Telecommunications (interception and access) and its Regulation in Arab Countries

Nazzal M. Kisswani
Department of Business Law,
Faculty of Business and Economics, Macquarie University
Sydney, Australia
nazzal.kisswani@mq.edu.au

Abstract. Telecommunication is a necessity in all countries. Communication has always been an essential part of our lives, education, family relations, business, government and other organizational activities. As telecommunication technology has advanced, so has the need for the interception of telecommunications and access by law enforcement authorities. In addition, lawful interception and the way it is performed have played an important role in the effectiveness of the monitoring of communications. Telecommunications interception and access law should also place a great deal of importance on the privacy of the individual as well as the needs of national security, crime investigation, counter terrorism efforts and economic growth. This paper looks at the applicability of regulations aimed at controlling telecommunications interception and access law in Arab countries. The Australian telecommunications interception and access law is taken as a relevant template that can be examined in light of Arab countries needs and requirements. Various issues unique to Arab countries need to be examined prior to adopting the Australian framework wholesale.

1 Introduction

Telecommunication is a necessity in all countries this century. Communication has always been an essential part of our lives, education, Family relations, business, government and other organizational activities are all completely reliant on communications. It is such an ordinary activity that we take it for granted. So far, without telecommunications technology most modern human activity would come to a stop. To a large extent, the success of almost every human activity is reliant on how available communications methods and techniques are effectively utilized.[1] As telecommunication technology has increased, so has the need for telecommunications interception and access by law enforcement authorities.[2] Arab countries have regulated telecommunication industries although other cyber-related laws have been enacted in some countries, most still lack adequate or comprehensive telecommunication interception and access legislation. This study highlights the absence of telecommunication interception and access legislation in Arab countries and the need for the regulation of newly introduced technological systems that allow control over usage of telecommunication tools. A justification for choosing the Australian law as a template for the Arab world is that Australia was the first country to have introduced telecommunication interception and access laws. Furthermore, Australia has also continually amended its regime with the advancement of technology maintaining its reputation as an advanced liberal democratic economy on the cutting edge of privacy/collectivist debate in this context.

1.1 Objective of Study

This study has a variety of aims: firstly to provide information to the Arab authorities concerned in the regulation of this filed and to examine perceptions about the extent of telecommunications interception and access law in Arab countries. The second aim of the study is to design legislation that assists government officials as well as providing information about the perception of government officials' usage of interception that is a conceptual framework as a foundation for the proposed legislative change. The third aim of the study will address issues concerning the effect of human rights and privacy that are relevant with respect to existing and proposed telecommunications legislation.

The main goal of this study is to determine to extent to which (if any) government officials in Arab countries have introduced and abide by telecommunications interception and access law.

[1] Ian Walden and John Angel, *Telecommunications Law Regulation* (2 ed, 2005)
[2] Whitefield Diffie and Susan Landau, *Privacy on the Line* (1998)

1.2 Statement of Problem

Designing a new regulatory system for telecommunications interception and access in Arab countries has became one of the essentials of achieving security in the battle against terrorism, as well as in the investigation of serious crimes.

In addition, the security level that telecommunications tools provide will affect the level of its usage among the different categories of Arab society. Hence, the problem relates to the degree of trust telecommunications interception and access law by Arab society as well as the security level established through the communications tools resulting from the execution of the law.

This problem will be addressed through an analysis of the advantages and disadvantages of applying the telecommunications interception and access law, and considering what are the most effective procedures and levels that could be used to make the telecommunications interception and access law effective in protecting the property of citizens and their businesses, as well as strengthening security through the use of these tools.

2.0 Overview of Telecommunication Law

2.1 What is telecommunications?

There are several definitions of telecommunication that can be the basis for this study**.** The standard definition of telecommunications is "the art and science of 'communicating' over distance by telephone, telegraph, and radio. The transmission, reception and the switching of signals, such as electrical or optical, by wire, fibre, or electromagnetic (i.e. through-the-air) means".[3]

Thus, it is evident from the above definition that telecommunication is split between two concepts that is the act of communicating and the communication infrastructure.

Other definitions of telecommunications can be found in various other sources; in a 1998 report produced by Association of Information Systems Professionals in Huston telecommunication was described as a process through which information is electronically transferred from one place to another. It is supported with vivid and real examples such as facsimile transmission, telephone system, cellular and mobile phones, credit card verification network and broadcast and radio/TV.[4]

A more academic definition, on other hand, has approached the topic by trying to understand the syllables of the word. Scholar Gabrielle Balbi explains that the first syllable 'Tele' refers to the distance that is commonly associated with other similar words such as telegraph and telephone and 'communications' refers to the link with the different technologies such as radio, mobile phone, television and internet. Balbi holds that all these modes are simply forms of media that allow telecommunications users to talk, view and listen to each other over distance.[5]

2.2 Telecommunication Law and Technology

Noted American Law and Economics scholar Richard Posner provides us with a brilliant analysis of the technological change and the regulatory problems that rise due to this change.[6] Posner points out that the technical problems that judges and lawyers have to face as they try to assess technical aspects of telecommunication matters. Posner takes into consideration the speed of innovation in these fast and new economic times and intelligently points out the vast gap between law time and real time of the new economy, while realizing that any judgment would become obsolete as time passes. This perspective is essential to the design and implementation of any regulatory regime founded on a rapidly changing subject of regulation – such as telecommunication technology. Posner recognizes this delay and foresees the increased risk in any investments and complications in business planning in such a regulatory environment.[7]

Posner debates that the characteristics of the new economy are such that it inclines towards monopoly and yet are open to competition. Posner eases the tension in the debate by explaining that the drive or the competitive

[3] Newton H,"Newton's Telecom Dictionary: The Official Dictionary of Telecommunication". (1998) *New York: Flatiron Pub*

[4] Sharon O'Neil and Donna Everett, *Telecommunications/Networking Information System Curriculum* (1998) ERIC <http://eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED299427&ERICExtSearch_SearchType_0=no&accno=ED299427> at 20 February 2009

[5] Gabriele Balbi, 'Studying the Social History of Telecommunications between Anglophone and Continental Traditions' (2009) 15(15) *Media History* 85.

