INTERNATIONAL REVIEW OF LAW

OPEN ACCESS

Research article

The "Right to Privacy" v. telecommunications interception and access: International regulations and implementation in the Arab Region

Yaser Khalaileh*, Nazzal Kisswani

College of Law, Qatar University, Doha, Qatar
*Email: khalaileh@qu.edu.qa

ABSTRACT

The right to privacy is a complex and controversial issue. Concerns pertaining to the 'Right to Privacy' have often become a stumbling block when preparing draft laws on telecommunication, specifically those that relate to governmental interception and access, and can prompt governments to cancel the drafting of the law. Governments attempting to defend the right to invade citizens' privacy in communication, whilst at the same time adhering to international obligations, habitually have to face opposition. Recently though, the dual concerns of national security and public security have repeatedly been used as tools to shift away from privacy protection toward allowing telecommunications interception and access by governments when needed.

Some Arab states have enacted interception and access laws, but only in an intermittent fashion, making it difficult to refer to it as a complete template for implementing an interception and access law. It is accepted that new, hi-tech systems are required to regulate the use of telecommunication tools so as to be in line with developed countries. The Arab states seem to be behind in introducing telecommunication legislations, or at least have not amended their laws to comprise interception and access in telecommunication. These states should be directed to securing a balanced approach between the rights of citizens and the necessary security needs.

This paper seeks to outline the gaps in existing legislative order in Arab countries. It also attempts to draw some guidelines towards introducing effective regulatory systems for telecommunications interception and access law in the Arab world.

Keywords: international law, privacy, national security, interception law, access to communication, human right

http://dx.doi.org/10.5339/irl.2013.10

Submitted: 27 April 2013
Accepted: 29 August 2013

QSCIENCE.com
Member of Qatar Foundation

Cite this article as: Khalaileh Y, Kisswani N. The "Right to Privacy" v. telecommunications interception and access: International regulations and implementation in the Arab Region, *International Review of Law* 2013:10 http://dx.doi.org/10.5339/irl.2013.10

1. INTRODUCTION

Inarguably, technological advancements have been the prime feature of the past century and the leap into the twenty-first century. Instantaneous communication is the most obvious gift of all. Unfortunately however, this also means, for some, an accessible tool to direct terrorism and other destructive criminal activities. From this perspective, one may not be surprised to learn that many Western governments have in fact taken severe proactive measures in attempting to prevent the use of telecommunications for covert terrorist planning. Whether these measures have been prolific, is a different matter. Indeed, critics are increasingly questioning the validity of this approach, especially because of human rights concerns.

Concerns regarding undesirable use of telecommunication, balanced against the right to privacy, abound at both national and international level. The absence of a clear definition on the extent of privacy has made it considerably difficult for States to produce a concise regulation on free communications. The events of 9/11 represent the date when serious rethinking of the legal and personal implications of monitoring individuals communications on grounds of ethnicity, race and religion, began. In an allegedly democratic world, such an extreme change of methodology is perhaps unacceptable from a human rights perspective, and the hopes were to produce legal principles duly as a reflection of democratic principles.

This paper looks at the issue of privacy when undermined by the state's use of monitoring methods. The objectives are to identify a proper definition for privacy; to consider this issue from a telecommunication standpoint; to analyse the influence of interception and access law, if any, on privacy; and finally the importance of providing a suitable balance between privacy and security. We present this through a review of the main concepts provided for in international law. To illustrate the current trends in securing a balanced nexus between the right to privacy, and the fight against international crime, it is imperative to first have a firm understanding of what constitutes a right to privacy.

2. THE DEFINITION OF PRIVACY AND CURRENT ORTHODOXIES

2.1. Definition and importance

Privacy interests are as old as civil society. Scholars normally quote 1890 Warren and Brandeis in describing the early understanding of the right to privacy as simply being "the right to be let alone".[1] This right has been recognised as one of the most fundamental human rights worldwide, and "has become one of the most important human rights of the modern age".[2] Gross defined privacy as "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited", and that "a legal right of privacy exists to the extent that such legal interest may be accorded protection by legal procedures".[3] Bloustein, describes privacy as an interest of the human personality and to protect the individual's personality, independence and it includes dignity and integrity.[4] Westin describes the concept of privacy as a "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[5] Westin goes further in explaining that "viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy, or, when among larger groups, in a condition of anonymity or reserve".[6]

Posner acknowledges the complexity of the privacy issue and that, as a word, it is of many meanings, one of which concerns telecommunication issues in today's world, and is normally referenced to as 'secrecy'.[7] On an individual basis, secrecy is manifested with people's attempts to conceal information

[1]Bashar H. Malkawi, *The information age and privacy protection in Jordan*, 17 Computer& Telecomm. L. Rev. 186, (2007) (citing Samuel Warren and Louis Brandeis, "The Right of Privacy" 4 Harv. L. Rev. 193, 195–96 (1890)).

