DOCUMENT RESUME

ED 477 037 IR 021 765

AUTHOR	Karmakar, Nitya L.
TITLE	Online Privacy, Security and Ethical Dilemma: A Recent Study.
PUB DATE	2002-06-00
NOTE	6p.; In: ED-MEDIA 2002 World Conference on Educational Multimedia, Hypermedia & Telecommunications. Proceedings (14th, Denver, Colorado, June 24-29, 2002); see IR 021 687.
AVAILABLE FROM	Association for the Advancement of Computing in Education (AACE), P.O. Box 3728, Norfolk, VA 23514. Tel: 757-623-7588; e-mail: info@aace.org; Web site: http://www.aace.org/DL/.
PUB TYPE	Reports - Research (143) -- Speeches/Meeting Papers (150)
EDRS PRICE	EDRS Price MF01/PC01 Plus Postage.
DESCRIPTORS	Computer Security; Ethics; Federal Government; *Federal Legislation; Foreign Countries; Information Policy; Information Technology; International Cooperation; *International Law; *Internet; *Laws; Privacy; *Public Policy; Technological Advancement
IDENTIFIERS	*Electronic Commerce

ABSTRACT

The Internet remains as a wonder for the 21st century and its growth is phenomenon. According to a recent survey, the online population is now about 500 million globally and if this trend continues, it should reach 700 million by the end of 2002. This exponential growth of the Internet has given rise to several security, privacy and ethical concerns. There are laws governing those issues in several countries, but these laws are difficult to apply due to the rapid change of the technology, as well as security breach. Internet commerce or electronic commerce (e-commerce) poses constant threats to privacy and security. The Web has become a playground for lawbreakers. The aim of this paper is to give a snapshot of the current status of the Internet and also to discuss how it is creating a nightmare for governments that try to find a way to safeguard both consumers and providers of information from possible misuse. The paper suggests that the use of the Internet must be controlled with proper legislation to minimize its negative impact on society. There should be an international law and or a third party monitoring authority so that proper protection could be offered to the users of this ever-expanding technology. (Contains 19 references and 1 table.) (Author)

Online Privacy, Security and Ethical dilemma: a Recent Study

Nitya L. Karmakar Ph.D
School of Management
College of Law and Business
University of Western Sydney, Australia
e-mail: karmakar@it.uts.edu.au

Abstract: The Internet remains as a wonder for the 21st century and its growth is phenomenon. According to a recent survey the online population is now about 500 million globally and this trend continues, it should reach 700 million by the end of 2002. This exponential growth of the Internet has given rise to several security, privacy and ethical concerns. There are laws governing those issues at several countries, but hard to apply it due to the rapid change of the technology and also security breach. Internet commerce or electronic commerce (e-commerce) poses constant threats to privacy and security. The web has become a playground for lawbreakers. The aim of this article is to give a snapshot of the current status of the Internet and also how it is creating a nightmare for governments to find a way to safeguard both consumers and providers of information from possible misuse. The author argues that the use of the Internet must be controlled with proper legislation to minimize its negative impact on our society. There should be an international law and or a 3rd party monitoring authority so that proper protection could be offered to the users of this ever-expanding technology.

Introduction

The rapid development of information technology and the Internet have dramatically increased the quantity of information available in digital form. This has resulted in a proliferation of uses of personal information. Some of these have major implications for the privacy of individuals. The World Wide Web (WWW or the Web) has created a totally new global business culture and environment. The new way of doing business across the globe is called electronic commerce (e-commerce) or online or Internet commerce or business by computers and networks. So the Internet will create a huge market in cyberspace and carry valuable information to a large number of people worldwide. This will give rise to a global knowledge based economy or information economy (Karmakar, 2001a & 2001b). The emerging electronically networked-based information economy will affect how we are governed and how we live (Kobrin 1998). The growth of the information economy also means that there are new threats of security, privacy, ethics and other types of online harassment such as fraud and deception.

