INTRINSIC LEGAL ISSUES IN IT SECURITY

Respickius Casmir and Louise Yngström

Department of Computer and Systems Sciences (DSV)

Stockholm University/Royal Institute of Technology

Forum 100,

164 40 Kista, Sweden.

Fax: +46 8 703 90 25

si-rc@dsv.su.se, louise@dsv.su.se

ABSTRACT

E-commerce is a rapidly expanding sector all over the world. While this is apparently good news to the world's consumers and business companies, it is creating big challenges to information security experts and legal experts. The former are striving to develop and implement technical solutions that can deter, detect, react and/or provide recovery measures from an attack. On the other hand, legal experts are working hard to ensure that e-business is conducted in a legally acceptable manner. In this paper, we focus on legal aspects of IT security in e-commerce environment. Specifically, we discuss the legal ramifications of e-procurement including privacy issues, electronic signature interpretation in different jurisdictions, and Intellectual Property Rights (IPR) handling in e-commerce. We conclude by suggesting three different approaches to address legal-IT related security problems in e-commerce.

KEY WORDS

IT Security, Legal Issues, and E-Commerce.

INTRINSIC LEGAL ISSUES IN IT SECURITY

1 INTRODUCTION

Internet-based procurement or more precisely e-commerce has created great opportunities to both consumers and entrepreneurs around the world. Shopping over the Internet has made interregional geographical boundaries blurred by providing access to world markets. Such kind of market presence and worldwide penetration had traditionally been exclusively available to a few "capable" individuals and larger companies.

In this paper we start by discussing e-commerce in a nutshell including its pros and cons. We then present and discuss various legal issues that are intrinsic to e-commerce including their possible causes and corresponding consequences if not addressed properly. Further we discuss various efforts done by different stakeholders in attempts to handle some of the issues. Finally we suggest complementary approaches that, we believe, if implemented can significantly take a step forward in the overall effort of addressing these issues.

2 E-COMMERCE IN A NUTSHELL

A search on Google.com search engine using "e-commerce definition" as a keyword gave numerous definitions for e-commerce. On browsing through them all we came out with three common keywords namely buying, selling and Internet. Thus in its simplest terms, e-commerce is all about buying and selling of goods and services on the Internet. E-commerce is thus, a process that involves many sub processes such as e-invoicing, e-contracting, e-government, e-auction/e-reverse auction and e-procurement just a few to mention.

Higher speeds for information propagation over the World Wide Web and wider range of outreach are the typical attributes of e-commerce that makes it superior over traditional commerce. Even an individual with a 28kbps dial-Up connection at home can do business electronically in a much faster way than traditional business mode. Other advantages include wider sphere for advertising and marketing, relatively less cost for marketing and promotion, quicker means for business owners to reach and update their customers of any latest changes in their business offering, and many more. E-commerce also, eliminates the necessity for the use of middlemen and intermediaries in business.

Despite its numerous advantages e-commerce equally has got numerous cons when it comes to the security of data and information that are stored, processed and/or transmitted within e-commerce systems. Particular concerns are on the privacy of personal data, confidentiality and integrity of business data and information, and availability of access to resources and services to legitimate users whenever they want to. All these IT security issues are both technical and legal in nature. In the subsequent sections we discuss the legal aspects only since are ones that constitute to the theme of our paper.

3 PRIVACY ASPECTS IN E-COMMERCE

Privacy is interpreted in different ways in different contexts. Some scholars have defined privacy as "The right to be let alone" (Warren & Bradeis 1890). In 1967 Alan Westin of Columbia University in Privacy and Freedom defined privacy as follows "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" (Westin 1975). There are many more different legal definitions and interpretations for privacy depending on which law applies to that particular environment. In any case, privacy can be conceptualised into 3-dimensions namely privacy of a person, territorial

privacy and informational privacy (Holvast 1993; Rosenberg 1992). Thus, different countries or authorities envision, interpret and create laws on privacy in somewhat different ways.