[2]Marc Rotenberg, Cedric Laurant, et al., *Privacy and Human Rights 2005: An International Survey of Privacy Laws and Developments*, Washington DC: Electronic Privacy Information Center, http://gilc.org/privacy/survey/intro.html#invasion. (accessed October 22, 2013).

[3]Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. Rev. 34, 36 (1967).

[4]Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 971 (1964).

[5]Alan Westin, *Privacy and Freedom, (*New York, Atheneum, 1967) p. 7, definition at: http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_11.pdf (accessed October 22, 2013).

[6]*Id*. at p. 7.

[7]Richard Posner, *Privacy, Surveillance, and Law*, 75 The University Chicago Law Review, 245, 245 (2008).

about themselves for a variety of reasons, most importantly information that may cause embarrassment or grievance, such as age, physical and mental health or criminal records.[8] Posner suggests that the concealment often aids clear communication e.g., in telephonic conversations, where people do not have the fear of outside infiltration. Accordingly, speech flows freely and the danger of misunderstanding is minimised. However, when there is fear of intrusion into private conversation, the tendency is to be somewhat more guarded in speech, with a concomitant lack of clarity between the conversationalists.[9] This is almost like preserving the right to privacy in a Catholic confession or a medical consultation. Here, clients will simply feel free to speak when assured that the information disclosed by them will remain confidential in the interest of the best possible treatment. No doubt, taking such privacy away would be a severe detriment to the mental, spiritual and physical health of such persons, and should be justified by law.[10]

In a wider social sense, Posner ascertains that the ability to speak freely has an indispensable value in alleviating the sense of becoming susceptible to unwanted attack. Promoting competition amongst colleagues in a firm's innovative process, which would probably require secretive strategic plans, becomes weakened if communication privacy is not protected.[11] Corporations should be able to initiate innovative designs and ideas without having to disclose these to their rivals – a matter that directly affects the development of the country's economy.

2.2. Privacy in telecommunication

Privacy in today's technology has become significantly complex, and definitions that have previously defined the concept of privacy, in relation to communication, have changed. In 2001, the 9/11 attacks made telecommunication privacy issues even more controversial, with governments attempting to advocate their own right to invade this privacy, and devalue demands of human rights groups advocating against this.

Although the horror of 9/11 has somewhat decreased, the concern with communication privacy remains, along with concomitant human rights concerns.[12] According to Posner, "People hide from the government, and the government hides from people, and the people and government have both good and bad reasons for hiding from the other".[13] A demand for transparency from the government, however appealing, should also be thought of in terms of its ability to make deterring plans and actions in the face of organized crimes. On the other hand, complete opacity is certainly not advantageous for the citizen-government relationship. Indeed, liberty and security are both at risk should the government maintain complete secrecy from the people. Similarly, taken from government's viewpoint, complete privacy may simply mean more room for terrorism to flourish, seriously hampering the government's ability to protect its citizens.

In light of the current exponential rise of computer technology, and the capability of governments to store vast quantities of digital information within seconds, the free speech rights provided for in many constitutions may well be hampered. By the same token, discouraging the free exchange of ideas among potential terrorists would also discourage terrorism. The latter is immensely important in relation to protecting innocent citizens. Governments are therefore under the pressure to convince the public that 'loosening the tie' for some rights is perhaps advantageous in retaining a certain way of life. It is simply, as Ware has noted, citizens' privacy rights dictate that information must be protected against surreptitious acquisition by unauthorised parties.[14] For instance, the Federal Government of Australia requested that the Australian Federal Police investigate internet giant Google over alleged privacy breaches.[15] Stephen Conroy, the Australian Communications Minister, in addressing the

[8] *Id.* at 249.
[9] Ib at 246.
[10] Patrick Breyer, *Telecommunications Data Retention and Human Rights: the Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 Eur. L. J. 365, 368 (2005).
[11] *Supra*, note 7 at 246.
[12] *Supra* note 10, at 369–79. Also *see* Nancy Benac and Jennifer Agiesta, *Post-9/11 Security Privacy Balance Remains Elusive*, The Meadville Tribune, http://meadvilletribune.com/local/x1078456243/SUNDAY-ISSUE-Post-9-11-security-privacy-balance-remains-elusive (accessed October 22, 2013).
[13] *Supra* note 7. at 246.
[14] Willis H. Ware, *Impact of Telecommunications Technology of the Right of Privacy*, 8 Computer Soc'y. 2, 5 (December 1977).
[15] Kristen Gelineau, Australia Launches Privacy Investigation of Google. USA Today (2010) http://usatoday30.usatoday.com/tech/news/internetprivacy/2010-06-07-australia-google_N.htm (accessed October 22, 2013).