[6] Richard Posner, 'Antitrust in the New Economy' (2001) 68 *Antitrust Law Journal* 925

[7] Ibid

spirit to obtain monopoly is also a vital form of competition. It is noted by the author that a successful monopolistic undertaking may be established by initially pricing its service at a very low price, especially in cases when it is advantageous to leverage facets from another existing business. Posner humbly admits that he does not possess the answers to these problems.[8]

Today's increasingly digitalized network environment needs a thorough examination of its efficient regulatory framework.[9] This task is carried out by Benkler who takes into consideration the possibilities of licensing becoming obsolete, privatization becoming dictated whine not ignoring the history of regulation; before coming to a conclusion that the most effective means and best way regulate communications infrastructure or computer networks. Benkler has also carried out an extensive examination that reveals the relative benefits of licensing and comparisons to auctioning property rights.[10]

3.0 What is Lawful Interception?

There are several definitions of telecommunication that can be the basis for this study**.** Some UK scholars state that lawful interception plays a vital role in preserving national security, investigating serious criminal activities or even combating terrorism. Law of interception is defined as "the legally authorized process by which a network operators or services provider gives law enforcement officials access to the communications (telephone calls, e-mail massage etc) of private individuals or organization".[11]

> Interception of communication in our current age includes cable systems, public switched telephone network and wireless. It is believed that it is a vital tool in safeguarding the economic well being of state by Straw.[12]

Straw defines interception on the basis of its process,

> "Interception of communication occurs where a private communication between two or more parties, sent via a communications handling system, is covertly monitored in order to understand the content. It is not confined to any particular communication handling system; covert monitoring of private massage sent through telephone networks, email system, paper communication or wireless transmutation is all examples for interception".[13]

More specifications to the definition of interception are introduced by CALEA

> "Communications Assistance for Law Enforcement Act". One of the primary prerequisites of initiating interception is secrecy as it opens up a broad exchange of data about the accomplishments and objectives about an individual without actually violating their privacy. This particular definition by CALEA actually helps in identifying the different parties involved in the process, which are sender of the telecommunication, Law Enforcement Agencies which comprise of any security purpose related agency such as intelligence agencies, state or federal police etc. and the receiver. The Lawful enforcements include 'phone taping' and 'wiretapping '.[14]

Thus it is clear that the purposes of interception are for the preservation of national security, investigating serious criminal activities, combating terrorism or even for some other announced purposes. Certain countries base their licensing in the grounds of the capacity of that telecommunication company for Lawful Interception.[15]

---

[8] bid

[9] Yochai Benkler, 'Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment ' (1999) 11(2 *Harvard Journal of Law & Technology* 286.

[10] Ibid

[11] Rupert Thorogood and Charles Brookson, *Lawful Interception* (2007) Telektronikk http://www.telenor.com/telektronikk/volumes/pdf/2.2007/Page_033-036.pdf > at 10 Augest 2008

[12] Jack Straw, ' Interception of Communications in the United Kingdom: A Consultation Paper' (Home office, 1999)

[13] Ibid

[14] CALEA, *AskCALEA- Frequently Asked Questions* (2003) Communications Assistance for Law Enforcement Act <www.askcalea.net/fags.html> at 10 March 2009

[15] Ibid

4.0 Introducing the Concept of Telecommunication Interception and Access Law

The development of the concept of 'Lawful Interception' has its origins in the European Council Resolution of January 1995[16] which outlined the International Requirements for the Lawful Interception of Telecommunications now recognized widely as the International User Requirement (IUR). The Council lists the requirements to be met by the Member States for the lawful interception of telecommunications traffic.[17] As far as possible, these requirements should ensure a common technical standard for the intercepting of telecommunications. Comparable standards are needed, on the one hand because of the importance of monitoring telecommunications in the fight against international organized crime and, alternatively, to make easy interception on the basis of authorization from the courts.[18]

The development of telecommunications interception and access law was the result of several years of work by the European governments in collaboration with Australia, New Zealand, Canada and the USA.[19] Countries in Asia and South America are beginning to consider mandating similar laws to those in the US and Europe that support the use of standards-based technical implementations for lawful interception.[20]

4.1 Goals of Telecommunications Interception and Access Law

Telecommunications interception and access law is potentially a powerful tool in security investigation and criminal. Telecommunications interception and access laws are not only used to detect networks of relationships between suspected criminals but are also important as they can be used to provide evidence for court cases. In addition, the ability to provide sufficient telecommunications interception and access law is an essential condition for a telecommunications corporation with a license to provide a large scale telecommunications service.[21] Hence, cancellation or delay in the rollout of a new service by telecommunications companies can be caused by governments because telecommunications companies were not able to fulfil their telecommunication interception and access obligations.[22]

4.2 Authorized Interception Agencies

'Wiretapping' or 'phone-tapping' is normally referred to in the interception of telecommunications. Telecommunications interception and access is the process that enables Law Enforcement Agencies (LEA) to secretly intercept within a network communications from person to person. Law Enforcement Agencies include Intelligence Agencies, National Police Forces and Anti- Corruption Commissions.[23]

4.3 Type of Telecommunication Interception and Access

Interception and access can be applied to any medium of communication. Although most interception is of telephone calls, voice over internet protocol (VOIP), SMS messages, email, chat rooms, could also be subject to interception orders. It is part of the culture of people working in telecommunications interception and access that criminals are the first users of any new communication technology and have the ability to develop any new techniques for telecommunication.[24] Since 11 September, 2001, for example, government agencies have insisted

---

[16] European Council Resolution, January 1995,JAI42 Rev 28197/2/95, published in the Official Journal reference 96C 329/01, 4 November 1996

[17] Rupert Thorogood and Charles Brookson, *Lawful Interception* (2007) Telektronikk < http://www.telenor.com/telektronikk/volumes/pdf/2.2007/Page_033-036.pdf > at 10 Augest 2008

