Privacy in the Converged Communications Platform

Gita Radhakrishna
Faculty of Business and Law, Multimedia University (Melaka Campus)
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
Email:- gita@mmu.edu.my

ABSTRACT

People care about their personal privacy and have a right to expect that their personal details remain confidential. Yet almost every organization we deal with in our daily lives holds some personal information about us. The convergence of telecommunications, broadcasting, data communication, multimedia and other related technologies and services has increased the ease with which personal data can be gathered, exchanged and transmitted to various buyers of information. These capabilities raise a number of legal issues relating to the regulation of personal privacy and data protection. This paper looks at privacy issues in relation to the fast developing convergence technology in the telecommunication industry. It examines the sources of threats to privacy, the existing regulatory and legal regime in Malaysia and recommends possible strategies to avoid privacy risks.

PRIVACY IN THE CONVERGED COMMUNICATIONS PLATFORM

1.Introduction

Take this scene from the recent movie "Rendition"[1]. A scientist attending a conference somewhere in South Africa gets a 'missed call' from an unknown source on his mobile phone and disappears on a flight from South Africa to Washington. He is kidnapped and taken to a detention facility outside the United States and interrogated for suspected terrorist links. Yet another case, perhaps not so extreme but simply annoying, was that of 'C' who made a one time online purchase and found his mail being inundated with advertisements from various merchants. Major cities around the world today, (including Kuala Lumpur) employ Global Positioning Satellites (GPS) and closed circuit television (CCTV) throughout their cities watching the movement of people as they go about their business.

People care about their personal privacy and have a right to expect that their personal details remain confidential. Who they are, where they live, who their friends and family are and how they run their lives, are all private matters. Individuals may divulge such information to others, but unless the law compels them to do so the choice ought to be theirs.[2] However the term 'privacy has not been specifically defined. In its ordinary meaning its simply the 'right to be left alone.'[3] As U.S. Supreme Court Justice William O. Douglas once observed, "The right to be left alone is indeed the beginning of all freedom." That right is a fundamental principle of common law (where invasion of **privacy** is defined as the wrongful intrusion by individuals or organizations into a person's private activities and effects)[4] Within the context of 'privacy' we have new legal concepts such as ' data protection' and 'information privacy'. The Malaysian government had in 2001 proposed the

[1] "Rendition" (Released October 19th, 2007). Directed by Gavin Hood and Produced by David J. Kanter, Keith Redmon (II) and Michael Sugar

[2] Report of the Information Commissioner to Parliament:- "*What Price Privacy? The Unlawful Trade in Confidential Personal Information*" 10th. May 2006 Available online:- http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf [Visited on 10 Dec. 2007]

[3] Hurriyah El Islamy :-" Information Privacy in Malaysia: A Legal Perspective" [2005] 1 MLJA 25

[4] Thomson and Knight LLP :-"*Privacy when the World is On-Line*" (18 June 2004) LexisNexis Martindale-Hubbell (R) Legal Articles [Visited 2Nov. 2007]

drafting of a Data Protection law. The proposed Bill was to regulate the collection, possession, processing and use of personal data by any person or organisation so as to protect individuals and set common guidelines on the handling of and treatment of personal data [[5]].

The Malaysian Ministry of Energy, Water and Communications defines Convergence as " the progressive integration of the value chains of traditional communications and content industries within a single value chain based on the use of distributed digital technology."[[6]] In other words 'Convergence technology' is the merging of voice, audio, video, data and image into a single flexible network, integrating telecommunications and computer technologies.[[7]] Convergence (converged environments/networks) defines a multi-media environment and/or network where signals regardless of type (i.e. voice, quality audio, video, data, etc.) and encoding methodology may be seamlessly exchanged between independent endpoints with similar characteristics. It is achieved by the merger of packet switching technology with telephony signaling and call-processing intelligence, allowing carriers to consolidate typically separate voice and data overlay networks and provide new and differentiated integrated communications services. Broadband internet provides the "pipe" through which a range of services can be offered. Voice telephony over the internet, denoted as Voice over IP (VoIP), has received the most attention as the challenger to traditional telephony services and is often used to denote a broader class of versatile services running on IP based networks, rather than pure voice alone. Such services include messaging, presence, video conferencing, IPTV and various personalisation and control capabilities. This brings together the products and capabilities of multiple vendors so that they provide services that customers want, be it business, government or individuals.