Australian accusations, said that Google was responsible for the "single greatest breach in the history of privacy".[16] The boundaries of privacy seemed to be the concern in this case.

It is also imperative to acknowledge that modern technology has facilitated many social and financial systems. It is now possible, for example, to initiate an instant communication, for a very low cost, with people across the world. Payment and credit systems are simplified to a large extent and often facilitate many global expansion ventures, even enabling those who have previously been excluded to become part of local and foreign exchange businesses. For example, airline and hotel reservation systems, social security administration networks and the payments-exchange mechanisms have all been a worldwide facilitation. These systems, that depend innately on technology, allow a free flow of information and records about users. Although strict security measures are usually in place for such systems, the increased access and availability of electronic records makes them nonetheless vulnerable to improper use. It is true that passwords and other security prerequisites have developed to protect private information, yet the issue here extends to users who could be governmental officials with multi-access rights, or even the rights of the government to access private electronic information.[17]

In this regard, Reidenberg asserted that the movement of computer technology – from being largely institutionalised to becoming personal – has largely decentralised the use, creation, collection and processing of personal information.[18] According to Reidenberg, "the sale of personal information alone [in the United States] was estimated at $1.5 billion in 1997".[19] Bearing in mind the increasing pace of online sales, it would be essential for fair economic practices to ensure the protection and privacy of citizens making use of online services, as well as for the sake of ensuring a healthy development of electronic commerce across the world.[20]

With technology advancement, one difficulty arises when countries try not only to optimize, but also to standardize their legislation regarding the protection of personal and electronic information. For instance, US policy seems to confer a degree of personal information protection according to a market-dominated paradigm, whereas limited statutory and common law rights are granted for information privacy.[21] In contrast, the privacy protection norm in Europe is dominated by virtue of privacy rights. The EU, for example, compels its member states to embrace a comprehensive statutory protections for its citizens when it comes to privacy rights.[22]

One more complication with the increasing electronic flow of information is seemingly global. The divergent national norms and statutes confronting one another more frequently, specifically where privacy protection is concerned. National responses to the issue of terrorism constitute a further complicating factor. This has increased international policy confrontations regarding privacy protection for citizens, with the initiation of prolonged international negotiation that only produced a compromise known as the 'Safe Harbor' agreements.[23] According to this compromise, relaxed privacy requirements to protect EU citizens substituted the stringent ones to match the more lenient requirements by the US, in the hope that more electronic commerce between the EU countries and the US will be facilitated.

It is apparent that whereas the EU operated on the basis of concluding privacy rights for citizens, other countries, such as the US, tend to focus on a more government-centric view. The latter stresses that national security, and politics in general, dictates privacy law norms. The years that followed the 9/11 incident have magnified this trend, mainly in political forums, while remaining controversial in e-commerce arenas.[24] As such, privacy advocates, and citizens in general, are now vehemently concerned with the electronic surveillance paradigms in the US, with an increased public distrust in electronic devices used by the law enforcement agencies (LEAs) for electronic surveillance of suspects. The Carnivore system created by the FBI, which was created to intercept and collect electronic

[16] *Id.*
[17] *Id.*
[18] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315, 1317 (2000).
[19] *Id.*
[20] *Id* at 1317–18.
[21] *Id* at 1331.
[22] William J. Long & Marc Pang Quek, *Personal Privacy Protection in an Age of Globalization: the US-EU Safe Harbor Compromise*, 9 J. Eur. Pub. Pol'y 325, 331 (2002).
[23] *Id* at 327–28.
[24] Kimberly A. Horn, *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet* Age, 29 Fordham Urban Law Journal, 2233, (2002). Horn addressed some of the issues that created a controversy in terms of the conflict between privacy rights and security after the 2001 attacks.

communications where criminal activity was suspected, has in itself become the focus of this distrust. The governmental justification for the new system was that criminals are becoming increasingly sophisticated in their use of the internet for illegal activities, and therefore, to counter this, Carnivore is installed on a computer network, to capture and store information running through these networks.[25] What is alarming however, is that the Carnivore system has been in existence since 1997 but only became known to the public in 2000.[26] As such, many of the arguments that were made to reason the use of surveillance systems, and providing the 9/11 incident as justification for such use, could well be out of context.