[18] Gerhard Schmid "on the draft Council Resolution on the lawful interception of telecommunications in relation new technologies" (1999)

[19] Rupert Thorogood and Charles Brookson, *Lawful Interception* (2007) Telektronikk < http://www.telenor.com/telektronikk/volumes/pdf/2.2007/Page_033-036.pdf > at 10 Augest 2008

[20] Lawful Interception <http://www.retentia.com/interception.htm > 5 February 2009

[21] Australian Commonwealth Parliamentary Library, *Telecommunication Legislation Amendment Bill* (1997) <http//www.aph.gov.au/pubs/1997-1998/98bd067/htm> at 28 October 2008

[22] Philip Branch, 'Lawful Interception of the Internet' (2003) 1(1) *Australian Journal of Emerging Technologies and society* 38

[23] ibid

[24] Ibid

that the new techniques of hiding messages within images that are sent from person to person need to be interceptable.[25]

4.3.1 Lawful interception of Telephone

The concept of the Interceptions of communication has been known since the beginning of the previous century. Interception was used from early 1900s to 1970s for specific reasons and circumstances. The purpose and objective of interception at the time was to investigate criminals and foreign threats. It mainly consisted on tapping into a telephone conversation of the suspected persons and was executed manually at this stage.[26]

Since then the methods applied to intercept calls have been changed dramatically to match the development in telecommunication. Execution of mass interception at a given time was made possible due to computerization.[27] The Law Enforcement Agency (LEA) relied on physical tapping a phone line of the target in response to a warrant.[28]

The direct tapping at this stage was executed through listening to the conversation while police registered the dialed number recorder with a pen attached to the phone line coming directly from particular telephone line. A pen register tap is only permitted to supply traffic analysis of targeted line and not the audio contents of calls.[29] For example, you plug in to right telephone line, and you can immediately listen in on communications.[30] In order to find out who called a suspected target "trap and trace device"[31] which is an electronic device that is used in order to prove all the incoming calls for an exact targeted telephone number. This device is usually used in concert with a pen register (as the pen register deals with the outgoing calls of a targeted telephone number).[32]

After the 1970s, intercepting the content of telephone calls was simple using well known physical sets. These sets evolved as technology of telecommunication also developed.[33] The process was conducted under law enforcement by listening to a person's conversations using a second phone line corresponding with that person's phone line. The legal responsibility of this process was left to the telecommunication company.[34]

The company played a role of simplifying the process through the usage of a punch down block to fix together an additional telephone wire onto the target's phone line. The second line picked up all of the electrical signals passing over it, including the contents of the call. The phone company would then run that second line directly to the police station by hooking up the call as receivers only to avoid any disturbances in the call. The line at the police station would ring simultaneously as the phone of the suspect ring.[35]

In the age of computers, the interception techniques changed to suite the time and age.[36] Manual methods such as pen registers and trap and trace interceptions were replaced by programming software at the telecommunication company's central office switch to pick up the dialled numbers to or from suspect target and to be send them to an electronic teletype to be printed.[37]

---

[25] Kevin Many, *Bin Laden's message could be hiding in plain sight* (2001) <http://www.ustoday.com/columnist/2001/12/19/many/htm> at 3 February 2009

[26] Tim Ehrlich, *Case study of lawful Intercept* (2004) Harvard Law school <http://cyber.law.harvard.edu/globaleconomy/lawful_intercept.pdf> at Febraury 2009

[27] Ibid

[28] Newport Networks, *Lawful Interception Overview* (2008) Newport Networks <http://www.newport-networks.com/cust-docs/87-Lawful-Intercept.pdf> at 5 February 2009

[29] Micah Sherr et al, 'Singling Vulnerabilities in Wiretapping System' (2005) 3(6) *IEEE security & privacy* 13

[30] Bert-Jaap Koops and Rudi Bekkers, 'Interceptability of Telecommunication is US and Dutch Law Prepared for the Future?' (2007) 31(31) *Telecommunication Policy* 45

[31] Jim X Dempsey, *CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections*, Centre for Democracy & Technology, Security & Privacy <http://www.cdt.org/security/000404amending.shtm> at 10 March 2009

[32] Ibid

[33] Tim Ehrlich, *Case study of lawful Intercept* (2004) Harvard Law school <http://cyber.law.harvard.edu/globaleconomy/lawful_intercept.pdf> at Febraury 2009

[34] Philip Branch, 'Lawful Interception of the Internet' (2003) 1(1) *Australian Journal of Emerging Technologies and society* 38

[35] Olmstead v. U.S., 277 U.S. 438, 457 (1928)

[36] Andro Milanović et al, 'Method for Lawful Interception in IP Telephony Network Based on H.323' (2003) 1 *IEEE Computer society*

[37] Federal Bureau of Investigation, 'Implementation of Section 104 of the Communication Assistance for law Enforcement Act' (1998) 63(48) *Federal Register*

The telephone lines coming from suspects' homes could now be monitored through software at the central office switch. Thus eliminating the need to do automatic punch-downs on individual telephone wires was removed as the traffic on telephone wires. The interception of phone contents could be completed by typing an extra command into the central office switch that ordered the switch to automatically send a duplicate signal of the phone call to law enforcement any time the target either dialled or received a call.[38]

Even in the age of the 20th century technology, most telephone calls are still carried over circuit switches. A circuit switch helps to maintain a devoted connection between two parties for the whole duration of the call. At this stage, the used technology ensures that all information of interest to law enforcement, whether it is a voice call or fax, follows the same transmission path and comes over a single line through the telephone company's central office where it can be intercepted.[39]

4.3.2 Lawful interception of the internet

The change in communication from circuit switching to packet switching assisted to change the way we communication. Email, instant messaging, chat, voice over internet (VoIP) are just example and they keep on converging into new means of communication in both mobile and fixed network[40].