[5] Khaw Lake Tee "Towards a Personal Data Protection Regime in Malaysia" Journal of Malaysian and Comparative Law [2002]JMCL 11.

[6] Ministry of Energy, Water and Communications "*Policy Challenges of Convergence*" Available online:- http://www.ktak.gov.my/template01.asp?contentid=240 [Visited on 7 Nov 2007]

[7] Wikipedia Available online:- http://en.wikipedia.org/wiki/Technological_convergence ; [Visited on 10 Dec. 2007]

2. Overview

The public switched telephone network (PSTN) is one of the oldest communications networks in existence. However, the growth of the internet has significantly spurred the growth of data over the PSTN and resulted in the need to rearchitect this traditional telephone network Convergence in the telecommunications industry has been a visible trend since the late 1990s with the emergence of new telecommunications technologies such as email, SMS and voice mail to communicate.

The incentive to this industrial movement has been based on the augmenting amount of technological intersections between data communication (i.e. computer science, ICT) applications and telecommunication systems. The convergence movement is still on-going, as observed in the wireless applications industry. In recent years it has also come to refer specifically to the ongoing 'bundling' of services by telecoms players, resulting in 'multiple play' among fixed line phone, TV, broadband services, and mobile phone. More and more operators are providing services which cross the traditional boundaries of communications; for example telecommunications operators are offering content over their infrastructure, and broadcasters are using the internet and mobile platforms for distribution. It is changing the way carriers will carry traditional voice and data traffic.—both from a cost and complexity standpoint.[[8]] The ability of technology to gather, store, retrieve, correlate, disseminate and manipulate personal data has given rise to concerns of infringement of personal privacy and the abuse of it. Technologies not originally conceived for such purposes provide powerful tools for different players to commit privacy invasive abuses. Examples of such technologies are internet data interception and tracking techniques, cookies, profiling based on data collection and data mining techniques, record linkage, surveillance camera technologies, mobile phone digital cameras, web cameras in private or public space, mobile communication technologies in combination with user location computation technologies (including those that are satellite based, such as GPS, smart tag or radio frequency identity (RFID), and biometric technologies.

[8] International Engineering Consortium:- "*Convergence Switching and the Next Generation Carrier*" Available online:- http://www.iec.org/online/tutorials/con_switch/topic01.html ; [Visited on 10Dec. 2007]

3 Is Privacy a Legal Right?

Respect for privacy is one of the foundation stones of the modern democratic state. **Article 12 of the Universal Declaration of Human Rights** specifically provides " No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks."[9] It was written into the **European Convention on Human Rights**, which guarantees certain fundamental human rights. **Article 8** of the Convention declares that 'Everyone has the right to respect for his private and family life, his home and his correspondence'. Adopted by the Council of Europe in 1950, the Convention is directly enforceable in UK courts through the **Human Rights Act 1998**. Failure to respect an individual's privacy can lead to distress and in certain circumstances can cause that individual real damage, mentally, physically and financially. The modern claim to privacy is based on a notion of boundary between the individual and other individuals, and between the individual and the state i.e. the distinction between public and private spheres.[10] The specific reasons for protecting privacy is based on four arguments:

- Privacy empowers people to control information about themselves;
- Privacy is a utility that protects people against unwanted nuisances, or the right to be left alone;
- Privacy is related to dignity in the reciprocal obligations of disclosure between parties;
- Privacy is also a regulating agent in the sense that it can be used to balance and check the power of those capable of collecting data.

Three domains of information privacy maybe identified, each of which though distinct is also necessarily inter related:

- The technical domain
- The regulatory domain
- The sociological domain

Within the technical domain privacy is taken up as a design issue related to such areas as network security and user interface design. The regulatory domain takes up privacy as an issue in the context of data protection and related statutes and regulations. The concerns here are (i) the initial collection of personal information (ii) subsequent use (iii) disclosure of that information, and (iv) the preservation and retention of information.[11] The gathering of such data with other kinds of information leads to 'data co-ordinability' i.e. data-capture and data-matching for customer profiling which could provide the basis for the creation of personal, even intimate, profiling of customers and users of ubiquitous networks.[12] The digital bread crumbs you leave everywhere make it easy for strangers to reconstruct who you are, where you are and what you like. In some cases, a simple Google search can reveal what you think.