The Internet Statistics in a Nutshell

The convergence of information and communication technology (ICT) is transforming most aspects of business and consumer activities. The growth of the Internet is dramatic. According to a recent survey by Nua[1], Internet population worldwide as of August 2001 was 513.41 million. The same survey gives the estimated number of online population around the world [Table 1].

Region	Number (million)
Africa	4.15
Asia/Pacific	143.99
Europe	154.63
Middle East	4.65
Canada & USA	180.68
Latin America	25.33

Table 1: The number of online population around the world

[1] http://www_nua.ie/surveys/how_many_online/

Electronic Commerce: A Challenge

Electronic commerce will significantly increase online business across countries. It will help the delivery of wide range of goods and services in a cost-effective way. With e-commerce set to top $US1000 billion at the end of 2002, the potential for making a fortune by exploiting security breaches is huge. A recent survey of Fortune 500 companies indicated that 62 per cent of firms have suffered computer break-ins during the past year. Identity theft – the use of another person's credit card number and personal details – is on the rise, and threatens the viability of electronic trading (Besserglik, 2000). As more and more business goes online, confidential files are increasingly exposed to the risk of infiltration.

Cyber crime in the new millennium

Companies worldwide have lost $3 trillion from cyber crime. Requests for assistance from the Australian Securities and Investment Commission have increased from eight to 200 in the past two years (Cant, 2002). Research shows companies fail to report cyber crime for fear of negative publicity. A survey by the US department of Defence Cyber Crime centre showed 36 percent of companies reported such crimes. In one of the biggest attempted cyber-scams to date, a thief stole 300,000 credit card number from Internet music company *CD Universe* in December 1999 and posted them on a website after it refused to pay a $US100, 000 ransom. From January 1 to December 31, 2001, federal ID Theft Data Clearinghouse received 86,168 reports of identity theft from across the US, with the District of Columbia and California being the main hot spots. Other uses for stolen information involved employment related fraud (9 per cent) and government benefits fraud (6 per cent)(Deanne, 2000). Network security is not generally very strong, and web and web server vulnerabilities are the main source of credit card information breaches.

Ethical Issues in Cyberspace

Ethics is at the heart of social and political debates about the Internet. Ethics is the study of principles that individuals and organizations can use to determine right and wrong courses of action (Laudon & Traver, 2002). Companies using Web sites to conduct electronic commerce should adhere to the same ethical standards that other businesses follow. Ethical considerations are important in determining advertising policy on the Web. Shea (Shea, 1994) identified 10 Core Rules of Netiquette:

i. Remember the Human
ii. Adhere to the same standards of behaviour online that you follow in real life
iii. Know where you are in cyberspace
iv. Respect other people's time and bandwidth
v. Make yourself look good online
vi. Share expert knowledge
vii. Help keep flame wars under control
viii. Respect other people's privacy
ix. Don't abuse your power
x. Be forgiving of other people's mistake

Issues on Security and Privacy

Security and privacy are interrelated. Information should be used only for the purpose it is collected. Many companies are using the Internet with caution because of concern about network and transaction security. Similarly many customers do not feel secured to making payments over the Internet. As the information concerning credit card numbers or other confidential records traverses on the Internet, there is not yet a reliable method of preventing third parties from accessing this confidential information. A third party unlawful intervention arises when a hacker or some other source has the potential to interrupt data or network resources. This may bring to a company heavy economic loss, which may be in the form of destruction, disclosure, modification of data and other form of abuses. In order to allay consumer fear and protect the confidential data on public networks, companies are starting to pay greater attention to transaction privacy, authentication, and anonymity.

The Internet with no legal boundaries raises concerns about personal privacy. The security and privacy issues are very serious as long as hackers continue to hack on the Net. Personal information and privacy of communications must be protected without any question. Business and consumer concerns about security are legitimate irrespective of countries we live. To minimise risks, the protocols and infrastructure for secure transmission of information are in place or developing.

