Theresa B. Flaherty and Johnson J. P., (2000), “Legal issues associated with international Internet marketing” International Marketing Review, Vol. 17 No. 3, pp. 253-271.

BIOGRAPHY OF AUTHOR

Dr. Prathiba Mahanamahewa, obtained LLB(Hons) Faculty of Law University of Colombo and LLM (Hons) University of Melbourne, Australia. In 2002 he was awarded the Legal and Judicial project scholarship to pursue postgraduate studies in Australia and awarded PhD in law from University of Queensland, Australia. Currently, Dr. Mahanamahewa is the Dean Faculty of Law, KDU and Senior lecturer, Faculty of Law University of Colombo.