Paper 1112

Dr. (Mrs.) Ashraf U. KAZI
Monash University
Australia

INTERNET SECURITY: LEGAL ISSUES, IMPLICATIONS AND CHALLENGES FOR INFORMATION COMMUNICATION TECHNOLOGY, E-COMMERCE, BUSINESS AND CONTRACTS

Dr. (Mrs.) Ashraf U. Kazi*

Dr. (Mrs.) Ashraf U. Kazi*
*Co-ordinator in Business Law, Corporations Law, IT Law,
Department of Business Law And Taxation, School of Business & Electronic Commerce,
Monash University, Churchill, Victoria, Australia 3842.
Telephone: (03) 51226567 or +61 3 99026567
FAX: (03) 51226524 or +61 3 99026524
Email: Ashraf.Kazi@buseco.monash.edu.au

*Corresponding author

ABSTRACT

Businesses are widely adopting and using internet and the information communication technology (ICT) due to easy accessibility of internet. Though the internet has changed life styles and has significant effect on electronic commerce (e-commerce), business contracts and business, internet is exposed to risks and internet security is open to threats. The accessibility to the internet has also posed new challenges and created legal issues and implications. Unauthorised access to data or internet has resulted in cyber crime, which has threatened internet security. Internet security is a complex issue as it encompasses computer system security, network security and personal privacy issues.

The aim of this research is to identify legal issues faced by business while using internet and the information communication technology (ICT). The threats posed to business, e-commerce, business contracts due to extensive use of internet are also identified by this research. The legal issues and implications in relation to internet security are highlighted with a view to minimise risks.

This research is important because it examines the challenges posed to the business, e-commerce, ICT, business contracts, while using the internet with a view to educate the business in relation to the risks involved and to minimise risks. This research is significant as it also seeks to examine the international response to internet security and penal provisions for breaches of internet security. This examination identifies measures to protect and safeguard internet with a view to assist business in identifying threats and thus prevent exposure to risks and increase internet security.

Key words: Information communication technology, legal implications, internet security, e-commerce, legal issues, e-business.

INTERNET SECURITY: LEGAL ISSUES, IMPLICATIONS AND CHALLENGES FOR INFORMATION COMMUNICATION TECHNOLOGY, E-COMMERCE, BUSINESS AND CONTRACTS

Dr. (Mrs.) Ashraf U. Kazi*

I. INTRODUCTION

The accessibility to the network, ICT and the internet has posed new challenges and created legal issues and legal implications. The development of the internet, network, e-commerce and ICT has changed our life styles and the way we conduct business. Unauthorised access to the network or

internet and ICT has resulted in cyber crime, which has threatened internet security. The community, governments and businesses are widely adopting and using internet, ICT and the network due to convenience and easy accessibility. Though the internet has changed life styles and has significant impact on e-commerce, e-business, e-contracts and ICT, internet is exposed to risks as anyone can access the internet and the network security is open to threats because hackers have breached security from time to time.

Internet security has posed challenges and has significant legal implications and legal issues. Internet security encompasses computer system security, network security and personal privacy issues and it is a complex issue. The aim of this research is to identify legal issues and legal implications faced by community, governments and businesses in the day to day use of the network and the internet. The threats posed to e-commerce, business, contracts and ICT due to extensive use of internet are also identified by this research.

The legal implications and legal issues in relation to internet security and breach of security are highlighted in order to minimise risks and suggest means to protect the internet. The research examines the challenges posed to the community, businesses, e-commerce, contracts and ICT due to constant use and access to the internet. An identification of these challenges and threats is important in order to educate the community and businesses in relation to the risks involved and to minimise and prevent risks in future. This research is important as it seeks to examine the response of international community towards the security of the internet. Penal provisions for breaches of network and internet security are also discussed. Finally, the research also identifies measures to protect and safeguard the network and the internet in order to assist the community and businesses in identifying threats and preventing exposure to risks and increasing the internet and network security.