The sociological domain can be further subdivided into (i) public versus private space, (ii) the control over personal information inflows and outflows and (iii) the importance of consumer education and awareness related to information privacy threats and protection.

In 2005, research conducted for the UK Information Commissioner's Office (ICO) into public attitudes gives us some idea of the value people place on privacy. Respondents put 'protecting people's personal information' as third in their list of social concerns, alongside the National Health Service. Preventing crime and improving standards in education were ranked first and second. The surveys showed that public concern about personal privacy were focused on threats to personal safety, health, and financial loss.

---

[9] Universal Declaration of Human Rights Available online:- http://www.un.org/Overview/rights.html ; [Visited 10 Dec. 2007]

[10] Bennett, Colin J. and Raab, Charles D. (2003). " *The Governance of Privacy: Policy instruments in global perspective"*. Aldershot: Ashgate, Quoted in ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf [Visited on 15Feb. 2008]

[11] ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf [Visited on 15Feb. 2008]

[12] Wallace, Kathleen. (1999). Anonymity." *Ethics and Information Technology"*, 1, 23-35. Quoted in ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf [Visited on 15Feb. 2008]

4. Sources of Threats to Personal Privacy

Public bodies holding personal information about individuals include government departments and agencies, local authorities, the National Health Service and the police. In the private sector, banks and other financial institutions, supermarkets, telephone companies and transport operators may all hold increasing amounts of information about individuals.

Among the 'buyers' are many journalists looking for a story, finance companies and local authorities wishing to trace debtors; estranged couples seeking details of their partner's whereabouts or finances; and criminals intent on fraud or witness or juror intimidation. The personal information they are seeking may include someone's current address, details of car ownership, an ex-directory telephone number or records of calls made, bank account details or intimate health records. Disclosure of even apparently innocuous personal information – such as an address – can be highly damaging in some circumstances, and in virtually all cases individuals experience distress when their privacy is breached without their consent

4.1 *Internet Marketing*

The privacy threat on the internet arises from a number of factors. Increasing disclosure by consumers of personal information allows companies to capture and process data to a significant extent. New technologies permit the capture of increasingly detailed levels of information. Meanwhile, new internet products often involve a requirement for user registration, enabling of identifying techniques and agreement to terms and conditions that are frequently hostile to privacy.

However the emergence over the past three years of an aggressive move by major internet companies into "ad space" has created the most recent and possibly most dangerous threat to privacy. With the creation of a greater range of products and services, increased disclosure of personal information and the evolution of a huge user population come the opportunity to establish new forms of user targeting and profiling to generate greater advertising revenue.

Database tools that are cheaper and easier to use than ever before allow businesses to collect and analyze information about customers' buying habits to better serve their needs. Business's database can also be linked with or supplemented by private databases for sale, sorted by gender or age or income level or credit history or zip code or all of these and more.[13]

4.2 *Anti-Terrorist initiatives*

Almost every country has changed its laws to reflect 'new' terrorist threats, increasing the ability of law enforcement and national security agencies to perform interception of communications and the type of data that can be accessed, and transformed the powers of search and seizure. George Orwell wrote in his '1984': "There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time." The covert surveillance nature of search/seizure of individuals' communications at telecommunications service providers' premises is vastly more open to misuse and abuse than execution of a search warrant at an individual's own premises. The novelty in these initiatives tends to arise in reduced authorization requirements and oversight. These included initiatives to weaken due process requirements.[14] Data protection legislation, as implemented, ought to take into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the internet and other emerging technologies.

4.3 *Interception of Stored Communication*

While all traffic on the internet is subject to interception, some hackers are spying on corporate / personal wireless networks from outside buildings, where they can scan e-mail and documents. Wireless networks broadcast signals over the public airwaves so they are vulnerable. There has to be an appropriate balance between protecting the privacy of telecommunications users and meeting legitimate needs for access by security and law enforcement agencies.