3. INTERNATIONAL LAW PARADIGMS AND THE RIGHT TO PRIVACY

Doubts around the effectiveness of public international law have been thwarted by assuming that the subjects of this realm of law have exceeded the classical notion of states. Human rights movements during the end of the last century have lent themselves forcefully to see certain rights maintained. The principle of internet freedom and the principle of privacy, alongside a modified principle of territorial jurisdiction adapted to cyberspace, have become clearer propositions.[27] The relevance of these, and specifically how these principles regulate the interrelationship between different actors, is evident.

3.1 The principle of privacy in international law

Privacy is a fundamental human right recognized in the 1948 Universal Declaration of Human Rights (UDHR), the 1966 International Covenant on Civil and Political Rights (CCPR), and in many other international and regional treaties. This principle reinforces human dignity and other pertaining values such as the freedom of association and the freedom of speech. It has indeed become one of the most important human rights issues of the modern age.

Article (17) of the CCPR provides for the protection of individual's privacy. This entails ones' family and home, individuals' correspondences, honour and reputation. Equally, article (8) of the European Convention on Human Rights (ECHR) states for both private and family life, as well as home and correspondence. Both provisions were broadly utilized and developed by the European Court of Human Rights. In Kennedy v. the United Kingdom, the ECHR did not distinguish between private life and correspondence, and as such, emails were considered a protected correspondence according to these articles.[28] On the other hand, data transmitted through the internet were considered an annexation of the person's private life, unless it is intended to be for public access. Accordingly, the European Court on Human Rights had no worries in suggesting that the employee's use of internet and correspondance is simply an extension of their private life.[29] In conclusion, state control over private internet use and content including emails amounts to an unwanted interference. By analogy, the same would be true for internet providers in attempting to store internet data, as is provided for in Article (3) of the European Directive 2006/24/EC.[30]

The European Court of Human rights in Wypych v. Poland has also dealt with the issue when public authorities publish information that have an effect of compromising the rights of persons who may or may not use the internet, or when there is a legislative imposition to publish such information with the result of interfering in private lives.[31]

Related obligations in this context can also be deduced from Article (17/2) of the CCPR, which provides for the right to legal protection against interference with one's privacy, and the proper protection that should be accorded to individuals. A positive obligation can be found in Article (8)

[25] *Id* at p. 2234.
[26] *Biting into Carnivore*, San Diego Union-Trib., April 1, 2002, at E3.
[27] For an overview of the internet freedom in the Arab World, *see*: Khaled Hroub, *Internet Freedom in the Arab World: Its Impact, State Controls, Islamisation and the Overestimation of it All*, Culture and Society, Development and Cooperation (2009) http://www.iemed.org/anuari/2009/aarticles/a267.pdf (accessed July 7, 2013).
[28] *Kennedy v. the United Kingdom*, application No. 26839/05, ¶ 113 (ECHR May 18, 2010) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-98473 (accessed October 22, 2013). *See Liberty et al., v. United Kingdom*, application No. 58243/00 ¶ 56 (ECHR July 1, 2008) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207 (accessed October 22, 2013).
[29] *Copland v. United Kingdom* - application No. 62617/00 ¶ 41 (ECHR April 3, 2007) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996 (accessed October 22, 2013).
[30] European Parliament and Council Directive 2006/24 of 15 March 2006, O.J. 2006 L 105/54 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services.
[31] Eur. Court H.R., *Wypych v. Poland*, Judgement of 25 October 2005, Application 2428/05.

of the ECHR, and even though the ECHR does not contain a similar specification, the European Court of Human Rights has derived a positive obligation.[32] Because internet privacy is not only threatened by public authorities, but also by private persons and enterprises who are able to store large amounts of private data that can harm individuals, it becomes a vital duty of the state – and therefore an obligation – to protect privacy.

