INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 5, NOS.1& 2 (2010); P. 48 – 52.

Latest developments in information technology law with respect to privacy protection

B. Eyo[*1] and E. Williams[1]

ABSTRACT

The spread of Information Technology (IT) on a global scale has made it imperative for nations and groups of nations to devise rules and legislation for the control of how Information Technology is developed, applied, and used within their domains. An examination of some legal issues arising from the evolution, production, acquisition and use of information and communications technology is given in this paper, with perspectives on the United Nations Model Law on E-Commerce and India's recently enacted IT Law. The paper discusses recent trends with regards to IT Law with some bias for privacy protection issues that might shape the future.

INTRODUCTION

Information Technology Law (IT Law) is a set of legal enactments, currently in existence in several countries, which governs the process and dissemination of information digitally. These legal enactments cover a wide area of different aspects relating to computer software, protection of computer software, access and control of digital information, privacy, security, internet access and usage, and electronic commerce. These laws have been described as paper laws for paperless environment (Wikipedia, 2010).

The emerging global IT market with different players in the industry has necessitated legislations to regulate developers on one hand and users on the other hand. Also, the global spread of IT has in one way or the other aided innovative and sagacious ways of perpetrating crimes such as advanced fee fraud, terrorism, child trafficking, to mention but a few. Edwards and Waelde (2009) gave a pointer to this fact when they noted that the development of sophistication in information technology, and expansion of usage of information technology, has also given rise to a new set of crimes and criminal behaviour.

Furthermore, IT Laws were necessary to deal with the use of IT to perpetrate crimes that already existed in the real world before the advent of IT (such as advanced fee fraud, child trafficking, etc), which places a lot of burden on countries with respect to modalities of marrying legislation on IT related crimes to existing criminal activities because prior to the global boom of IT, laws were enacted with penalties spelt out for crimes that occur in the real world, but now that there is a great potential (which is already existent) for IT to be abused and used as a tool for perpetuating these same set of crimes, new laws that deal with these IT related crimes with penalties had to be spelt out as a deterrent for would be criminal minds.

As a result of the broadness of IT Law as a subject, this paper narrows its scope to discussing the growth of e-commerce as a precursor for IT regulation, followed by the United Nations model law on e-commerce; after which a treatise on some areas of India's recently enacted IT law is given, with some comparison as to its consistency and inconsistency in terms of its privacy definitions with that of the European Union Directives and the United States Digital Millennium Act. This is followed by an analysis of how some major players in the IT industry have attempted to use technology to avoid the dictates of Federal legislation on the IT industry. Finally, a case is made for a wider definition of privacy in IT regulations to cater for the emerging trends in the IT industry.

THE GROWTH OF E-COMMERCE AND THE UN MODEL LAW)

Several studies have shown some statistical growth of electronic commerce which is an indication of its global importance. One of such studies (Organization for Economic Co-operation and Development, 1998) concluded that although electronic commerce in the globe was estimated at about US$ 26 billion in 1995, it was estimated that it would hover around $330 billion between 2001 and 2002 and $1 trillion by 2003/2005; business-to-business transactions was said to have accounted for 80 per cent of total e-commerce activity as at 1999 (United Nations Trade and Development, 1999). Between 1995 and 1997, electronic commerce was equivalent to 37 per cent of US mail order catalogue shopping, but estimates are that it will quickly overwhelm US catalogue shopping.

*Corresponding author.
[1]Department of Mathematics/Statistics & Computer Science, University of Calabar, Calabar, Nigeria

Although between 1995 and 1997 electronic commerce accounted for only 0.5 per cent of retail sales in the seven Organization for Economic Co-operation and Development (OECD) economies, it was also estimated to rise 300 fold (to 15 per cent) by 2003-2005 (United Nations Trade and Development, 1999).

The United States has been reputed to account for about four-fifths of worldwide electronic commerce activity over the past few years; and a study by the United States Department of Commerce posited that information technology industries have accounted for over one-third of the real growth in United States Gross Domestic Product (GDP) over the past three years (United States Working Group on Electronic Commerce, 1998). It was anticipated that the growth of electronic commerce the world over would lead to the proportion of such activity in the United States decreasing as electronic commerce activity outside the United States increases (United Nations Trade and Development, 1999), which is the case today as the European Union and indeed Asia have undoubtedly taken a great slice of the market.