---

[13] Theodore F. Claypoole:- "Privacy Regulations a Concern with Internet" LexisNexis Martindale-Hubbell (R) Legal Articles (June 27, 2004)

[14] Privacy International :-" *Responding to Terrorism"* PHR 2005; Available online:- http://www.privacyinternational.org/article.shtml?cmd[347]=x-347- [Visited on 10 Dec. 2007]

4.4 ***The disclosure of blocked calling number information to dial-up Internet Service Providers ("ISPs")***

Many, ISPs store log-in information including user names and blocked calling numbers, (if the ISP is receiving same as a result of carriers over-riding blocking), on computers connected to the Internet which carries a risk of unauthorised access by crackers and hackers This poses serious real-world risks and consequences to individuals. [15]. In the **Forcellina Case [16]**, Randall Forcellina, 23, accessed chat rooms, used a device to capture screen names of chat room participants; then sent e-mails pretending to be the ISP requiring correct billing information, including current credit-card number. He then used the credit-card numbers and other personal data to arrange for wire transfers of funds via Western Union Bank, but had other accomplices pick up the funds from the Bank.

4.5 ***Identification of Individuals' Physical Whereabouts-***

Risk of bodily harm or death. The customer asks an ISP staff member to give them the calling numbers used to log in to their account so they can see whether any of the calling numbers were not used by them. There is potential danger in such a reasonable request eg. the abusive husband or boyfriend who wants to trace his estranged wife, an internet stalkers. By giving him the phone numbers, you're giving him enough information to enable him to track down the physical location of his ex-partner for the purpose of assaulting /maiming /killing / blackmailing her.

An ISP having access to blocked calling number information operates on a practical level much like a "reverse phone-book". It can be used by an ISP staff member, or a temporary contractor, or anyone obtaining unauthorised access to the information, to match an anonymous arbitrary identifier (phone number) to a real-world identity and also their physical whereabouts. An ISP staff member/contractor could match the IP address being used by an otherwise anonymous participant in online activities such as Internet Relay Chat ("IRC"), Instant Messaging (such as ICQ, AOL Instant Messenger, MSN Instant Messenger), or sending and receiving emails, against the ISP's login records to find out from the IP address and calling numbers, the number the person dialled in from, which may then be used to find out the person's physical whereabouts as well as information about a person's offline life.. This could be information that would not be ascertainable by the person without knowledge of the blocked calling number. The calling number may not be the number given to the ISP, if any, as a contact number (a mobile or business hours number may have been provided). The person's physical location may be a different address from the one provided to the ISP for billing purposes. Both addresses may be valid addresses for contacting the individual but the one identified from the calling number may be confidential for personal safety reasons.

Examples of individuals who are particularly vulnerable to blackmail and/or physical harm, as a result of their silent or other blocked number and physical location /address being identified in this manner are, sex-workers and their clients, many of whom use the internet to communicate. Others include victims of domestic violence and stalking, people in sensitive occupations such as psychiatric health care, womens' shelters, prison management, counsellors, VIPs, celebrities, politicians, notorieties, political activists/lobbyists, gay and lesbian people, whistleblowers, protected witnesses, judges and other court officials, ex-criminals trying to go straight and avoid their previous colleagues, probation officers, undercover law enforcement and security officers etc. [17]

5. Legislative Responses

5.1 ***Malaysia***

The Constitution of Malaysia does not specifically recognize the right to privacy nor is the term defined in any statute. However there are various sector specific laws to regulate the handling, use and dissemination of information or data as in the banking and financial services, medical records and

[15] Electronic Frontier Australia:-" *Privacy Risks of Supply of Blocked Calling Numbers to ISPs* "(25 July 2003) Available online:- http://www.efa.org.au/Issues/Privacy/cni-complaints/cni-isps-risks.html#risks; [Visited on 10 Dec. 2007]

[16] United States Attorney's Office District of Connecticut; Press Release 26 May 2004; Available online**:-** http://www.usdoj.gov/usao/ct/Press2004/20040526-3.html [Visited 10 Dec. 2007]