Security, Privacy in Cyberspace: Legal Framework

Real space means our physical environment consisting of temporal and geographic boundaries, where as *cyberspace* is defined the realm of digital transmission not limited by geography. Privacy online is a legal issue and there is difficulty of applying traditional law to the Internet. The creation and use of knowledge or information are key economic activities all over the world. Sometimes information does harm. It ruins reputations, exposes personal secrets, inflicts emotional injury, and misleads people into mistaken purchases and investments. The law must determine who bears the risk of loss from such harm-not only originators and victims, but also among originators, victims, and all the intermediaries who handle injurious information (Perrritt, Jr. 1996).

Commercialization of the Internet has created a difficult task to establish an international legal framework to maintain security and privacy in cyberspace. There should be technological means to secure data on the net and also a legal safeguard to protect individuals from the possible misuse of the medium. Electronic commerce presents fundamental challenge to the law. The suitable law should tackle the threat of security and privacy when we do business online in the digital economy (Karmakar et al., 2001).

Network security will help to protect privacy. Legal systems must be adaptive to the rapid changes of technology. Existing legal frameworks are outdated for protecting privacy (Loudon 1996). Until the legal environment of privacy regulation becomes clearer, electronic commerce sites should be conservative in their collection and use of customer data. Mark Van Name and Bill Catchings, writing in PC Week in 1998, outlines four principles for handling customer data that provide a good online for Web site administrators. These principles include (Schneider and Perry, 2000):

- Use the data collected to provide improved customer service,
- Do not share customer data with others outside your company without the customer's permission,
- Tell customers what data you are collecting and what you are doing with it,
- Give customers the right to have you delete any of the data you have collected about them.

International Dilemmas

Surveys have found that privacy, piracy, and pornography are the most serious concerns of Internet users. The European Union has established strict privacy laws: "all members countries of the European Union must restrict the export of personal data to countries that do not provide privacy protection that is up to European standards, at least from October 1998 for those that have not already done so, and the restrictions are much tougher than in previous European laws." The European Union's privacy Directive of 1995 is the most significant international statement of information privacy principles since the early 1980s [Greenleaf 1998]. The Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2] attempt to balance the protection of privacy and individual liberties and the advancement of free flows of personal data through eight privacy principles: **Collection Limitation**, **Data Quality**, **Purpose Specification**, **Use Limitation**, **Security Safeguards**, **Openness**, **Individual Participation** and **Accountability** which, if observed, are supposed to guarantee a free flow of personal information from other OECD countries[Greenleaf 1998]. All 25-member countries of the OECD have adopted the Guidelines [Tucker 1988]. Most European countries have passed laws for the public and private sectors based on the OECD principles. New Zealand, Hong Kong and Taiwan also have privacy laws that apply to both public and private sectors. Other countries like Australia[3] have implemented them in part only.

The Council of the OECD has adopted Guidelines for a Cryptography Policy in March 1997[4], setting out criteria for encryption of computerised information for governments to adopt and for businesses, individuals and law enforcement officials to apply in safeguarding electronic transactions, communications and data storage.

The U.S. Government's *Framework for Global Electronic Commerce* calls for governing commercial transactions on the Internet 'consistent principles across state, national, and international borders that lead to predicable results regardless of the jurisdiction in which a particular buyer or seller resides' (Clinton & Gore 1997). European-American disagreement on encryption and piracy may lead to a constant problem to introduce a uniform safeguard (Kobrin 1998). An increase in the use of tools such as E-mail, data bases and computer networks has Canadian companies generally feeling more exposed when it comes to the security of internal communications and proprietary information (Church 1998). Northern Telecom, based in Toronto, Canada has programs to ensure that its employees realize how important it is to safeguard sensitive information. It also conducts physical and electronic audits to ensure that important papers aren't left on desks.