According to the imperativeness of securing the right to privacy, one can notice that nearly every country in the world has, to a varying degree, recognized the right of privacy in its respective constitution. Provisions, at the very least, have made a specific mention to the right of inviolability of one's home and the secrecy of communications. For example, the constitutions of Hungary and South Africa include specific prohibitive provision for the right to access and control one's personal information. In other countries that did not explicitly include the right to privacy in the constitution, such as the United States and India, their respective courts have impinged this right in other provisions. Other countries have incorporated international agreements that recognize privacy rights, such as the CCPR or the European Convention on H.R., into their laws.[33]

Besides constitutions, the early 1970s witnessed the start of adoption of specific laws akin to the right of privacy by various countries. Broad laws were made and intended to protect individual privacy. Most of these laws were, in fact, a reflection of the model that was introduced by the Organization for Economic Cooperation and Development (OECD) and the Council of Europe. In 1995 however, the shortcomings of both of these laws was apparent, and the various levels of protection accorded by them varied in each states. Therefore, the European Union passed its directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" so as to set a benchmark for national laws, which each EU state must abide by and incorporate into their domestic laws.[34]

Despite all of this, the concept of privacy in today's world has made a vicious detour. Technology has become significantly more complex, and indeed, the very definitions that have previously been connected to the concept of privacy in relation to communication have changed. After 9/11, privacy was the subject of controversial dialogue between governments, a few of whom started to believe that their own right to invade the communication privacy of citizens no longer contravenes basic human rights principles. Groups advocating against this, struggled in convincing governments that such extreme measures were unnecessary.

3.2. The principle of internet freedom

This principle is tightly entrenched in international human rights law and is evolving rapidly. Indeed, freedom of expression is core in attaining the freedom of the internet. Article 19/2 of the CCPR guarantees this freedom of expression on an international level.[35]

On a European level, Article (10) of the European Convention on Human Rights attempts to confer guarantees to the corresponding rights.[36] The European Court of Human Rights in Times Newspaper Ltd. v. United Kingdom, found that internet archives fall within the reach of Article (10) ECHR.[37] On an international level, Article (19/2) of the CCPR expressly refers to expression "through any ... media of his choice" and therefore expressly protects expression through the internet.[38] As such, it is fair to assume that information and ideas expressed on a webpage shall fall within the scope of both Article (10) ECHR and (19/2) of the CCPR.[39]

---

[32] *See Marckx v. Belgium*, application no. 6833/74, p. 257 (ECHR December 13, 1979) (obligation to protect private life requires a court to actively determine what is private live and prevent governement interference). *See also*, Robert Uerpmann-Wittzack, *Personal Rights and the Prohibition of Discrimination*, in European Fundamental Rights and Freedoms, 67, 76 (2007).

[33] David Banisar & Simon G. *Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 Journal of Computer & Information Law, 3 (1999).

[34] *Id* at p. 4.

[35] Covenant on Civil and Political Rights, 999 UNTS, 171, 178 (1966).

[36] Convention for Protection of Human Rights and Fundamental Freedoms, Council of Europe Treaty Series No. 5, http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm / (accessed March 5, 2013).

[37] Times Newspapers Ltd v. United Kingdom – applications Nos. 3002/03 & 23676/03, ¶ 37 (ECHR March 10, 2009) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91706 (accessed March 5, 2013).

[38] 999 UNTS at 178.

[39] *Perrin v. United Kingdom*, application no. 5446/03 (ECHR October 18, 2005) (prohibitions against a obsenity on a web page examined under CCPR Article 19/3 of the CCPR and ECHR 10/2) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-70899 (accessed October 22, 2013).

It appears that, despite the clear provisions in favour of the right to privacy outlined in the previous section, and the case law that empowers certain standing, a logical deduction may be the possibility of having two recognized international concepts negating one another. On one hand, we have manifested the right to privacy for all, on the other a conflict might rise in the face of the freedom of internet and the flow of communication. In this case, legal and factual circumstances might well be the basis for realizing any of the two conflicting principles.[40] Against favouring internet freedom, the European Court of Human Rights admitted the significance of state control in Megadat.com v. Moldova.[41] Likewise, Articles (19/3) CCPR and (10/2) ECHR mirrors this structure containing ingredients of the legitimate aims that could possibly justify any interference, to include certain interests and rights of others, national security, morals and preserving the public order. Accordingly, and in cases of conflict, a fair balance ought to be struck between the competing interests.[42] The 'necessity test' laid down in Articles (19/3) CCPR and (10/2) ECHR is perhaps a realization of this balance, which simply necessitates that the interference should be proportionate to the legitimate aim pursued.[43]

In conclusion, an approach of restricting any one thing in favour of the other should be recognized by governments working on securing the freedom of communication as well as according a fair ground in favour of the right to privacy.[44] It appears that applying any restriction must be proportionate to the aim pursued. In fact, criminal sanctions should also be imposed in case of infringement when an individual is seriously affected.[45]

3.3. The limits of territorial jurisdiction and impact on privacy

So far, the above is mainly related to the duties imposed on states, as a reflection of the obligations set in human rights norms, that limit their scope of surveillance actions in favour of a better guarantee of individual privacy freedoms. These duties are mainly negative, i.e., disallowing state intervention in private individual concerns. It would therefore be reasonable to discuss the issue of privacy when such interventions are made by a foreign state, whether they are imposed with prior knowledge of the national state or not.