II. SECURITY OF INTERNET AND INFORMATION COMMUNICATION TECHNOLOGY: LEGAL ISSUES AND LEGAL IMPLICATIONS

The popularity, easy accessibility and widespread use of internet and ICT have legal implications and have raised legal issues in relation to internet security. The unauthorised access of internet and a series of virus attacks on popular websites including Amazon.com in the year 2000 have raised awareness of the importance of internet security. The legal issues concerning internet security overlap with privacy and pose problems about how to balance freedom of speech, government regulation and the role of private companies, which control the internet [7].

The judiciary and the courts play an important role in protecting the internet and maintaining internet security by sentencing hackers, deciding cases of electronic commerce and contracts [2]. Much needs to be done in relation to internet security as more and more people tend to conduct public and private business online. Internet security breaches and attacks endanger the privacy of the internet users and the integrity of their personal data.

1. INTERNET SECURITY: LEGAL ISSUES AND LEGAL ANALYSIS

A legal analysis of internet security exhibits three tiers. The uppermost layer consists of the internet as a network, which is the weakest point as it can be easily exploited by hackers. In February and May 2000, hackers made a denial of service attack, which comprised of an excessive number of false, computer-generated hits on a particular web site causing the web site to overload and become unavailable to users and customers [2].

The second layer consists of transactional security commonly known as commerce and personal identity. It involves the question of who really sent the email to you or whose website was accessed. The third and final layer of the internet security consists of personal privacy, which is represented by encryption [2]. All three layers are commonly put together but must be understood independently to deal with the issues of internet security and cyber crime [1].

III. INTERNET NETWORK SECURITY: LEGAL IMPLICATIONS

Citizens, community, business and governments constantly use and access the internet and network. However, they are exposed to risks while dealing with e-commerce, e-business, e-contracts and

information communication technology. As a result of a number of denial of service attacks, the then U.S President Bill Clinton convened a White House Summit on computer security. In order to prevent future security threats or atleast to track down the perpetrators or hackers, an expanded Federal role was proposed to monitor internet activity [17]. The initiative was internationally supported and an announcement was made by the British Government that the government would play a more active role in monitoring internet activity.

The G-8 Internet Security Conference held in Paris, in France on 15 May, 2000 also examined how the government and the private sector could deal with the menaces resulting from the development of information and communication technologies or the use of these technologies by criminals. On grounds of privacy, suggestions such as, Internet Service Providers gather and store more information about users was opposed. Efforts to protect internet security have failed to some extent due a desire to retain privacy of individual users as the users prefer not to let the government know every little thing they do. One solution to network security without compromising privacy is to spend more money on implementing improvements such as configuring software in order to prevent outside access to servers [2].

1. INTERNET AND INFORMATION COMMUNICATION TECHNOLOGY: TRANSACTIONAL SECURITY

While accessing internet for e-commerce, e-business, e-contracts and ICT, issues arise in relation to transactional security. Problems are posed with regards to online security in the field of identity. It is hard to establish the identity of the person, who sent the email. Some other person may send an email from the other person's computer. Security of identity may be provided by passwords, but passwords are not failsafe. Security built on passwords has proved easy for hackers to access. One solution to secure identity is a digital signature, which is issued by a trusted authority, which checks identification prior to issuing a certificate with the identity [24]. Validity of transactions requires personal identification as seen with day to day banking, government dealings, business contracts, which may also be exposed to insecurity. In such cases, privacy of individuals may be protected by adopting false identity.

2. LACK OF CONFIDENTIALITY: PERSONAL PRIVACY AND CYBER-SNOOPING

Internet is used not only by the public, community, citizens and governments but also by the employees and employers. The issue of privacy poses problems to the users of the internet and also to the network and service providers [25]. Use of internet has many advantages as it provides instant access to knowledge, shopping and business. However, unprecedented snooping exists alongside the merits [9]. Most employers have access to their employees' emails [4]. While providing internet security through internet monitoring and by identifying hackers, personal privacy [5] and confidentiality may not be guaranteed. Bill McLaren, an employee was fired after his last employer accessed some of his emails. Texas court rejected his argument about privacy and confidentiality.