[17] Electronic Frontier Australia:-" *Privacy Risks of Supply of Blocked Calling Numbers to ISPs*" (25 July 2003) Available online:- http://www.efa.org.au/Issues/Privacy/cni-complaints/cni-isps-risks.html#risks; [Visited on 10 Dec. 2007]

government records. The word **privacy,** however, has been used in several statutes including: **Births and Deaths Registration Act 1957** (Revised 1983); **Child Act 2001**; **Law Reform (Marriage & Divorce) Act 1976**; **Penal Code** (Revised 1997); **Private Healthcare Facilities & Services Act 1998**; and in two regulations namely **Communication and Multimedia (Licensing) Regulations 1999** and **Private Hospitals Regulations 1973**. There are separate regulations for the government and private sector. Malaysia has as early as 1998 proposed a **Personal Data Protection Bill** which has yet to materialise. The proposed Bill was intended to protect the privacy of personal data and information however recorded, whether manually or by recorded means including those physically residing in computer systems and those transmitted over networks and the internet. It was designed to regulate the collection, possession, processing and use of personal data by any person or organization so as to provide protection to an individual's personal data and safeguard his/her privacy. Towards this purpose it lays down 9 principles of compliance for a data user covering collecting, processing, holding, and using of personal data It also provides for a regulatory structure with a Commissioner for Personal Data Protection playing administrative, supervisory and advisory roles on all matters concerning data protection activities, promoting awareness and understanding of the Bill. The Commissioner is empowered to receive and investigate into complaints on data contravention. Where he is satisfied that the data subject is likely to suffer or has suffered damage or distress, he may serve an enforcement notice on the data user directing the data user to take such steps to remedy the contravention.[18] However exemptions are also recognized in relation to national security, crime and taxation, health, social work, regulatory functions, judicial appointments, legal professional privilege, domestic purposes, staff planning, relevant process, personal references, statistical and research purposes, news, sensitive personal data after death and information available to the public by or under any written law.

The Bill also seeks to impose restrictions on 'data matching' and requires any person proposing to carry out data matching procedures to first obtain the consent of the Commissioner for Data Protection.[19]

The recent case of credit reference companies such as CITOS need to be licensed, controlled and regulated. They must be made to assume liability for inaccurate reporting that results in loss to any party. Countries such as the United States (US) and United Kingdom (UK) have set up specific legislations to protect privacy and personal information. In the US, there are the **Fair Credit Reporting Act 1970** and the **Fair and Accurate Credit Transactions Act 2003**. Banks can also obtain personal credit information from Bank Negara's Central Credit Reference Information System (CCRIS) which imposes certain self regulatory measures. Currently all loan applicants have to sign a consent form for credit verification investigation.[20] Financial institutions using CCRIS data are required to observe banking secrecy under the **Banking and Financial Institutions Act 1989** (BAFIA) and the **Islamic Banking Act 1983** (IBA).[21] These laws prohibit the institutions from divulging the affairs of their customers, except in legally permitted circumstances, like court proceedings between the customer and financial institution or when disclosure is authorised by law to be made to the police. The **Central Bank of Malaysia Act 1958** also allows the bureau to disclose credit information on a person to himself to verify the information's accuracy, report any inaccuracy, which will be investigated by the bureau and conveyed to the financial institution for its immediate rectification.

Section 90(1) of the draft provides that '... every act done ... contrary to this Act ... shall be an offence against this Act. Any person who is convicted of this offence would be liable to a fine not exceeding fifty thousand (50,000) Ringgit Malaysia or **s. 90 (2)** to imprisonment for a term not exceeding six months or both**.. Section 92(1)(a)** provides that if an offence is committed by a body corporate, then any person who at the time of the commission of the offence was a director, chief executive officer, manager, secretary or other similar officer of the body corporate he may be charged severally or jointly in the same proceedings with the body corporate. Under **s 92 (1)(b)** if the body corporate is found guilty for such offence, these officers shall also be deemed guilty of

[18] Khaw Lake Tee "Towards a Personal Data Protection Regime in Malaysia" Journal of Malaysian and Comparative Law [2002]JMCL 11

[19] Schedule 3 proposed Bill.