The debate on domestic jurisdiction over internet content located on servers abroad is controversial.[46] Any rational debate over this, would first acknowledge the well-established principle of 'territorial jurisdiction' as is known in public international law.[47] According to Article (2/1) of the UN Charter, a regime of sovereign equality between all members of the UN has to be respected. The rules of jurisdiction deal with the relationship between states, whereby the jurisdiction of one state finds its limits with relation to the jurisdiction of another. Accordingly, the state's exercise of jurisdiction over its nationals, their property and any event within its national boundaries requires a genuine link between them.[48] However, one has to stress the arguments provided in modification of this general proposition, specifically in terms of the jurisdiction of a state when cyberspace is concerned. The 'effect doctrine' gives jurisdiction to foreign states over acts allowing it to proclaim extra-territorial jurisdiction, provided that the effect of these acts extends beyond the national space and territory.

---

[40] Robert Alexy, *A Theory of Constitutional Rights*, Oxford University Press, at pp. 47–48, (2002).

[41] *Megadat.com SRL v. Moldova*, application no. 21151/04 ¶ 68 (ECHR April 8, 2008) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-85732 (accessed October 22, 2013).

[42] *Von Hannover v. Germany*, application no. 59320/00 ¶ 57–58 (ECHR June 24, 2004) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853 (accessed October 22, 2013).

[43] Dirk Ehlers, *General Principles, in European Fundamental Rights and Freedom* 25, 53 (2007).

[44] For an overview of the internet freedom in the Arab World, *see*: Khaled Hroub, 2009. Supra note 27.

[45] *K. U. v. Finland*, application no. 2872/02 ¶ 43 (ECHR December 2, 2008) available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964 (accessed October 22, 2013); *X and Y v. the Netherlands*, application no. 8978/80 ¶ 27 (ECHR March 26, 1985) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57603 (accessed October 22, 2013).

[46] Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007).

[47] *Banković and Others v. Belgium and Others*, application no. 52207/99 ¶ 59 (ECHR December 12, 2001) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-22099 (accessed October 22, 2013); *In re S.S. Lotus*, Collection of the Judgments of the PCIJ Series A, No. 10, 1, 18 (PCIJ 1927); *See* Ian Brownlie, *Principles of Public international Law*, 299 (2008).

[48] *See generally*, on the principle of effectiveness, Sergio Marchisio, *National Jurisdiction for Regulating Space Activities of Governmental And Non-Governmental* Entities, UN/Thailand Workshop on Space Law, Activities of State in Outer Space in Light of New Developments: Meeting International Responsibilities and Establishing National Legal and Policy Frameworks, November. 16–19, at p. 1 (2010), http://www.oosa.unvienna.org/pdf/pres/2010/SLW2010/02-02.pdf (accessed October 22, 2013).

Article (22) of the 2001 European Convention on Cybercrime approves the classical principle of territorial jurisdiction. Sub-Article (22/1/a) states that "each contracting party establishes jurisdiction over offences committed on its territory". Classically, an offence is deemed committed at the place where the perpetrator acted. So, if a person downloads harmful content, such as pornography on a website, the state where the acts were concluded may have the right to intervene. Yet, it is also accepted that where the effect of the criminal activity is felt abroad, an objective territorial principle might also apply. The Council of Europe Committee of Ministers also confirmed the effects doctrine in its comment on Article (22) ECC by stating that a state should not only "assert territorial jurisdiction if both the person attacking a computer system and the victim system were located within its territory", but also "where the computer system attacked is within its territory, even if the attacker is not."[49]

Whilst the genuine link between the attack and the state is easily determined in cases where the computer used is related to where it has been used, the situation is less clear when harmful content is published through the internet through a webpage accessible from any point of the world. Here, harm could be established by the simple viewing of a webpage with harmful content from one's office desk. Accordingly, courts decisions have made it clear that in such circumstances, a genuine link between the state and its citizens has been established, allowing courts to admit such dispute as falling in their competencies. As such, British courts convicted a French national of publishing obscene material on a US website because a police officer had viewed it in a London police station.[50]