Courts in United States of America have held that, 83 million Americans who send more than one-trillion emails a year from workplace have no right to email privacy. According to Phil Clements, an Employment Attorney, the privacy of an employee is weighed against the business needs of an employer. The courts have been more protective of the business needs of the employer than the privacy of the employee [14]. The local government in the United States of America has a legal right to read the email and watch web surfing of its employees including the judges and the courts [15]. Even the Federal judges' internet use is provided and monitored by the U.S. government. Thus, there is a threat to personal privacy through cyber snooping as seen in Re Randolph Furman [18], Randolph Furman, a rural judge of the Cowlitz County Superior Court in Kelso, Washington was forced to resign by the Commission on Judicial Conduct after a network administrator accessed, reviewed and reported on the personal use of the internet by the judge. Furman had visited "adult only" shopping sites, surfed porn and some sites like eBay and Expedia [18].

IV. INTERNET SECURITY AND CORPORATE INFORMATION: LEGAL IMPLICATIONS

During the use of internet by citizens, community, business and governments a large number of records are created almost every day. Companies or corporations hold personal information about

individuals or clients. The legal issues surrounding the internet security relate to the fact that in today's business environment, the day to day transactions of a business, government and company important records are created, used and stored in electronic form using the internet [3]. Most businesses, government and corporations thus have two important legal obligations, [20] which are as follows:

- A duty to provide adequate security for corporate/government information and
- A duty to disclose internet breaches involving personal information to those who are affected [22].

The importance of corporate security obligations and obligations of business to provide internet security [11] was realised, when ChoicePoint, a company, previously unknown to many disclosed that, personal information collected from 145,000 individuals was at risk of unauthorised use for the purpose of identity theft by criminals.

ChoicePoint collects information from U.S households and it is a leading provider of identification and credential verification services to business, government and customers. Class action law suits were filed against ChoicePoint as seen in Goldberg v ChoicePoint, Inc. (12) and in Perry v ChoicePoint, Inc. [16]. It was alleged that ChoicePoint failed to implement adequate security measures and failed to fully disclose the breaches, once they occurred. Many states in the United States are adopting legislation related to security obligations. The first law to adopt security approach to personal information on the internet is the California Security Breach Information Act (S.B. 1388), which became effective on 1 July, 2003. Under the California Security Breach Information Act, all companies doing business in California must disclose any breaches of security in relation to personal information of individuals [21].

V. INTERNET AND NETWORK SECURITY: INTERNATIONAL RESPONSE

National and international organisations have identified the importance of internet and network security. In the year 1997, the High Tech Subgroup of the G-8's Senior Experts on Transnational Organised Crime has developed a plan of action to combat computer crime. Its goals are to ensure that no criminal breaching internet security receives safe haven anywhere in the world and that the law enforcement authorities have the technical and legal ability to find criminals, who abuse the internet and bring them to justice [19].

1. INTERNET AND NETWORK SECURITY: THE RESPONSE OF THE EUROPEAN UNION AND THE PROTECTION OF INTERNET

The European Union (EU) has taken a number of steps to protect internet [10]. A proposal from the EU Commission for a Council Framework Decision on attacks against information systems, published on 19 April, 2002, identified substantive criminal law in the following two articles:

- Article 3, deals with illegal access to Information Systems and
- Article 4, deals with illegal interference with Information Systems.

2. INTERNET AND NETWORK SECURITY: THE RESPONSE OF THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

A large number of international conventions including the Council of Europe Convention on Cyber crime have recognised the importance of legislation to prevent unauthorised access to data or information. Offences under the Convention are committed if any person unlawfully and intentionally enters into a cyber system for which access is restricted, without legally recognised authority, permission or consent. Any illegal access, illegal interception, data interference or misuse of devices to breach internet security is considered as a cyber crime [19].