Internet accessibility globally makes electronic commerce a more realistic possibility, whereas the hitherto lack of awareness of electronic commerce, the lack of suitable products and integrated systems, and the lack of a sound legal basis, combined with the newness and continued evolution of the market, the complexity and cost of electronic commerce, and uncertainty about its benefits and security, are perceived as significant barriers and obstacles to the development and usage of electronic commerce (Working Party on SMEs, 1998).

A major concern of many countries before promulgating their various IT Laws and regulations was that existing legal frameworks would not have adequately accommodated electronic commerce, and that existing law centring on paper-based systems may prove to be a barrier to increased global electronic trade. During the first quarter of 1985, the United Nations Commission on International Trade Law (UNCITRAL) mandated all Governments to "review legal requirements of a handwritten signature or other paper-based methods of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication" (UN General Assembly, 1999); a call of which gained the blessing of the United Nations General Assembly afterwards (United Nations Trade and Development, 1999).

The United Nations model law on e-commerce

The inexistence of a definite legal structure for field of electronic commerce which was growing at a geometric rate encourage the preparation of a set of legal principles and basic legal rules governing electronic commerce by the UNCITRAL, which completed its work in 1996 and officially adopted the Model Law on Electronic Commerce (United Nations Commission on International Trade Law, 1997). The General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 adopted the Model Law on Electronic Commerce, adopted by the United Nations Commission on International Trade Law (United Nations Commission on International Trade Law, 1997). This Model law defines digital/electronic entities/jargons and activities that are common to all nations, such as information system, electronic data interchange, intermediary, etc. The resolution recommends that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information (United Nations Commission on International Trade Law, 1997).

The main objective of the Model Law was to provide an internationally accepted standard set of rules for national legislatures to adhere to in drafting their own IT laws, whilst allowing a number of legal obstacles to be removed and a more secure legal environment created for electronic commerce (United Nations Trade and Development, 1999). A number of key principles are spelt out in the Model Law; for instance, Article 5 of the law prescribes rules for non-discrimination: information should not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form (United Nations Trade and Development, 1999). The core of drafting a model law for nations to follow was for uniformity across the board but social and cultural differences have tended to derail some of the set objectives with respect to IT laws of independent nations or group of nations.

INDIA'S INFORMATION TECHNOLOGY ACT

India recently amended her Information Technology Act of 2000, adding much anticipated provisions on data protection, cybercrimes, ISP liability, and electronic signature authentication. On December 23rd, 2008 the Indian Parliament enacted the Information Technology Amendment Act 2008 (which was promulgated into law by the Government of India on February 5, 2009) to provide legal recognition and regulate the transactions carried our by means of electronic data interchange and other means of electronic communication, commonly referred to as Electronic Commerce (Harvey and Sanzaro, 2009). The amendments are binding and impact all countries doing business with or in India (Harvey and Sanzaro, 2009), thereby addressing the issue of trust between the management and employees of outsourcing firms.

Also, it included provisions for the identification of, and establishment of penalties for, certain cybercrimes and protection of intermediaries, such as network service providers, when unlawful content is transmitted on their sites or via their networks, as long as they were not involved in the transmission and exercised "due diligence" in discharging their duties. This law is Similar to the

Digital Millennium Copyright Act (DMCA) in the United States (Harvey and Sanzaro, 2009).

The problem of cybercrime is underlined in Section 66 which expands the definition of cybercrime to include identity theft and makes it punishable by up to three years in jail. While Sections 66A – 66F define and impose penalties for other cybercrimes, including cyber-terrorism, Sections 69 through 69B grant the Central Government the authority to intercept, monitor and block access to electronic information in the interest of national security, and to monitor and collect traffic data (data identifying a person, computer system, or location to or from which the communication was transmitted, including origin, destination and other details) for purposes of enhancing cyber security (PlanetIndia, 2009). Section 43A of the law underlines the need for all foreign corporations with offshore Indian service partners maintaining reasonable security practices and procedures when handling sensitive personal data on their computer systems (PlanetIndia, 2009). The Law defines personal data as information which directly or indirectly identifies a person, whether by reference to an identification number or the person's physical, economic, cultural, physiological, or mental details (Richard and Shekar, 2009).