[20] Giam Say Khoon and Husna Yusop:- "*Years Away from Data Protection Bill*" The Sun 16 July 2007; Available online:- http://www.malaysianbar.org.my/bar_news/berita_badan_peguam/years_away_from_data_protection_bill.html [Visited on 15 jan. 2008]

[21] S.43(4); s. 87(3) BAFIA 1989; ss.31, 32 and 34(1) IBA 1983; s.16 CBMA 1958

such offence**;** unless if such officer can prove that the offence was committed without his knowledge, consent or connivance; and he has taken all reasonable precautions and had exercised due diligence to prevent the commission of the offence.)[22]

5.2 ***The United Kingdom (UK)***

The UK seeks to strike a balance between the right to protection of personal data, the right to obtain, process and store data with the right of accessing personal information held by public authorities except where there are legitimate reasons for keeping it confidential eg. national security. Data protection is accorded by the **Data Protection Act 1998 (DPA),** the **Privacy and Electronic Communications Regulations (PCER)**, and the **Freedom of Information Act (FIA).** The ICO is the UK's independent public body set up to protect personal information and promote public access to official information - from data protection and electronic communications to freedom of information and environmental regulations.[23]

The **DPA 1998** covers how information about living identifiable persons is used specifies that personal data must be:-

1. Processed fairly and lawfully;
2. Obtained for specified and lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up-to-date;
5. Not kept any longer than necessary;
6. Processed in accordance with the "data subject's" (the individual's) rights;
7. Securely kept; and
8. Not transferred to any other country without adequate protection in its original place.

The PECR set out rules for people who wish to send you electronic direct marketing, for example, email and text messages. The sending of unsolicited direct marketing by phone, fax, email, text or any other electronic means is strictly regulated. You have the right to object to electronic marketing messages and can register with a statutory preference service if you don't wish to receive sales calls or junk faxes. The FIA gives you the right to obtain information held by public authorities unless there are good reasons to keep it confidential.

5.3 ***The United States of America (USA)***

In the USA, the word privacy does not appear in the Constitution, but it is has been construed by legal scholars as contained in the **Bill of Rights.** Further instead of one general statute dealing with general protection of personal data, a sector-based approach has been taken. These include, the **Health Insurance Portability and Accountability Act** (HIPAA) has been enacted to deal with protection of health information; the **Gramm-Leach Biley Act** (GLB) governing financial privacy provisions; the **Children's Online Privacy Protection Act** (COPPA) which regulates the privacy of children under the age of 13 and the **Electronic Communications Privacy Act** (ECPA) which limits the circumstances under which federal and state governments may access the contents of transactional data in both real time communications and stored communications. [24] For most Americans the focus is primarily in preventing the government from unnecessarily intruding into the lives of its citizens, as whatever protections that existed have been steadily eroded since 'September 11.' Statutes such as the **PATRIOT Act** which provides law enforcers with sweeping powers of surveillance, search and seizure raises concern among privacy advocates and civil rights lawyers.

6. Recommendations to Avoid Privacy Risks

6.1 ***Security Technology***

Privacy and security issues must be addressed in the planning phase, and may impact the timing or selection of a specific type of wireless service. Specific programs have been developed and released on the Internet to facilitate access to networks using the Wired-Equivalent Privacy (WEP) encryption system. There are various tools that can be used to grab passwords and other sensitive data. Additional security protocols are being developed for networks,

[22] Hurriyah El Islamy :-" Information Privacy in Malaysia: A Legal Perspective" [2005] 1 MLJA 25

[23] The Information Commissioner's Office. Available online:- http://www.ico.gov.uk/what_we_cover.aspx [Visited on 10 Dec. 2007]

[24] Hurriyah El Islamy :-" Information Privacy in Malaysia: A Legal Perspective" [2005] 1 MLJA 25

and some vendors are offering enhanced security features in specific products. [25]

6.2 ***Privacy Education for Staff***

On what they can disclose – advertently & inadvertently and the consequent risks / harm. There is no need for individuals' privacy and well-being to be placed at greater risk by ISPs having access to blocked calling number information. ISPs do not need to receive silent and other blocked calling number information for the provision of dial-up Internet access services, and none of the personal information ascertainable by use of calling numbers is any of an ISP's business