---

[2] http://europa.eu.int/comm/dg15/en/media/dataprot/priv.htm

[3] The 11 Information Privacy Principles in the *Privacy Act 1988(Cth)* are intended to implement the OECD's 8 principles insofar as personal information held by Commonwealth public sector agencies are concerned. Australia has still failed to comply with the guidelines for thirteen years after announcing its adherence in 1984.

[4] http://www.oecd.org/dsti/sti/it/secur/index.htm

The global Internet governance is a big issue. Under the present system, an Australian company in dispute with a multinational company over a domain might have to fight that battle in a US court. There is now a genuine concern that Australian companies are going to be faced with having to go US courts to have their Internet disputes resolved (Riley 1998). The law should respond to business concern in the information economy. The existing law cannot cope with the transborder data flow. Technology and business are changing very rapidly, but law is somewhat static. Many business firms are very adaptive to rapidly changing global environment due to the information revolution (Johnston et al. 1997).

Privacy & Australia

The Commonwealth *Privacy Act 1988*[5] lays down strict privacy safeguards which Commonwealth (federal) and ACT government agencies must observe when collecting, storing, using and disclosing personal information. The Act also gives individuals access and correction rights in relation to their own personal information. The Act applies to the wider community (including the private sector and state and local governments) only in relation to specific categories of information: tax file number information and consumer credit information.

Privacy issues arise in a wide range of areas and circumstances. Privacy legislation deals mainly with information privacy - the handling of personal information. Other privacy issues such as video surveillance, telephone interception or 'bugging', and other laws may cover physical intrusion into private spaces.

In December 2000, the *Privacy Amendment (Private Sector) Act 2000* (the Amendment Act) was passed by federal Parliament. The private enterprises became subject to privacy laws on December 21, 2001. The application of the Privacy Act is triggered by the financial size of the organization and the nature and use of the data it collects or processes. It is also subject to some ad hoc exceptions and differing start dates. The National Privacy Principles (NPPs) in the Privacy Act set out how private sector organisations should collect, use, keep secure and disclose personal information. The principles give individuals a right to know what information an organisation holds about them and a right to correct that information if it is wrong.

The surveys showed that Australians regard privacy as a closely held and highly personal value. People look for signals that an organisation will manage their personal information well, for example, 59% said they would trust an organisation more if that organisation gave them control over how their information was to be used, 55% said that organisations with privacy policies would be more likely to gain their trust. Various government bodies have been involved in projects and activities designed to encourage the uptake of E-commerce and Electronic Service Delivery.

Among critics of the private sector privacy regime has been the European Commission (EC), which commented unfavorably. In essence, the EC said it did not regard Australia's privacy regime as sufficiently protective on about nine grounds. All in all, as noted at the time of is passage into law, the application criteria is open to criticism for being arbitrary and the wording of the provisions makes it less than crystal clear how, or even if, it is to apply in given cases, especially, to small businesses (Minahan, 2002).

Australia should be prepared to keep pace with technological innovation and join the new global business environment if it is to remain competitive internationally. Australian Business law in the current form cannot cope with the contemporary business operations. The technological change is revolutionary, but the change in the legal system is evolutionary. There should be a number of changes in Australian legal systems to accommodate electronic commerce. Under Australian law, if someone steals a credit card it is not an offence until the card is used. But in the US it is against the law to misuse an identity with the intention of committing a crime.

Concluding Remarks

We have introduced debate concerning Internet regulation. The U.S.A is the key player to bring about any effective change. There is a need to keep clean our online information environment through generally accepted international laws or other regulatory mechanisms. The Internet is global, multi-jurisdictional structure; national legal systems will not control the uses and abuses of Internet use. The continuing growth of the Internet has seen a corresponding growth in concern about online ethical privacy and security. Surveys continue to show that users are concerned about the collection, security, use and disclosure of information about them on the Net.

[5] http://www.privacy.gov.au

References

Besserglik, B. (2000). Spotlight turned on cyber crime. *The Australian IT/Cutting Edge* (*The Australian*) Tuesday, May 16, p.3.