For instance, in 1995 the European Union ratified the Data Protection Directive 95/46/EC in order to harmonize member states' laws in providing consistent levels of protection for citizens and to ensure the free flow of personal data within the European Union (Official Journal 1995). The directive sets a baseline common level of privacy that reinforces existing data protection law and also establishes a range of new rights. The directive applies to the processing of personal data in electronic as well as in manual file systems. The 1995 directive also imposed an obligation on member states to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, third part countries outside the European Union. This requirement implicitly pressed other countries outside Europe for the passage of privacy laws for them to be able to conduct business with EU member states. Third part countries that have not adopted adequate privacy laws have found themselves unable to conduct certain types of businesses that involve information flows with EU member states, especially, if they involve transfer of sensitive personal data. Implementations of the 95/46/EC directive varies even among member states themselves, however, the key elements of the directive are maintained.

In search for synchronization on privacy issues and business continuity, the United States introduced negotiations for a "Safe Harbor" agreement with the European Union in 1998 in order to ensure the continued transborder flows of personal data. However, it was not until July 26, 2000 when the EU Commission approved the agreement (Safe Harbor 2000). Primarily, the idea of the "Safe Harbor" was that US companies would voluntarily self-certify to adhere to a set of privacy principles worked out jointly by the US Department of Commerce and the Internal Market Directorate of the European Commission. The agreement required that only certified US companies would have a presumption of adequacy and they could continue to receive personal data from the European Union.

Implementation of the US-EU "safe harbor" agreement was, however, later revealed to have some holes (Alan 2002). A European Commission progress report for 2001 revealed a number of flaws in the EU-US Safe Harbor Agreement. The report highlighted the facts that few organisations had signed up to the scheme; and that over 50 per cent of those that had signed were failing to comply with all of the required principles for ensuring adequate data protection. The Commission had also identified that some organisations lacked transparency in their privacy statements, leaving customers with little or no information as to what is done with their details. Further doubt had also been cast over the effectiveness of enforcement procedures, with the suggestion that organisations that failed to comply with their obligations were unlikely to be prosecuted. Issued in February 2002 the report, however, concluded that all the essential elements of the agreement were in place and that a structure existed for individuals to lodge complaints if they felt that their rights had been infringed. On July 12, 2002 the EU also released another Directive 2002/58/EC specifically for addressing privacy in electronic sector (Official Journal 2002).

Countries other than EU member states and US have also formulated laws that govern privacy issues. For example Australia through Privacy Act 1988; Act No. 119 of 1988 as amended incorporating amendments up to Act No. 125 of 2002 (Australia 1988, pp. 48-105) addresses privacy issues including the privacy of information. Specifically, the Privacy Act 1988 describes 11 information privacy principles as listed below:

Principle 1 - Manner and purpose of collection of personal information

Principle 2 - Solicitation of personal information from individual concerned

Principle 3 - Solicitation of personal information generally

Principle 4 - Storage and security of personal information

Principle 5 - Information relating to records kept by record-keeper

Principle 6 - Access to records containing personal information

Principle 7 - Alteration of records containing personal information

Principle 8 - Record-keeper to check accuracy etc of personal information before use

Principle 9 - Personal information to be used only for relevant purposes

Principle 10 - Limits on use of personal information

Principle 11 - Limits on disclosure of personal information

(Source: Australia Privacy Act 1988, pp. 53-59)

Although there seems to be with some correlations among different laws on privacy and probably similar goals, yet relationships are not one-to-one, thus missing an element of legal compatibility. Legal interpretations of terminologies used are different from one jurisdiction to another. Such situations are creating legal problems in e-commerce environments where a buyer and a seller are not necessarily located in one and the same jurisdiction. It also makes it complicated to handle e-commerce related disputes arising in such environments.

Privacy, however, is not the only legal concern when it comes to e-commerce and IT security. Copyrights, trademarks and other Intellectual Property rights are also increasingly becoming topics for discussion in the realm of e-commerce and IT security.

4 COPYRIGHTS AND OTHER INTELLECTUAL PROPERTY RIGHTS

Copyrights and other Intellectual Property Rights (IPR) such as trade secrets and trademarks are among aspects of IT security that a law has to protect. Infringements on IPR are apparently increasing with advancement in Internet technology. In electronic environment IPR infringement takes many forms from software piracy to illegal redistribution of licensed software, from illegal copying of literary to musical or artistic works.