6.3 Privacy Legislation

Communications that are being, or have been, carried over a telecommunications system should be afforded protection under the Telecommunications legislation while they remain stored on a telecommunications service provider's equipment. On 21 February 2006, the Council of the European Union approved the data retention directive, amending the existing directive on privacy and electronic communications (2002/58/EC). The new directive will require providers of telephone, text and internet communications to retain data on traffic (calls made and received) and location (detailing the point where a call is made) but not the content of any communications, for a minimum of 6 months and a maximum of 24 months. Some UK providers currently store these data for up to 12 months under a voluntary code of practice.[26]

"**Stored Communication**" should be defined as " communication that is being, or has been, carried on a telecommunications system and is stored on a (telecommunications) carriage service providers' equipment, ('equipment as defined in the Telecommunication legislation), but does not include a VOIP or other highly transitory communication. [27] Privacy legislation should require:-

(i) ***Destruction of personal information and Third Party content communications*** obtained from collection of stored communications under warrant or any other form of authorisation that is not directly related to and necessary for the purpose for which the warrant or other authorisation was issued.

As a counterbalancing force, the principles of data protection set out in law require that personal information shall be 'adequate, relevant and not excessive' and also that it shall not be kept for longer than is necessary.[28]

(ii) ***Disclosure Reports*** should be required under Telecommunications legislation to show the number of disclosures involving content of communications, including the section authorising such disclosure and the names of government agencies/departments to whom disclosures were made. It should also require the Minister to issue a report annually concerning disclosures of information, including the effectiveness of such disclosures in combatting crime.

(iii) ***Privacy protection for telephone subscriber information*** stored in the Integrated Public Number Database (IPND). The information held in relation to each public telephone number includes:[29]

[25] Ramana Mylavarapu:-" *Security Considerations for WiMAX-based Converged Network*" RFDESIGN Aug 1, 2005 ; Available online:- http://rfdesign.com/mag/radio_security_considerations_wimaxbased/ [Visited on 10 Dec. 2007]

[26] Report of the Information Commissioner to Parliament:- *"What Price Privacy? The Unlawful Trade in Confidential Personal Information*" 10th. May 2006; Available online:- http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf [Visited 10 Dec. 2007]

[27] US Code TITLE 18 > PART I > CHAPTER 121 > § 2701 Unlawful access to stored communications Available online:- http://www.law.cornell.edu/uscode/18/2701.html

[28] Report of the Information Commissioner to Parliament:- "*What Price Privacy? The Unlawful Trade in Confidential Personal Information*" 10th. May 2006; Available online:- http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf; [Visited on 10 Dec. 2007]

[29] Australian Govt. Dept. of Broadband Communication & Digital Economy; Available online**:-** http://www.dcita.gov.au/communications_and_techn

- the telephone number itself
- name of the customer
- address of the customer
- the name of the carriage service provider (CSP)
- the purpose for which the telephone number is used (for example, government, business, charitable or private).

The IPND also includes information about whether a public telephone number is to be listed or unlisted in telephone directories. Unlisted numbers are flagged and not provided to public number directory producers.

(iv) ***Establishing a 'Do Not Call Register'*** applicable to direct marketing/commercial calls to residential numbers in the first instance. Additional measures are also necessary, including regulations governing the use of automated calling systems and minimum national contact standards…an 'opt out option for customers'. It will be necessary to define what constitutes '***unsolicited direct marketing/commercial calls'*** which would not be permitted to be made to numbers on a Do Not Call Register. Such a definition should be substantially similar to the definition of "***commercial electronic messages***" as in Spam. It should also include other types of organisations making unsolicited calls (e.g. charities seeking donations, social or market research organisations)etc.

(v) ***unsolicited direct marketing messages or other solicitation be made illegall*** for companies/organisations to leave call messages on a mobile phone message bank facility because many mobile phone users are charged a fee to access their mobile phone voice mail box.

(**vi**) ***Legal Professional Privilege*** should be a matter required to be taken into consideration in the issue and use of warrants executed at telecommunications service provider's premises for the purpose of obtaining stored communications

ology/policy_and_legislation/numbering/integrated_public_number_database_(ipnd) ; [Visited on 10 Dec. 2007]

7. Conclusion

One of the fundamental challenges that arises in the right to privacy debate is how to manage the conflicts between the needs of society and those of the individual, and to do so in an ethically acceptable manner. Privacy in the converged communication platform requires making every attempt to respect the rights of others. It means ensuring a balance between the right of the individual to be 'left alone' and the ability of business and government departments to carry out legitimate activities for the sustenance and expansion of the economy and ensuring national security.