Although the extra-territorial jurisdiction is a widely accepted norm by both courts and scholars,[51] there have been nonetheless different attempts to restrict the 'effects doctrine' taking into account the ubiquitous nature of cyberspace. US courts, for instance, relied on reasonableness according to the effects doctrine.[52] It is to be noted here, however, that court's practice throughout the world is not uniform on this issue. Yet, a strong tendency to use several criteria in order to determine whether a webpage has a sufficient link to a given country is also apparent. These include the language, the content and the publicity of the webpage, as well as whether web content is intended to be retrieved by a targeted country, or from a specific country. This would simply allow the intended country to have a good claim to jurisdiction.[53]

It is to be noted here that making use of an unqualified application of the 'effects doctrine', though simply infringing the territorial sovereignty of other states, as outlined above, would nonetheless negate another fundamental principal of 'internet freedom'. In fact, Articles (19/2) of the CCPR and (10/1) of the ECHR on the freedom of expression 'regardless of frontiers' would be devalued if content providers had to block access for foreign users for fear of being sued or prosecuted abroad. Here, a logical juncture of making a fair balance between the conflicting principles of territorial jurisdiction and internet freedom is feasible. In essence, a qualified effects doctrine based on the idea of reasonableness might just be closer to this vital balance.

Finally, it is to be noted that the concept of 'territorial jurisdiction' encompasses the state's country code Top Level Domain (ccTLD) which is referred to as the cyber-territory. The effects doctrine on cyberspace does not defeat the principle of territorial jurisdiction. Rather, the principle adapts itself to the specific situation of the internet. According to this, the Wold Summit of Information Society produced a document in 2005 to recognize "that each government shall have sovereignty over its respective country code top level domains."[54] As such, states may proclaim full jurisdiction over its own ccTLD. Indeed, the ccTLD becomes a state's territory in cyberspace.[55]

3.4. Balancing between privacy and security

In addressing privacy rights, Rix mentions the possibility that states may require a revised concept of national security in attempting to handle new technology uses where impacts on an individuals privacy rights are likely to occur. Although it can generally be assumed that national security should take

[49] *Convention on Cybercrime, sec. 3, art. 22, ¶ 233, (8 Nov. 2001), ETS No. 185* http://conventions.coe.int/treaty/en/reports/html/185.htm (accessed October 22, 2013).

[50] *Regina v. Perrin*, Case no. [2002] EWCA Crim 747, 2002 WL 347127, ¶¶ 2–4 (22 March 2002).

[51] Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity*, p. 13 (2007).

[52] *Zippo Mfg. Co. v. Zippo Dot Com Inc.*, 952 F.Supp. 1119 1124 (W.D. Pa. 1997).

[53] Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 Jurimetrics Journal, 261, 264 (2002).

[54] World Summit of the Information Society, Chair of the Internet Governance sub-committee, *Chair's Report*, Doc. WSIS-II/PC-3/DT/10 (Rev.4)-E, ¶ 54 (30 September 2005), http://www.itu.int/wsis/docs2/pc3/working/dt10rev4.pdf (accessed October 22, 2013).

[55] Robert Uerpmann-Wittzack, *Principles of International Internet Law*, 11 German Law Journal, 1256-1258, (2010).

priority in times of heightened terrorist activity, it is also true that the Rule of Law should ensure that the impact upon the privacy rights of citizens should be minimised.[56] In other words, there seems to be a need to achieve a balance between attempting to combat terrorism and the security measures taken in the face of citizens. Although human rights are less respected in times of war, this should not mean that these rights should be disregarded altogether.[57] Rix addresses two questions that are directly relative to the Australian legislations: (1) whether the measures included are necessary for the protection of the country's national security in the presence of terrorism; and (2) whether any protective measures are included to mitigate the effects on individuals and society, protecting them from state power that claims necessity when the rule of law protecting citizens is weakened.[58] A clear conclusion was reached by Rix: the measures adopted by the legislation mentioned fell short of the second requirement; citizens are clearly not protected, and the legislation inherently assumes a position of draconian power that does not allow detained citizens the full extent of legal assistance. Indeed, it is argumentative in considering the government's response that, 'measures were necessary'. A possibility that the same measure eventually be applied to all citizens, whether suspect, guilty, or innocent, will certainly not reflect justice.