Cant, S. (2002). Cyber Crime a $3 trillion nightmare. *The Sydney Morning Herald*, Tuesday, March 5, p.5.

Church, E. (1998). Business Ethics/The on-line world has firms fretting about losing their ideas to rivals. *The Globe and Mail*, Thursday, March 26, B17.

Clinton, W. J. & Gore, Jr., A. (1997). A Framework for Global Electronic Commerce. Washington, D. C., July (http://www.iif.nist.gov/eleccomm/ecomm.htm), 4.

Dearne, K. (2002). Online ID theft is top of the pops. *The Australian IT* (*The Australian*), Tuesday, February 12, p.31.

Greenleaf, G. (1998). Global Protection of Privacy in Cyberspace – Implications for the Asia-Pacific. Internet Law Symposium, Science & Technology Center, Institute for Information Industries, World Trade Center, Taipei, Taiwan, 23-24 June.

Johnston, D., Handa, S. Morgan, C. (1997). Cyber law: What You Need to Know about Doing Business Online. Stoddart, Canada.

Karmakar, N.L., Kehal, H.S. & Agrawal, R (2001). Information Economy in the Digital Era: A Global View. for a book *Globalization, Flexibility and Competitiveness, A Technology Management Perspective*,335-346, edited by Professors Sushil and Momaya (Indian Institute of Technology, Delhi) published by the Vikas Publishing House Pvt. Ltd., New Delhi, India, May.

Karmakar, N. L. (2001a). A Global Overview of New Business Paradigm: The Digital Divide Published in the *Proceedings of the* **World** *Conference on the WWW and Internet* (**WebNet 2001**), Oct.23-27, 2001, Orlando, Florida, USA.

Karmakar, N. L. (2001b). Emerging Issues in Information Economy & Electronic: A Strategic Analysis. Published in the *Proceedings of the World Conference on Educational Multimedia, Hypermedia & Telecommunications* (ED-MEDIA 2001), June 25- 30, 2001, Tampere, Finland.

Kobrin, S. (1998). You can't declare cyberspace national territory: Economic Policy Making in the Digital Age. In D. Tapscott, A. Lowy & D.Ticoll (Eds). Blueprint to the Digital Economy: Creating *Wealth in the era of E-Business*. McGraw-Hill, 355-370.

Laudon, K. C. (1996). Markets and Privacy. *Communications of the ACM,* Sept. Vol. 19, No. 9, 92-99.

Laudon, K. C. & Traver, K. C., (2002), *E-commerce: business, technology, society.* Addison-Wesley.

Minahan, S. (2002). European privacy rules pack some punch for Australia. *The Sydney Morning Herald*, Tuesday, February 26, p.6.

Perrit, Jr. H. H (1996). Law and the Information Superhighway: Privacy, Access, Intellectual Property, Commerce, Liability. John Wiley & Sons, Inc.

Riley, J. (1998). Forum seeks Net rules, The AUSTRALIAN: Tuesday, August 11, 36

Schneider, G. P. and Perry, J. T. (2000). *Electronic Commerce.* Course Technology.

Shea, V. (1994). *Netiquette.* ISBN: 0-9637025-1-3

Tucker, G. (1988). Present situation and trends in privacy protection in the OECD area. *Committee for Information, Computer and Communications Policy*, OECD, Paris.

Acknowledgements

The author expresses his gratitude to the School of Management, University of Western Sydney for allowing him to present this paper at the prestigious World Conference on Educational Multimedia, Hypermedia & Telecommunications (ED-MEDIA 2002), Denver, Colorado, USA, during June 24 -29, 2002. Special thanks to Professor Len Fertuck, Professor of Information Systems, Joseph L. Rotman School of Management, University of Toronto, Canada for contributing ideas and suggestions. Finally, last but not least, he would like to thank his wife, Mrs Mitra Karmakar, daughter, Indira and son, Bikram, without whose support this paper would not have been possible.

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

NOTICE

Reproduction Basis

X	This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.
	This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").