The Indian IT Law privacy definitions for personal data for outsourcing firms is consistent with the European Union Privacy Directives (Richard and Sekar, 2009), while the protection of intermediaries from unlawful activities of users is consistent with the United States Digital Millennium Act (Harvey and Sanzaro, 2009). In spite of efforts at drafting laws that bears a form of uniformity across nations, differences would always exist in some areas of definition; for instance, the definition of sensitive personal data in the Indian IT Law 2009 excludes references to racial or ethnic origins and political or religious beliefs which are in sharp contrast to the European Union Directives (Richard and Shekar, 2009). Some of the consistencies and uniformity in the IT regulations of different nations could be viewed as an attempt at following the spirit and the letters of the United Nations Model Law on E-commerce which encouraged uniformity of IT laws of different countries.

LEGISLATION AND INDUSTRY SELF- REGULATION

Legislation on privacy protection for the IT industry by countries did not come without some opposition by industry players and their allies in government and the legislature. For instance in the United States, the Department of Commerce in 1995 established a model of industry self-regulation (National Telecommunications and Information Administration, 1995) as the government's preferred approach to the protection of Internet privacy. This model was viewed as pro-self-regulation by the legislature and therefore culminated to a variety of legislative proposals aimed at curtailing industry self regulation; these proposals faced stiff opposition from legislatures who favoured self-regulation (Hochheiser, 2002).

In a bid to shove aside the legislative guidelines for privacy protection, companies like Microsoft developed tacit self-regulatory technological measures to privacy protection; the announcement of Microsoft Internet Explorer (IE) 6.0 in 2001 was aimed at avoiding federal Internet privacy legislation in the United States (Hochheiser, 2002). IE 6.0 included a privacy thermostat that enabled system control of Web cookies (Walker, 2001); although cookie cutters and related programs had been available prior to IE 6.0, the difference in cookie handling is that I.E 6.0 was the first major web browser that used the Platform for Privacy Preferences (P3P), developed by the World Wide Web Consortium, to provide this capability – which was a milestone in the development of P3P. The P3P is a facility that gives the user the option of deciding whether to interact with a particular website or not by first all informing the user about the privacy practices of the website (Hochheiser, 2002).

CHALLENGES FACING IT LEGISLATION

The issue of inconsistencies between nations' IT regulations brought into bear some cases of illegal retention of personal data on transit by some nations which is a dangerous precedent that has to be nipped in the bud. For instance, the Federal Constitutional Court of Germany decided on March 2, 2010, ruled that the collection and retention of traffic data, as provided in Sections 113A and 113B of the German Telecommunications Act as well as in Section 100G Paragraph 1(1) of the German Code of Criminal Procedure was unconstitutional and declared that these provisions are void. The court maintained that the aforementioned regulations did not comply with both the European Union legislation and Article 10 Paragraph 1 of the German Constitution which guarantees privacy of communication (Schmidt**, 2010)**. This is one of such cases of inconsistencies in IT laws of nations with bodies (both regional and global) of which they are signatories to which has affected their independent internal regulations.

Another major challenge that tends to underscore the limit of IT Laws, especially as it concerns privacy protection, has to do with the societal movement towards ubiquitous computing. The emergence of location, communication and mobile technologies, such Global Positioning System (GPS), Radio-Frequency Identification (RFID), and advanced wireless devices, with their complimentary potential integration, provide enhanced capability to accurately locate and track people and things in real time anywhere in the physical world, thereby making them ubiquitous. Although there are compelling advantages to such capabilities in serving a wider public interest, the privacy implications, however, are of major concern (Uteck, 2009). This is because there is the tendency for abuse of these capabilities by those

that benefit from these technologies - individuals, governments, and organizations.