At the Internet Protocol age, the emergence of new, packet-based forms of communications such as email and the Internet, law enforcement agencies' capacities and protocols to preserve the advantage in the fight against crime were presented with serious new challenges.[41]

The new challenges are expected given the fundamental nature of packet-based networks, in which the contents of any communication. Email or web pages are sliced up into millions of individual packets before being sent along to their final destination or recipient. Along the way, each packet can take a different route over the Internet and is not reassemble until the final destination is reached. In addition, most Internet Service Providers (ISP) do not tend to keep track of the sites that their customers visit or have any easy way of correlating particular communication traffic with an individual.[42]

5.0 Why is There Need Regulate Telecommunications interception and access

5.1 National Security

National security for any nation is a very wide and a varied subject, ranging from border control to combating terrorism to detecting and identifying fraud to even protecting against spread of epidemics. Thus it is obvious for governments to safeguard information and communication technologies through enhanced national security.[43]

5.2 Combat terrorist and Investigation Crime

Terrorist have realized that they are being monitored and look to means to outsmart the system by learning new and advanced technology for communication not only through coded messages but as well as encryption. The best way to eradicate such a menace is understand the importance and the reasons for telecommunications interception.

After 11 September 2001, and other terrorist attacks in the USA and Europe, most countries have taken legal action to allow for security to access information, in order to determine what material is to be considered personal and not be compromised. For example, through the monitoring of telephone calls and access to their

---

[38]Tim Ehrlich, *Case study of lawful Intercept* (2004) Harvard Law school <http://cyber.law.harvard.edu/globaleconomy/lawful_intercept.pdf> at Febraury 2009

[39]Balamurugan Karpagavinayagam, Redu state and Olivier Festor, 'Monitoring Architecture for Lawful interception in VoIP Network' (Paper presented at the the Second International Conference on Internet Monitoring and Protection-ICIMP, 1-5 2007)

[40] Jari Raman, 'Building Lawful Interception Capabilities: Need for Legal Safeguards' (2009) 2(3) *International Journal of Private Law*
305

[41] Thomas Wong, 'Regulation of Interception of Communications in Selected Jurisdictions' (2005) *Research and Library Services Division Legislative Council Secretariat,Hong Kong*

[42] Susan Landau, *Security, Liberty, and Electronic Communication" (Invited talk) in Matt Franklin(ed) Advances in Cryptology: CRYPTO* (2004) Springer Verlag <http://www.springerlink.com/content/69nnwc07dqq48xvb/ > at 5 April 2009

[43]Mathieu Gorge, 'Lawful Interception – Key Concept, Actors, Trends and Best Practice Considerations' (2007) 2007(9) *Computer fraud & Security* 10

messages in the mail, and knowledge of their location and their movements, by monitoring the vibrations of their mobile phones.[44]

6.0 Telecommunication Interception and the Economic Perspective

The rapid development of information communication and technology (ICT) has brought in cultural, economic, political and social transformation all over the world. At the Marco level, Telecommunication technologies have contributed to significant economic growth in most Arab countries.[45] Evidence collected in a Maddar Centre report indicates that the ICT investment in Arab countries has contributed 32.9 in 2007.[46] Other empirical studies have shown That ICT improves productivity and economic growth based on data collected from developed countries since mid 1990.[47]

At the micro level, the emergence of the Internet, electronic business and electronic government has expanded the ability to have unprecedented access to information. In addition, the internet play important role in connecting between Arab countries with developed countries. Therefore, Internet is deemed as important facilitator for the Arab Countries in achieving economic growth in the new economic.[48]

Arab countries still, however, require an appropriate legal foundation, generally referred to as telecommunication legislation. By definition, telecommunication is a virtual world that is broad and varied, one that includes such broad topics as privacy protection, intellectual property, personal data and other related issues. That digital world, created by computers and communications tools, needs to be organized.

Communications interception is an essential part of law enforcement and intelligence activities. Nations have engaged in the interception of electronic communications for more than a century. Most countries have agencies, policies, and legal structures that control and take advantage of interception techniques. These control mechanisms also secure the country's own communications networks and information from the interception efforts of others.[49]

For example foreign investment in the United States is part of a broader effort in the United States to maintain interception capabilities. Most of developed countries reported that the technological improvement that made communication better and cheaper can also make interception more difficult. These improvements included the use of packet switching, fibre optics, the spread of Voice over Internet Protocol ("VoIP"), and strong commercial encryption.[50]Many of the regulators in developed countries are in the middle of a battle between the government and the telecommunications and information technology industry.[51] In Australia, statutes such as the Telecommunication interception and Access Act and the Communications Assistance to Law Enforcement Act ("CALEA"), the Patriot Act in the United State, Regulation of Investigatory Power Act in the United Kingdom - involved the governments of developed countries making efforts to constrain or respond to technological change.

Technological challenges to interception are now complemented by challenges that arise from changes in the international economic environment: the globalization of supply chains and ownership, especially foreign ownership of Telecommunication networks. This new challenge will form future policy and regulatory interventions of communications interception.[52]

A more gradual set of challenges to telecommunication interception emerged from the regulatory and policy changes that encouraged global economic integration and the internationalization of ownership. The USA foreign policy for more than a century has encouraged an open, international economy and the removal of restrictions to trade and foreign investment. Technological change reinforces globalization.[53] Expanded trade, new

---

[44] Ibid

[45] Ebrahim Nasab and Majid Aghaei, 'The Effect of ICT on Economic Growth: Further Evidence' (2009) 5 *International Bulletin of Business Administration*

[46] Arab Technology (2008) http://www.madarresearch.com/news/newsdetail at 10 September 2009

[47] Mudiarasan Kuppusamy and Solucis Santhapparaj,"Cyber- Law in the New Economic: The Case of Malaysia"(2006) 5(8) *Asian Journal of Information Technology*

[48] Ebrahim Nasab and Majid Aghaei,(2009) "The Effect of ICT on Economic Growth: Further Evidence" 5 *International Bulletin of Business Administration*

[49] James A. Lewis, "New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception" (2005) *57 Federal Communications Law Journal*

[50] Jari Ramon "Building lawful Interception Capabilities: need for Legal Safeguards (2009) 2(3) *International Journal of Private Law*

[51] Ibid

[52] James A. Lewis, "New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception" (2005) *57 Federal Communications Law Journal*

[53] Ibid

technologies, and the resultant international economic integration changed how companies must do business if they want to remain financially and technologically viable. These changes, however, have created a new series of concerns in the national security community.[54]

On the other hand the report prepared to chambers of commerce in the UK summarize the impact of telecommunication interception on the UK business sector and the economy can be measured by the impact it will have on: The nature of business-to-business relationships; the functioning of individual businesses, Direct costs associated with meeting the requirements of the legislation, Investor confidence, and the overall level of consumer confidence in e-commerce.