For instance, in recent years there have been developed a number of programs for peer-to-peer communications across the Internet (Casmir & Yngström 2003). The earliest and perhaps the best known of these was *Napster* that was used across the world to exchange MP3 (music) files. Other programs developed since then have offered file sharing for more general types of files. A non-exhaustive list of such programs include: Kazaa, Edonkey2000, Napster, Aimster, WinMX, Morpheus, Napigator, Limewire, Gnutella and Bearshare. The use of such programs, especially, by teenagers around the world is increasing at an alarming rate. Much as we concede that such programs can be used for professional purposes, their misuse might result into copyright infringements such as illegally sharing of audio and video files and pirated of versions of commercial software.

A typical example of such misuse and consequences was published in US media (Foxnews 2003) whereby the Recording Industry Association of America (RIAA) sued a 12-year old girl in New York for illegally downloading music songs using Kazaa. If convicted, under the US federal copyright law she could face penalties of up to $150,000 per song. In this example, had the little girl been well informed of the possible consequences probably she would not have fallen into such troubles. This example agrees with one of our recommendation in the succeeding section with respect to interweaving IT security basics into lower level education curricula.

5 FRAUD IN E-COMMERCE ENVIRONMENT

Advancement in electronic technology is both a blessing to innocent citizens and a handy tool for fraudsters. Today it is not uncommon that when you read a newspaper or a story on the Internet news you are likely to find an article on trading fraud, identity theft, credit card fraud, money laundering or any other form of fraudulent practices around the world. Theft of personal identities is increasing, especially, in US and Europe. It has been reported that in the UK alone incidents rose by 55 per cent in the first three months of year 2002, to 10 057 cases (Hoggarth 2003). Identity theft is lamented as the fastest growing category of fraud.

Unfortunately, fraud is much easier in electronic environment than is in traditional business. Bruce Schneier has identified at least three key features of e-commerce that are likely to make fraud even more devastating (Schneier 1998). Such features include:

i) The easy of automation: An element of automation that makes e-commerce systems more efficient than paper-based systems equally makes fraud more efficient. A particular act of fraud that would have taken a criminal half an hour to execute on the paper world can be completed with a single keystroke or even automatically while the doer is sleeping.

ii) The difficulty of isolating jurisdiction: The electronic world is a world without boundaries. A criminal does not have to be physically near a system he is defrauding; one can easily attack a commercial bank system in Sydney from Brussels. He can as well perform a jurisdiction survey, and launch his attacks from countries with poor criminal laws, and lax extradition treaties.

iii) The speed of propagation: Information travels fast on the Internet unlike counterfeiting paper money that needs skills, equipment, time to plan and sometimes some sort of organisation. If one or even a few people can do it, effects are not that much. Of course it is still a crime, but it is very unlikely to affect the money supply. However, if for instance someone figures out how to defraud an e-commerce system and posts a malicious program on the Internet that could bring down a particular currency, a thousand people could have it in an hour and probably hundreds of thousand in a couple of weeks. Perhaps only the first attacker needs skills, but everyone else can just use the malicious program by clicking on a single icon. On something like “Just click here to drop the Japanese Yen”.

Though fraud has always been a risk to traditional businesses, in e-commerce it even becomes much easier to perpetrate, as money is no longer pieces of paper but bytes of data.

Alas, besides fraud there are many other Internet-based criminal incidents that adversely affect e-commerce. A non-exhaustive list of such incidents includes counterfeiting of currency, child pornography or exploitation, virus and other malicious code creation and launching, computer intrusion and other forms of passive attacks such as wiretapping. These incidents are not only illegal but also unethical in most cultures. Much as we concede that technical security mechanisms and laws are essential in addressing a number of raised legal-IT related incidents, a holistic approach using a well-panned interdisciplinary educational system is equally important.

6 ELECTRONIC SIGNATURE

Electronic signature like many other terminologies is interpreted differently between lawyers and technical people.

i) From the legal perspective, an electronic signature means something that *replaces the signature in the paper world*, something that can be used if a business counterpart or the law require that a contract be signed; whereas

ii) The technical concept of and electronic signature is a digital code created with a private key. Signatures allow authentication of information by the process of signature verification.