REFERENCES

1. Australian Govt. Dept. of Broadband Communication & Digital Economy; Available online**:-** http://www.dcita.gov.au/communications_and_technology/policy_and_legislation/numbering/integrated_public_number_database_(ipnd) ;

2. Bennett, Colin J. and Raab, Charles D. (2003). *The Governance of Privacy: Policy instruments in global perspective*. Aldershot: Ashgate, Quoted in ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf

3. Electronic Frontier Australia:- Privacy Risks of Supply of Blocked Calling Numbers to ISPs (25 July 2003) Available online:- http://www.efa.org.au/Issues/Privacy/cni-complaints/cni-isps-risks.html#risks;

4. Giam Say Khoon and Husna Yusop:- "*Years Away from Data Protection Bill*" The Sun 16 July 2007; Available online:- http://www.malaysianbar.org.my/bar_news/berita_badan_peguam/years_away_from_data_protection_bill.html

5. Hurriyah El Islamy :-" Information Privacy in Malaysia: A Legal Perspective" [2005] 1 MLJA 25

6. Information Commissioner's Office. Available online:- http://www.ico.gov.uk/what_we_cover.aspx

7. International Engineering Consortium:- "*Convergence Switching and the Next Generation Carrier*" Available online:- http://www.iec.org/online/tutorials/con_switch/topic01.html ;

8. ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf

9. Khaw Lake Tee "*Towards a Personal Data Protection Regime in Malaysia*" Journal of Malaysian and Comparative Law [2002]JMCL 11

10. Ministry of Energy, Water and Communications "*Policy Challenges of Convergence*" Available online:- http://www.ktak.gov.my/template01.asp?contentid=240

11. Privacy International :-" Responding to Terrorism" PHR 2005; Available online:- http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-

12. Rendition" (Released October 19th, 2007). Directed by Gavin Hood and Produced by David J. Kanter, Keith Redmon (II) and Michael Sugar

13. Report of the Information Commissioner to Parliament:- "*What Price Privacy? The Unlawful Trade in Confidential Personal Information*" 10th. May 2006 Available online:- http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf

14. Thomson and Knight LLP :-"*Privacy when the World is On-Line*" (18 June 2004) LexisNexis Martindale-Hubbell (R) Legal Articles [Visited 2Nov. 2007]

15. Theodore F. Claypoole:- "Privacy Regulations a Concern with Internet" LexisNexis Martindale-Hubbell (R) Legal Articles (June 27, 2004

16. Universal Declaration of Human Rights Available online:- http://www.un.org/Overview/rights.html ;

17. United States Attorney's Office District of Connecticut; Press Release 26 May 2004; Available online**:-** http://www.usdoj.gov/usao/ct/Press2004/20040526-3.html

18. Wallace, Kathleen. (1999). Anonymity. *Ethics and Information Technology*, 1, 23-35. Quoted in ITU Workshop on Ubiquitous Network Societies Document:UNS05/ April 2005 Available online:- http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf

19. Wikipedia Available online:- http://en.wikipedia.org/wiki/Technological_convergence ;

STATUTES:-

MALAYSIA

Banking and Financial Institutions Act 1989
Births and Deaths Registration Act 1957
Central Bank of Malaysia Act 1958
Child Act 2001
Communication and Multimedia (Licensing) Regulations 1999
Draft Personal Data Protection Bill
Islamic Banking Act 1983
Law Reform (Marriage & Divorce) Act 1976
Penal Code
Private Hospitals Regulations 1973

United Kingdom

Data Protection Act 1998 (DPA),

Freedom of Information Act (FIA).

Privacy and Electronic Communications Regulations

United States of America

Bill of Rights
Children's Online Privacy Protection Act
Electronic Communications Privacy Act
Fair Credit Reporting Act 1970
Fair and Accurate Credit Transactions Act 2003
Gramm-Leach Biley Act
Health Insurance Portability and Accountability Act
PATRIOT Act