Also the report provides that most businesses in the UK expressed concern about the following interception related direct costs to their operations: additional insurance costs arising from interception of telecommunication related liability, opportunity costs arising from the inefficient use of specialist staff, costs associated with securing legal and professional advice, and losses arising from inability to create value added services

The report concluded that "the UK government should ignore the economic impact, whilst business is fully supportive of the need for efficient and effective policing of criminal activities". The UK government, in 2000, thus sought amendments to the overall regulation of interception of telecommunication by enacting the Regulation of Investigatory Power Act, One of the justifications for the new act was that regulating the interception of telecommunication was one way of safeguarding the economic well-being of the United Kingdom.[55]

7.0 Australian Telecommunication Interception and Access law

Interception is defined in the Amended TIA Act to apply to "live" or "real-time" communications, that is, communications that are "passing over a telecommunications system."[56] Interception "consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication."[57]

One of the fundamental issues surrounding the act of interception is that of privacy – the privacy of individuals using the telecommunications system. As the Blunn Report states, "a general tenet has always been that communications intended to be private should be private."[58] Balancing these privacy considerations with law enforcement and national security interests, while also expanding the definition of types of new communication technologies and modalities that also fall under the same privacy protections, is at the crux of much of the regulatory debate.

7.1 Laws Prohibiting Interception

Both the TIA Act (in its original and various amended forms), and the Telecommunication Act of 1997 clearly prohibit the interception of communications, other than in the case of specific exceptions (described in detail in section 5.3.2, below). Specifically, and in no uncertain terms,

"A person shall not:
(a) intercept;
(b) authorize, suffer or permit another person to intercept; or
(c) do any act or thing that will enable him or her or another person to intercept; a communication passing over a telecommunications system."[59]

In O'Malley v Keelty, Australian Federal Police Commissioner, Emmett J state the logic fundamental of s 7 as following:

> "There is no doubt that the principle behind s 7 is a very important one. Any member of the community is entitled to his or her privacy and is entitled to ensure that people do not unlawfully listen in to their communications by telephone.[60]

---

54 Ibid

55 The British Chambers of Commerce" The Economic Impact of The Regulation of Investigatory Power (2000) http://eprints.ucl.ac.uk/4117/1/4117.pdf at 5 September 2009

56 *Telecommunications system* have been defined in TIA Act s 5(1) as "(a) a telecommunication network that is within Australia; or (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and within Australia.

57 Telecommunication Interception and Access Act s 6 (1)

58 Anthony Blunn, 'Report of the review of the regulation of access to communications' (Australian Government Attorney-General's Department, 2005)

59 TIA Act s 7 (1)

60 O'Malley v Keelty, Australian Federal Police Commissioner (2004) FCA 1688 at [2].

As Sherman emphasized, "it is often not appreciated that one of the most important provisions in the Interception Act is to make it an offence to conduct unlawful interceptions."[61] To enforce the seriousness of this legal prohibition, any person who violates the interception provisions of the TIA Act is subject to punishment up to two years in prison.[62]

Multiple monitoring and review structures have been put in place, intended to ensure that interception activities are conducted appropriately. Sherman summarizes:

"At the time of the enactment of the Interception Act in 1979 it was recognized by the Parliament that [the TI Act] was highly intrusive and that there needed to be significant safeguards built into the legislation to protect it from abuse. Accordingly, a number of important safeguards were built into the original legislation and these have been refined by legislative amendment in the intervening years."[63]

These safeguards include both internal (warrant procedures) and external (monitoring and reporting) structures.

7.2 Exception to the Laws Prohibiting Interception

The exceptions to prohibitions on interception are related to either national security or law enforcement considerations, as specifically authorized by warrant. As TIA Act provides that the class' of offences now are divided into serious 'Class 1 offences' which include murder, kidnapping, narcotic offences and, currently, terrorism offences, with less important offences elected 'Class 2 offences' which include serious offences involving loss of life or serious injury, serious property damage, corruption, tax, serious fraud, cybercrime, money laundering and child pornography.[64]

Aside from exceptions allowed by warrant, there is one further category of exceptions to the general prohibitions against interception, which are for only very specific circumstances where a warrant is not required. These special, warrantless exceptions include urgent law enforcement situations where there is a risk of loss of life or the infliction of serious personal injury or seriously injure another person serious or damage to property. Also, the suspecting that another party to the communication has take action that would may endanger his or her own life or create a serious threat to his or her health or safety.[65] The urgency of the need for the act to be done, it is not reasonably practicable for an application Access to communications data by carrier employees in the course as necessary for the performance of their job duties[66]

A. National Security

National security and law enforcement agencies are treated slightly differently under the provisions of the Amended TIA Act. The national security role for exceptions to the prohibition on interception has gained particular prominence in the post-9/11 era with concerns about terrorist activity.