When you sign a message or file, the program uses your private key to create a digital code that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature. It is synonymously referred to as a Public Key Infrastructure (PKI) digital signature.

Besides differences in interpretations of electronic signature in legal and technical contexts, there are also many differences in legal definitions of an electronic signature from country to country and from one world legislature to another. For example,

1. *United Nations Commission on International Trade Law (UNCITRAL), – Definition: (UNCITRAL 2001, pp. 5)*

[Art. 2.a of Model Law on Electronic Signatures] "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message.

2. *European Union (EU), Directive 1999/93/EC, (Official Journal Jan. 2000, pp. 14) – Definitions:*

[Art. 2.1] "Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication; and

[Art 2.2] "Advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

3. *Sweden, (Qualified Electronic Signatures Act, 2000) - Definition:*

[Art. 2] "Electronic signature" data in electronic form attached to or logically associated with other electronic data, and used to verify that the content originates from the alleged issuer, and has not been altered.

4. *U.S. (DoE., Standards for Electronic Signatures, 2001, pp. 4), - Definition:*

"Electronic Signature" means an electronic symbol or process attached to, or logically associated with, a record and used by a person with the intent to sign the record.

5. *Russia, The Federal Law No. 1-FZ "On Electronic Digital Signature" (Baker & McKenzie, 2002)*

The law defines an electronic digital signature as:

1) A part of an electronic document that is designated to protect the document from falsification;
2) A product of encryption using a secret key; and
3) The part of the document that allows for the authentication of the rightful holder of the secret key, as well as, a point of reference that can assist in detecting any distorted information contained in a document.

Based on the above legal definitions of electronic signatures that were picked at random, it is obvious that in legal context what constitutes an e-signature depends on which law applies to that specific situation. Despite slight deviations of e-signature definitions in different legal contexts, yet we can pick up a common denominator that; *the legal concept*: - e-signature is meant to have the legal effect equal to handwritten signature, and *the technical concept*: - digital signature (PKI) is meant to ensure integrity and authenticity of the signed data. Therefore, Figure 1 depicts a conceptual view of the relationship between a legal e-signature and the PKI digital signature. A point to emphasize here is that the legal effect of e-signature is not global but depends on the legal system applicable in a specific context. Non-discrimination i.e. not denied legal effect solely because it is in electronic form is one of the key elements of any e-signature, unless when the law necessitate formal requirements such as when creating a will.

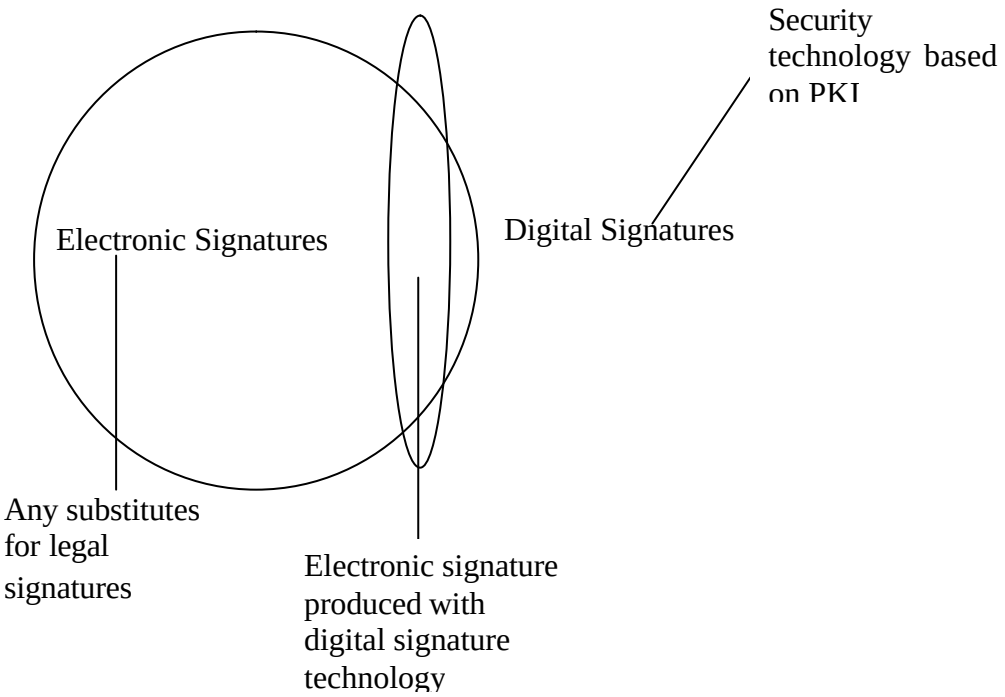

Figure 1. Relationship between Legal Electronic Signature and PKI Digital Signature