Finally, the issue of placing more emphasis on the data protection model of information privacy neglects the central spatial threats to privacy that is posed by ubiquitous computing technologies (Uteck, 2009). As Reiman (2004) puts it, "privacy results not from locked doors and closed curtains, but also from the way our publicly observable activities are dispersed over space and time," which is an extension of the conventional definition or description of privacy to include a new frontier - the societal space. Pursuant to a more unified approach to protecting all that is termed as privacy in our present day world, privacy protection sections of IT laws should be defined, not just for personal and sensitive personal data only, but also for the privacy interests at risk and the spaces which one expects these interests to be protected.

CONCLUSIONS

Nations are admonished to harmonise their IT laws to give room for more consistencies than inconsistencies across the board in vital areas; the reason for allowing inconsistencies being that it would be unrealistic for nations to draft IT legislations that are exactly the same in all areas due to societal, ethnic and cultural differences. Nonetheless, rapid and global spread of Information Technology should spur countries to be consistent and uniform in the enactment of IT Laws to regulate its development and application. Nations should also adopt mechanisms that would enable relevant bodies to modify sensitive areas of their IT laws so as to be in tandem with every changing trend in the industry, especially with respect to potential mechanisations against privacy protection.

REFERENCES

Edwards, L .and Waelde, C. (2009). *Law and the Internet*, Third Edition. Hart Publishing.

Harvey, J. And Sanzaro, K. (2009). *India's New IT Law Impacts Outsourcing Transactions*. Available from: www.lexology.com/library/details.aspx

Hochheiser, H. (2002). *The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context*. ACM Transactions on Internet Technology, Vol. 2, No. 4.

National Telecommunications and Information Administration.(1997). Privacy and Self-Regulation in the Information Age. Available from: http://www.ntia.doc.gov/reports /privacy/privacy rpt.htm.

Organization for Economic Co-operation and Development. (1998). *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, Chap.3. Available from:http://www.oecd.org/subject/e_commerce/summary.htm.

PlanetIndia (2009). *India Information Technology Act 2008*. Available from:cybercrime.planetindia.net/it-act-2008.htm.

Reiman, J. (2004). *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Highway Technology of the Future.* In: Privacies (B. Rossier ed), Physical Evaluations. Stanford California, University of Stanford Press:194-196.

Richard, A. and Shekar, A. (2009). *India Implements brand-new Data Protection Laws*. Available from: www.ichay-mullenex.com/download/india-implements-brand-new-data-protection-laws.pdf

Schmidt**,** S. (2010). Privacy - Ruling by the Federal Constitutional CourtofGermany. http://itechlaw.org//enewsletter/2010/march10/mar10-VM.html.

United Nations Commission on International Trade Law (1997). *United Nations Model Law on E-Commerce*. Available from: www.un.org/documents/ga/res/51/ares51-162.htm.

United Nations General Assembly (1999). *Official Records of the General Assembly, Fortieth Session*. Supp. No. 17 (A/40/17), para. 360. Available at http://www.lawcom.govt.nz/ UploadFiles/Publications/Publication_66_129_R58.pdf.

United Nations Trade and Development (1999). *Trade and Development Board Commission on Enterprise, Business Facilitation and Development Expert Meeting on Capacity Building in the Area of Electronic Commerce: Legal and Regulatory Dimensions*. Geneva, Item 3 of the provisional agenda.

United States Working Group on Electronic Commerce (1998). *First Annual Report*. Available from: http://www/ecommerce.gov

Uteck, A. (2009). *Ubiquitous Computing and Spatial Privacy.* In: *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society (*Ian Kerr, Valerie Steeves, Carole Lucock eds):83-101. Available from: http://www.idtrail.org/files/ID Trail Book/9780195372472.kerr_05.pdf

Walker, L. (2001). *Browser Aimed at Protecting Users' Privacy*. Washington Post, March 29.

Wikipedia (2010). *Information Technology Law – Revised edition*. Available from: www.wikipedia.com

Working Party on Small and Medium Sized Enterprises (1998). *SMES and Electronic Commerce.* DSTI/IND/PME(98)18/REV1. Available from: http://www.ottawaoecdconference.org /english/homepage.html.