Interception warrants for national security purposes may be issued to the Australian Security Intelligence Organization ("ASIO"). Warrants can be issued to ASIO by Attorney-General's to intercept communications "where the communications are being used by a person who is reasonably suspected of engaging in activities prejudicial to security, and the interception will, or is likely to, assist the ASIO in its function of obtaining intelligence relevant to security."[67] Interception warrants can also be issued to ASIO for accessing stored communications.[68]

---

[61] Tom Sherman, 'Telecommunications (Interception) Act 1979: Report of Review of Named Person Warrants and Other Matters' (Public Affairs Unit, Australian Government Attorney-General's Department,2003)
[62] TIA s 105 (2)
[63] Tom Sherman, 'Telecommunications (Interception) Act 1979: Report of Review of Named Person Warrants and Other Matters' (Public Affairs Unit, Australian Government Attorney-General's Department,2003)
[64] Attorney-General's Department, Telecommunications (Interception) Act 1979- *Report for the Year Ending 30 June 2005* Publication No 4321.
[65] TIA Act s 7(4)
[66] TIA Act s 7(5)
[67] TIA Act s 9 (a)
[68] TIA s 109

B. Law Enforcement

The issuance of interception warrants for law enforcement purposes is only to specified criminal law enforcement agencies for the purpose of investigating specified "serious crimes".[69] Therefore, the inclusion of law enforcement purposes among the permissible reasons for interception activity was a development of the 1979 TI Act.[70] This is evolution is discussed in greater detail in section 5.2, above.

7.3 Operation of Interception Warrants

In operation, despite the advancements and clarification made by the 2006 Amendment Act, the regulations remain subject to interpretation by law enforcement and the judiciary. There had been a degree of uncertainty about the conceptual basis and fundamental objectives of the legislation. On the one hand, In *Grollo v Palmer* judges explain that at least in part of TIA Act is designed to protecting of communication of privacy.[71] In contrast, some of the courts provides that the prohibition on interception and maintain national infrastructure telecommunications levels through protection against illegal interference more willingly than directly involved in the protection of privacy.[72]

Even after the implementation of the 2006 Amendments, "operators who are subjected to the access and interception regime are being faced with the increasing difficulty of acting in the spirit, but not to the letter, of the law in matters of law enforcement."[73] Nicholls and Rowland identify three key problems that typically arise in the implementation of the Amended TIA Act:

Existing practices by some law enforcement agencies rely on longstanding conventions, instead of following the letter of the law. For example, "warrants which have either expired, not been properly served, or are invalid for other fundamental reasons such as mis-naming the operator on whom is it purported to have been served. Frequently, warrants incorrectly cite the grounds on which access is being demanded."[74]

Law enforcement agencies do not fully appreciate technical limitations that need to be applied to a given intercept or access warrant, and submit requests that are too broad or undefined in scope. For example, "stored communications warrants that have been issued covering periods of over 12 months, seeking all SMS messages sent and received by any person in a particular city, containing any or all key words listed in the warrant including (by way of illustration only) 'Arab', 'building', 'suitcase' and 'car'."[75] Law enforcement officials do not fully comprehend the complexity and quantity of effort that such a request will engender, the fact that SMS messages are often purged daily, and the difficulty of gleaning meaningful data from it.

Additional implementation challenges arise due to the complicated regulatory, network, and contractual complexities under which telecommunications carriers operate. Nicholls and Rowland explain that "telecommunications operators understand that the nature of the industry requires a form and level of regulation not seen in other sectors, but inconsistent approaches to regulation and continually being made 'the fall guys' for the sake of a media grab does nothing to progress the carrier-law enforcement agency relationship."[76]

7.4 Type of Interception Warrants

The Amended TIA Act sets two types of interception warrants: firstly, telecommunications service warrant, which allows the interception of only one "service" at a time (e.g. one telephone number). The 2006 Amendment also states that warrant issue in relation to a particular telecommunications service that is likely to use by named individual.[77] The second type is named person warrant, which allows law enforcement to intercept more than one telecommunications service used by one person (a suspect).[78] For example, more than one telephone number,

[69] Electronic Frontiers Australia, *Telecommunications Interception and Access Laws* (2006) <http://www.efa.org.au/Issues/Privacy/tia.html#defin> at 3 November 2009

[70] Thomas Wong, 'Regulation of Interception of Communications in Selected Jurisdictions' (2005) *Research and Library Services Division Legislative Council Secretariat,Hong Kong*

[71] O'Malley v Keelty, Australian Federal Police Commissioner (2004) FCA 1688 at [2].

[72] Marriage of Parker and Williams (1993) 117 FLR 1

[73] Rob Nicholls and Michelle Rowland, "Lost in Transcription: The Australian Regime for Interception of, and Access to, Communications Content and Metadata", (2008) *Record of The Communications Policy & Research Forum held in Sydney, September 29-30, 2008,* Network Insight Institute, pp. 390-401

[74] Ibid

[75] Ibid

[76] Ibid

[77] TIA Act s 9

[78] TIA Act s 11(b)

email service(s), etc. The 2006 Amendment Act also defined "Equipment-based interception", that is, interception of communications made by means of a particular "telecommunications device"[79] that a person is using, or is likely to use.[80] In addition, the Explanatory Memorandum states:

A telecommunications device may be identified by any unique number including a telephone number for mobile phone handsets, a Media Access Control address for computer terminals, or an e-mail address. The definition of telecommunications number is inclusive so as not to limit the unique numbers which may be used to identify telecommunications devices, thereby maintaining a technology neutral approach to the regulation of telecommunications interception[81]

7.5 Duration and Authorization of Interception

Interception warrants are required to specify a time period for the warrant to be in force, up to a maximum duration of 90 days, except in the case of 'B-Party' warrants, in which case the maximum is up to 45 days.[82] However, Interception warrants issued to ASIO can have duration of up to a maximum of 6 months, unless they are 'B-Party' warrants, which have an ASIO limit of 3 months maximum duration.[83]

The ASIO is the agency coordinating national security warrants. Only designated criminal law enforcement agencies can apply for and be issued interception warrants for law enforcement purposes (Electronic Frontiers Australia 2006).