All that have been discussed so far are various initiatives made by different authorities in an attempt to handle legal-related security problems in e-commerce environments. Perhaps, it is important to mention here that these are not the only ones but just a random sample taken to exemplify the situations. Despite randomness, the samples were handpicked from the realm of countries that have taken a bigger step forward in terms of e-commerce deployment.

As researchers and academicians we are professionally bound to always not to table a problem and leave it hanging, thus in the next section we propose and discuss multilayered approaches in an attempt to address problems that have been discussed in the preceding sections of this paper.

7 PROPOSED APPROACHES

A careful look at all security problems discussed in the preceding sections of this paper predispose to a belief that most security problems are centred to people than to technology. If security technologies were left to operate/work as intended without human intervention, today we could have been discussing a few software-bugs related and hardware-faults related problems only. Since most IT security problems in e-commerce are apparently emanating from people, new ways of

handling them should be directed to their source, that is to people. This assertion thus, acts as a stepping-stone to our recommendations in the next section.

7.1 Interdisciplinary Curricula

Traditionally, most academic curricula are mono-disciplined. They focus on a particular specialisation such as law, engineering, computer science, and sociology, just a few to mention. However, if one looks at the patterns of today's security problems in e-commerce, it is obvious that some are technical, legal and ethical oriented. For example, teenagers who are accused of writing and launching software viruses seem to lack some security ethics.

In this case, we recommend that academia and other curricula developers think towards developing curricula that are interdisciplinary in nature. This is particularly to those disciplines that are in a way involved in e-commerce activities. For example, Law students need to have a tangible understanding of what IT/IS systems are, how they work, and their capabilities and limitations. Likewise, students doing IT-related programs need to have a significant understanding of the law. Specifically, they need to know the existence of different jurisdictions with different laws, what actions, activities or behaviour constitute an illegal act in their IT environments.

It is important to point out that we are neither trying to convert IT specialists into lawyers nor lawyers into IT professionals. The ultimate goal is to make lawyers and IT specialists "talk the same language", especially, when it comes to legal-IT related security issues in e-commerce that are common to both. The idea here is that today's students are tomorrow's decisions makers and lawmakers, and that students groomed from such interdisciplinary approaches are likely to make better laws and decisions. Also, when designing systems for e-commerce such as e-procurement platforms ex-students from such programs will easily take into considerations important legal issues. Such issues include making it explicit at what point a browsing user gets into a binding contract on the e-commerce platform, and of course not hiding important liability clauses into the middle of a very long legal text.

We understand concerns that existing curricula are already full in their status quo, and that they cannot accommodate extra courses from other disciplines. However, we suggest that new courses from other disciplines can be included into existing curricula during the evaluation and review process of a particular curriculum.

We are aware of a few universities that have already adopted such an interdisciplinary approach including the Stockholm University in Sweden (Laakso 2004). The Department of Law of Stockholm University is offering a Masters Program called Master of Law and IT. The participants into the program also enjoy the additional privilege of gaining the European Computer Driving Licence.

7.2 Interweaving Ethics Topics into Lower Level Education

Sometimes it may be too late to introduce ethics at college or university level education. This is because, some teenagers start using computers, surfing the net and writing computer programs earlier than the time for joining universities. Referring to the example of a 12-year old girl in New York cited earlier in this paper, the girl was still at the primary level of education. To this end, we recommend that some topics on ethical use of computers and Internet be introduced and interweaved into upper primary and secondary level education so that pupils grow up with it into their mind.