3. INTERNET AND NETWORK SECURITY: UNAUTHORISED ACCESS AND PENAL PROVISIONS

Unauthorised access to the internet is considered as the most important offence in the field of computer crime, because, access is the fundamental predicate of the misuse of internet. Unauthorised access leads to a series of cyber crimes related to internet security [6]. Based on the recommendations of the Organisation for Economic Cooperation & Development (OECD) and the

Dr. (Mrs.) Ashraf U. KAZI
Monash University
Australia

Council of Europe Convention, many countries have made unauthorised access to data or information liable to punishment. Forty four countries [26] have introduced penal legislation punishing cyber crime related to unauthorised access to data or information. In Australia, under the Cyber Crime Act 2001, section 478, a person guilty of unauthorised access is liable for imprisonment up to 2 years. In India, under the Information Technology Act, 2000, section 66, unauthorised access and hacking with computer system is punishable with imprisonment up to three years or with fine up to two lakh rupees or with both. In United States under the Federal legislation, United States Code, unauthorised access, fraud and related activity in connection with computers, is punishable under section 1030 with imprisonment and fine [19].

4. INTERNET AND NETWORK SECURITY: THE RESPONSE OF WIPO AND THE PROTECTION OF INTERNET

The World Intellectual Property Organization (WIPO), through its Member States [23] is responsible not only for the promotion but also for the protection of intellectual property at the international level. In September 1999 at the first International Conference on Electronic Commerce and Intellectual Property, the Director General of WIPO not only highlighted WIPO's focus on the development of intellectual property but also the protection of intellectual property on the internet by the announcement of Digital Agenda, a plan of action for the WIPO. The Digital Agenda was subsequently adopted by its Member States at the General Assembly [13].

The Digital Agenda promotes adjustment of the international legislative framework in order to facilitate internet and e-commerce through protection of databases. It also broadens the participation of developing countries through the use of WIPOnet and other means for access to intellectual property information [8].

VI. CONCLUSION

The internet, network and ICT are exposed to risks. However, the use of internet, e-commerce and information communication technology by the community and business is unavoidable. The issues of internet security require a balance between the ability of the government to track individual identity and activity on the internet or online activity with personal privacy. With the increased use of internet and network, concerns have been raised on how to prevent unauthorised access of internet and future attacks by hackers. The international response for the protection and security of internet has been overwhelming.

The European Union, the Council of Europe Convention on Cybercrime, the World Intellectual Property Organization (WIPO) and other national and international bodies have made significant efforts to prevent unauthorised access to internet and provide network security. Despite the national and international efforts to protect the internet, e-commerce, e-business, e-contracts and information communication technology, unauthorised access is made from time to time and the network security is breached. It has to be accepted that, internet security may solve some issues but raises fresh concerns due to innovations on the internet. Legislation on internet security should consider the requirements to install latest software, which could prevent denial of service attacks. Though security of personal identity is important, personal privacy cannot be sacrificed.

REFERENCES

1. Adler, M., 1996, 'Cyberspace, General Searches And Digital Contraband: The Fourth Amendment And The Net-Wide Search', Yale Law Journal, Vol.105, pp.1093-1120.
2. Bradley, H., Internet Security and the Courts, Jurist: Legal Intelligence, http://jurist.law.pitt.edu, accessed on 18 December 2005, pp.1-7.
3. Brien, C., 1996, 'Internet: The New Trade In Goods, Services And Ideas', Journal of Law And Information Science, Vol.7, pp.69-86.
4. Bronitt, S., 1996, 'Contemporary Comment: Electronic Surveillance And Informers: Infringing The Right To Silence And Privacy', Criminal Law Journal, Vol.20, pp.144-152.