The TIA Act identifies two types of interception warrants as following:

1. Pt 2.2 warrants can be issued by Attorney-General[84] and Director-General to the Australian security organization for one of two purposes national security or law enforcement. The Director-General of Security may be issued national security that can be in force for no more than 48 hours in limited circumstances. Also, the Director-General of Security must make a request to the Attorney-General for the issue of warrant and the warrant can be revoked by the Attorney-General at any time before it expires.[85] Therefore, section 10 of TIA Act provides circumstances when issuing a warrant by Director-General of Security:
   a. the Attorney-General has not, to the knowledge of the Director-General of Security, made a decision with respect to the request and has not, within the preceding period of three months, refused to issue a warrant under section 9 in respect of the telecommunications service or under section 9A in respect of a person
   b. the Director-General of Security has not, within the preceding period of three months, issued a warrant under this section in respect of the telecommunications service or person; and
   c. the Director-General of Security is satisfied:
      i. that the facts of the case would justify the issue of a warrant by the Attorney-General; and
      ii. that, if the interception to which the request relates does not commence before a warrant can be issued and made available by the Attorney-General, security will be, or is likely to be, seriously prejudiced.[86]
2. Pt 2.5 warrants can be issued to federal and State law enforcement agencies by eligible Judges and the Administrative Appeal Tribunal (AAT) members.[87] Section 6 (d) states that the eligible Judge means a person who is a Judge of a court created by the Australian Parliament who is authorized to be nominated by the Minister and who had been declared Judge by the Minister to be eligible Judge for the purposes of this Act. Furthermore, a nominated AAT member who are eligible to issue interception warrant are Deputy President, full-time senior member, part-time senior member

---

[79] Telecommunications device means 'a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system'. See TIA Act s 5

[80] TIA s 9 (a)

[81] Telecommunications (Interception and Access) Amendment Bill 2006 – *Explanatory Memorandum*, circulated by the Australian Government Attorney General's Department, Canberra 2006. (Referenced as Explanatory Memorandum 2006)

[82] TIA Act s 50 (3)

[83] TIA Act s 9 (b)

[84] The Attorney-General is the minister responsible for police, legal affairs and the Australian Security Organisation (ASIO). The Attorney –General is appointed by the Prime Minister who is the leader of the party in the House of Representatives.

[85] TIA Act s 10 (a)

[86] TIA Act s 10

[87] TIA Act Pt 2.5

and member AAT.[88] Part time senior or members are not eligible to issue interception warrant unless the person is qualified as Deputy President.[89]

The High Court of Australia in *Grollo v Palmer*[90] provides:

> The applicant does not assert that, as a result of their duties under the Act as personae designate, the judges of the Federal Court in fact lack independence or would be unable to perform their duties impartially. But the independence and impartiality of those judges is not an answer to the applicant's case. The question is not whether the impartiality and independence of federal judges make them appropriate persons to authorize the issue of telephone interception warrants. The question is whether, in the light of the separation of powers mandated by the Constitution, the functions that an "eligible Judge" performs under the Act are functions that are compatible with the exercise of federal judicial power by those judges.

The Attorney-General issues authorization to the various State/Territory agencies designating them as allowed applying for warrants. In order to be authorized by the Attorney- General the State/Territory must have its own legislation in place imposing supervisory and accountability provisions parallel to the federal guidelines outlined in the Amended TIA Act.[91]

The application procedures for national security warrant must be made by Director-General of Security ASIO, while that the eligible agency may apply for interception warrant shall be made on agency's behalf by:

1. Australian Federal Police;
2. Australian Crime Commission;
3. New South Wales Police;
4. New South Wales Crime Commission;
5. Independent Commission Against Corruption;
6. Police Integrity Commission;
7. South Australia Police;
8. Victoria Police;
9. Western Australia Police;
10. Western Australian Corruption and Crime Commission; and
11. Tasmania Police.[92]

The issuing of warrant for national security in relation to a named person or a telecommunications service recognise in TIA Act as following

> (a) the attorney-General may issue warrant in admiration of a person is engaged in or rationally suspected of being engaged in activities prejudicial to national security; or
>
> (b) the Attorney- General satisfied that foreign intelligence to be obtained is significant to the defence of Australia or to the conduct of Australia's international affairs.93At the same time, law enforcement warrants must be issued for investigation serious offences.94 Serious offences include but are not limited conducts involving an act of murder, terrorism, narcotics offences and Kidnapping.95 Also the TIA Act provides offences that are punishable by imprisonment for period of life or for life or maximum period of at least seven years96 such as loss of life or serious injury, serious property damage, corruption, tax, serious fraud, money laundering and child pornography.97

[88] TIA Act s 6 (DA) 1
[89] TIA Act s 6 (DA) 2
[90] Grollo v Palmer (1995) 184 CLR 348; 82 A Crim R 547.
[91] TIA Act s 35
[92] Attorney-General's Department, Telecommunications (Interception) Act 1979- *Report for the Year Ending 30 June 2005* Publication No 4321.
[93] TIA Act s 11 A,B and C
[94] The Amendment TIA Act 2006 removed the difference between class 1 and class 2 offences- both classes of offencesbecome serious offences
[95] TIA Act s 5 D
[96] Attorney-General's Department, Telecommunications (Interception) Act 1979- *Report for the Year Ending 30 June 2009.*
[97] TIA Act s 5 D

8.0 Telecommunication Interception and Access Law in Arab Countries

Arab countries are a developing country. In the last few years, the adoption of technology in Arab society has doubled. This is despite the fact that the number of internet users is still restricted to a mere 4.6% of the population (in 2006).[98]

As a result, the lack of internet usage and other telecommunications facilities in business or for other purposes has resulted in a degree of negligence with respect to national security. Therefore, the internal security issues related to the establishment of secure local conditions and the reservation of good relationships with other countries indicates, in addition, the necessity of introducing new technological systems that allow control over usage of telecommunication tools in Arab Countries in a way that makes it secure for citizens and controlling the security issues inside the countries.

Arab Countries does not have *telecommunication interception and access statutes*. There is no writing on the issue of a law relating to *telecommunications interception and access.* There is also no analysis of the specific topic presently under examination, *telecommunication interception and access law Arab Countries*. However, Lebanon the first country enactment interception law in 2009.