7.3 Synchronization of E-Commerce Laws

As researchers the only thing we can offer to Legislative Authorities is to urge them to think on inter-jurisdictions alternatives to synchronize e-commerce related laws. Since the cyberspace in which e-commerce is conducted is a global and continuous medium, laws and regulations governing it should be global and continuous as well. The current situation whereby each jurisdiction handles legal-IT security related problems in its own way is likely to create more problems in future. However, we leave this challenge to the lawyers and legislatures to tackle.

8 CONCLUSION

As discussed in our analysis, there is no single solution that can address all legal-IT related security problems in e-commerce at once. Thus, we believe that the approaches we have proposed for interweaving some topics on ethical use of computers and Internet at lower level education, creation of interdisciplinary curricula at university level and global synchronization of laws and regulations governing e-commerce can play a crucial role in addressing security problems in e-commerce. Also, with exception of a few medium-specific problems, most of security problems we encounter today in e-commerce are not new to businesses. The only thing that is new, though, is the electronic medium environment where e-commerce is conducted.

9 REFERENCES

1. Australia Privacy Act 1988, pp. 48-105; http://www.privacy.gov.au/publications/privacy88_240103.pdf. (Accessed: February 10, 2004)
2. Baker & McKenzie, Legal Alert Electronic Digital Signature Law, January 14, 2002. http://www.bakernet.com/ecommerce/Russia-E-Signature-Alert.doc. (Accessed: March 29, 2004)
3. Casmir, Respickius and Yngström, Louise, "*Security Dimension of IT in Developing Countries: Risks and Challenges*". IN: Journal of Information Warfare Volume 2, Issue 3, 2003: pp. 38-47.
4. EU Directive on Privacy Protection in the Electronic Communications Sector, October 2002, http://www.cdt.org/privacy/guide/protect/privacy-memo.pdf (Accessed: March 15, 2004)
5. Foxnews 2003, http://www.foxnews.com/story/0,2933,96797,00.html (Accessed: January 20, 2004)
6. Hoggarth, Bill, http://www.itweb.co.za/sections/techforum/2003/0303040841.asp. March 2003. (Accessed: February 10, 2004)
7. Holvast, J, "Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?", IN: J. Berleur et al. (Eds.): Facing the Challenge of Risk and Vulnerability in an Information Society, *Proceedings of the IFIP-WG9.2 Conference*, Namur May 20-22, 1993, Elsevier Science Publishers B.V. (North-Holland, 1993.
8. http://www.privacyinternational.org/survey/phr2003/overview.htm
9. Laakso, Pia, Course Administrator, Department of Law Stockholm University http://www.juridicum.su.se/jurweb/utbildning/master/master_of_law_and_it/index.asp (Accessed: March 16, 2004)
10. National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000), http://www.privacy.gov.au/publications/npps01.html. (Accessed: March 11, 2004)
11. Official Journal of the European Communities of 19 January 2000 No L. 13 p. 14
12. Official Journal of the European Communities of 23 November 1995 No L.281 p. 31.
13. Official Journal of the European Communities of 31 July 2002 No L. 201 p. 37.
14. Pedersen, Alan, Privacy Laws & Business, International Newsletter, "EU Report Reveals Holes in US Safe Harbor Agreement", 2002
15. Rosenberg, R, The Social Impact of Computers, Academic press, 1992.
16. Safe Harbor Documents: http://www.export.gov/safeharbor/sh_documents.html, 2000. (Accessed: January 27, 2004)
17. Schneier, Bruce, Electronic Commerce: The Future of Fraud, *1998.* http://catless.ncl.ac.uk/Risks/20.08.html#subj4. (Accessed: January 10, 2004)
18. Sweden, Qualified Electronic Signatures Act (SFS 2000:832), 2000.
19. U.S. Department of Education, Standards for Electronic Signatures in Electronic Student Loan Transactions, 2001, pp. 4.

20. United Nations Commission on International Trade Law UNCITRAL (A/CN.9/WG.IV/WP.88), Working Group on Electronic Commerce, Thirty-eighth session New York, 12 - 23 March 2001
21. Warren, Samuel D., and Brandeis, Louis D., “The Right to Privacy” Harvard Law Review, Vol. IV BOSTON, December 15, 1890.
22. Westin, Alan Furman, “Privacy and Freedom”; Vintage/Ebury (A Division of Random House Group), 1975.