5. Bronitt, S., 1997, 'Electronic Surveillance, Human Rights And Criminal Justice', Australian Journal of Human Rights, Vol.3, pp.183-207.
6. Carroll, M. and Schrader, R., 1995, 'Computer-Related Crimes', American Criminal Law Review, Vol.32, pp.183-211.
7. Dearing, M., 1999, 'Personal Jurisdiction And The Internet: Can The Traditional Principles And Landmark Cases Guide The Legal System Into The 21st Century?' Journal of Technology, Law and Policy, Vol.4, p.4.
8. Developing countries that have ratified or acceded to the WIPO are Albania, Argentina, Belarus, Bulgaria, Burkina Faso, Chile, Columbia, Costa Rica, Croatia, Czech Republic, Ecuador, El Salvador, Gabon, Georgia, Honduras, Hungary, Indonesia, Jamaica, Kyrgyzstan, Latvia, Lithuania, Mali, Mexico, Mongolia, Panama, Paraguay, Peru, Philippines, Republic of Moldova, Romania, Saint Lucia, Senegal, Slovakia, Slovenia and Ukraine.
9. Electronic Privacy Information Center, http://www.epic.org, viewed 12 May 2006.
10. EU Data Protection Directive: European Union Directive 95/46/EC of 20 February, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Article 17, available at http://europa.eu.int/comm/internal_market/privacy/doc/95-46-ce/dir1995-46_part1_en.pdf.
11. Ford, P., 1997, 'Operation Cybertrader', International Journal of Forensic Computing, Issue 1, pp.7-9.
12. Goldberg v ChoicePoint, Inc. No. BC329115, (Los Angeles Superior Court, filed February 18, 2005).
13. Intellectual Property on the Internet: A Survey of Issues, http://ecommerce.wipo.int/survey/html/7.html, viewed 9 May 2006, pp.1-8.
14. Lee, H., 'E-Avesdropping, News hour with Jim Lehrer, Oregon Public Broadcasting' 7 January, 2000, http://www.pbs.org/newshour/bb/cyberspace/jan-june00/email, pp.1-7.
15. Marlowe, B., 1999, 'You are being Watched', ZDNet Magazine, December.
16. Perry v ChoicePoint, Inc.No. CV-05-1644 (C.D. Cal. filed March 4, 2005).
17. Report on Privacy and Security, 2000, The Federal Trade Commission Advisory Committee on Online Access and Security, 15 May.
18. Re Randolph Furman, CJC No. 3245-F-84, filed 2 June, 2000.
19. Schjolberg, S., 'The Legal Framework – Unauthorised Access to Computer Systems, Moss Tingrett' Moss District Court, Moss, Norway, http://www.mosstingrett.no/info/legal.html, viewed 10 May 2006.
20. Smedinghoff, T., 2005, 'The New Law of Information Security: What Companies Need To Do Now?' The Computer & Internet Lawyer Journal, November, pp.9-25.
21. Smedinghoff, T., 2005, 'World Data Protection Report, Security & Surveillance, Defining the U.S. Legal Standard For Information Security', The Bureau of National Affairs, Washington, D.C.,U.S.A, Volume 6, Number 4, April, pp.1-11.
22. Smedinghoff, T., 2005, 'World Data Protection Report, Security & Surveillance, The Coming Expansion of Corporate Information Security Obligations', The Bureau of National Affairs, Washington, D.C.,U.S.A, Volume 5, Number 4, April,
pp.1-4.
23. Some of the Member States of the World Intellectual Property Organization (WIPO) are Australia, Austria, Belgium, Luxembourg, the Netherlands, Cuba, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Japan, Norway, Singapore, Spain, Sweden, Switzerland and United Kingdom.
24. Strassman, M. and Atkinson, R., 'Jump-Starting the Digital Economy', Seventh Annual Report to the Prime Minister, June 1999.
25. Swire, P., 1998, 'Of Elephants, Mice And Privacy: International Choice Of Law And The Internet', International Lawyer, Vol.32, p.99.
26. The forty four countries are Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, Peoples Republic of China, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Iceland, Israel, Italy, Japan, Latvia, Luxembourg, Malaysia, Malta, Mauritius, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Philippines, Singapore, South Africa, Spain, Sweden, Switzerland, Tunisia, Turkey, United Kingdom, United States and Venezuela.