Jordanian Constitution Act Article 18 stipulates that "all postal, telegraphic and telephonic communications shall be treated as secret and as such shall not be subject to censorship or suspension except in circumstances prescribed by law." Consistent with human rights reports, security officers monitor internet communications and telephone conversations, conduct surveillance and read private mail of persons who are considered to pose a threat to the government or national security.99

On the other hand, the Telecommunication Act provides that “telephone calls and private telecommunications shall be considered confidential matters that shall not be violated”100 and “any person who intercepts, obstructs, alters or strikes off the contents of a message carried through the telecommunications networks or encourages others to do so, shall be punished by imprisonment or fine.”101

Similarly, any person who “spreads or discloses the content of any communication through a Public or Private Telecommunications Network or a telephone message which came to his knowledge by virtue of his post, or records the same without any legal basis, shall be punished by imprisonment, fine or both”.102

In addition, the Telecommunication Act provides that any person who “withholds a message … copies or reveals a message or tampers with the data related to any subscriber, including unpublished telephone numbers and sent or received messages shall be punished by imprisonment, fine or both.”103

Bahrain's Telecommunication Authority has issued a policy in relation to telecommunication interception and access; this policy aimed to impose restrictions on companies such that they maintain records of all telephone calls and email communication, VOIP (Voice Over IP) and all website accessed by all citizens and residents in Bahrain for the last three years on the basis of national security concerns. This policy, however, from the Telecommunications Authority was never submitted for due process by the Bahraini Parliament. The policy has never even been discussed by members of the Bahraini Parliament.

Lebanon was the first Arab country to enactment a telecommunication interception regime in 1999 which did not come into force until 2009 when the Lebanese Cabinet finally adopted the Act. The Lebanese Telecommunication Interception Act aims to prevent abuse by and assault on the freedom of private citizens. Article 1 of the telecommunication interception Act provides “all postal, telegraphic and telephonic communications shall be treated as secret and as such shall not be subject to intercept or suspension except in circumstances prescribed by law “.104

The Act regulates the interception and access to telecommunications by requiring such conduct be based on judicial or administrative decisions.

On the other hand, Morocco has enacted amendments to the criminal law by adding articles containing telecommunication interception provisions. Morocco has attempted to balance its new articles by controlling offensive activities whilst protecting national security. The amendments were enacted by the addition of 8 articles regulating telecommunication interception and the entities that provide them by requiring such entities obtain a note to get permission to intercept or access telecommunications as well as the time limit for listening. Furthermore, the offence being investigated should also be serious crimes.

---

[98] Jordanian Department of Statistics, (2007) Information Technology use at home survey <www.dos.gov.jo> at 8 August 2008

[99] US State Department Human Rights Report 2006 - Jordan, at <http://www.state.gov/g/drl/rls/hrrpt/2006/78855.htm>. 28 February 2009

[100] Jordanian Telecommunication Law(1995) S 56

[101] Ibid at S 76

[102] Ibid at S 71

[103] Ibid at S 77

[104] Lebanon telecommunication Act S 1

In Egypt there is considerable controversy about telecommunication interception. Recently the Egyptian Minister of Communication, Dr. Tariq Kamel, noted that the ministry would allow security agencies to intercept telecommunications.[105] This stance has provoked unrest in relation to such interceptions. Critics have noted that article 64/2 of the Telecommunications Act in Egypt permits the security authorities to intercept telecommunications only when approved by a competent court. On this basis the role of the Public Prosecutor in Egypt is the protection of general privacy and the privacy of citizens and balancing the requirements of national security.

9.0 Conclusion and Recommendation

The advancement in telecommunication during the last decade has required many countries to amend their laws or the enactment of new laws to address these developments. After 11 September, 2001 Australia and other developed countries responded to these calls and started to apply communication interceptions to protect their strategic interests. Communication interceptions raised wide objection through the organizations of human rights worldwide. Many of these organizations have shown that the interception of communication violates human privacy. However, Australia has been balanced away from privacy protection to allowing Law Enforcement Agencies to obtain access to such telecommunication for the purpose of national security and public security.

Arab countries have regulated telecommunication industries and have amended their regulations many times. Arab countries need, however, to introduce new technological systems that allow control over usage of telecommunication tools to follow developed countries such as Australia that make it secure for citizen whilst balancing the security needs inside the country. This can be accomplished through the introduction of a telecommunication interception and access Law that will also protect national economic interests from any potential threats (internal and external).

Arab countries still lack telecommunication legislation or have not yet amended their current laws to include interception and access to telecommunication in terms of the legal aspects and issues raised. This paper seeks to help Arab countries fill a significant gap in existing knowledge and go some way towards designing a new regulatory system for telecommunications interception and access law in the Arab World. The recommendations set below are intended to clarify the path that those countries could follow to achieve their stated goals.

Recommendations

- Arab countries should first ensure that privacy protection is a core consideration in all activities. For any legislation providing interception and access to telecommunication for security and law enforcement purposes.

- Arab countries should ensure that the implementation of telecommunication of interception and access law covers serious offences connected corruption or organised crime.

- The legislation adopted by Arab countries should place a condition on Carriers that before any signals or data is intercepted; a licence should be required by government agencies (law enforcement and national security agencies).

- All government officials in Arab counties should require a warrant from the court before obtaining call data from carriers. Whether or not the call data was related to an interception warrant. Also a warrant should be required when government officials seek to store accessed communication data.

- Carriers in the Arab countries should be aware of the initial cost of obtaining an interception capacity. Also the governments of Arab countries should allow the carriers to recover the cost on a commercial basis that is itself based on an agreement worked out between the carriers and the government agency seeking interception of communication data or signals or the capacity to access and intercept data or signals.

[105] www.alarab.com.qa/detaials

- In order for Arab countries to build a new telecommunications technology infrastructure they should support the development of new international user requirement standards setting an international benchmark for telecommunications interception and access facilities.

- Arab Government officials should closely monitor international developments in encryption and its control, and government agencies should monitor the use of encryption by interception targets.

- Arab countries should become active and have a general role in organizing and addressing international considerations related to interception and access issues associated with new technology.

- Arab governments should also develop standard procedures for carriers as to what is required under the licensing conditions applicable to government agencies.

- Arab countries should invite and encourage the telecommunications equipment suppliers to participate in consultations on new technology and its interception and access implications.