Legislations in Western countries have been particularly stringent since the 9/11 attacks. Indeed, a large number of anti-terrorism laws have been enacted since 2002. Rix states that 35 pieces of Commonwealth legislation on terrorism were in place in the country up to 2001, and seventeen additional items were added into the law since then. These additional legislation pieces were almost universally restrictive of civil freedoms to such an extent that both civil society and the legal community questioned their necessity, particularly in light of significant legislation already focusing on terrorism before 2001.[59]

In addition to the concern for civil liberty, there was also a concern regarding the somewhat broadly defined provisions in the new legislations. A legitimate concern was raised regarding the apparently increasingly powerful position of the state, while restricting judicial review and due process of law. The government tended to insist upon the legitimacy of their legislation in light of the terrorist threat, while opponents maintained their call for retrospective remedial action regarding the somewhat hastily implemented laws.[60]

In the UK, Bhatt mentions the controversy surrounding the RIPA 2000.[61] According to the author, "This Act has been one of the most controversial pieces of legislation in recent times due to the conflict and the difficulty of balancing the power of the state and rights of citizens."[62] Bhatt suggests that legislation such as RIPA, as well as the safeguards provided in such legislation should be carefully and critically examined, without the interference of media and government presentations of the war on terrorism.[63] Inherent in this controversy is not so much the content of the legislation, as its complexity. Some of the elements, particularly those relating to human rights, are unclear or subject to interpretation. This in itself creates difficulty when ensuring a compliance with human rights laws in Europe.[64]

For reasons like these, authors like Von Doussa are calling for a better balance between anti-terrorism measures and human rights. The author notes the general conception among proponents of anti-terrorism laws that human rights laws stand in direct opposition to their efforts.[65] Instead, Von Doussa refers to the 'practical utility' of integrating the principle of human rights into counter-terrorism. He also calls attention to the fact that international human rights laws were indeed created in response to significant global conflicts, precisely in order to maintain a balance between the security of nations and the rights of individuals. Much more than a simply esoteric, idealistic paradigm, these rights are

[56]Mark Rix, *Australia and the "War Against Terrorism": Terrorism, National Security and Human Rights*, 2 Crimes & Misdemeanours 40, 40–41 (2008).

[57]*Id* at 41.

[58]*Id at* 41.

[59]*See id. at 43*. Perhaps the most publicised and prominent of government measures against terrorism is the US Patriot Act, a piece of legislation that was passed into a law almost instantly.

[60]*Id* at 42–44.

[61]Hiral Bhatt, *RIPA 2006: A Human Rights Examination*, 10 The International Journal of Human Rights, 285, 287–88 (2006).

[62]*Id. at 285*.

[63]*E.g., Id* at pp. 286–302.

[64]*Id.* at 288–89.

[65]John Von Doussa, *Reconciling Human Rights and Counter-Terrorism – A Crucial Challenge*, 13 James Cook U. L. Rev., 104, 105 (2006).

'fundamental to being human'.[66] This balance is maintained not only during times of peace but also in times of war, where the importance of both sides—security and privacy—are considered for their impact upon each other.[67] As an example, the author mentions Article (12) of the ICCPR. This protects the human right of freedom and movement but can be restricted subject to the fact that such restriction is the least intrusive means possible of protecting security for the entire nation.

Indeed, international human rights laws acknowledge that states can and must take measures towards self-preservation when perceiving the threat of a terrorist attack. What is emphasised, however, is that these measures must be neither excessively invasive, nor to the entire exclusion of human rights. Certain rights are so fundamental that they must be protected at all times. Examples of these are the right to life and the right not to be tortured. In theory, this achievement of balance between anti-terrorism measures and human rights appear to be both logical and sound, and highly possible among states. However, in practice, this is often not the case. One simply has to take into account the Patriot Act in the US and the UK's tendency towards governmental secrecy to understand the gravity of the issue. Governments appear to apply different laws to themselves and to others.[68]

4. THE RIGHT TO PRIVACY IN TELECOMMUNICATION IN THE ARAB WORLD: POTENTIAL TELECOMMUNICATION INTERCEPTION AND ACCESS LAWS AND OBSTACLES OF IMPLEMENTATION

This section examines whether there are adequate legal ingredients to display the 'right to privacy' as one basic human right implementable in the Arab region. An examination also should entail the regulation of telecommunication in Arab countries such as Jordan, Lebanon and Morocco, in order to understand whether the laws in these countries serve as a template for their respective governments in implementing telecommunication interception and access laws.[69] These countries were chosen merely to give an indication of the types of legislative governance, if any, of the subject matter in the Arab region, and open the possibility for future country-to-country specific research.

The Arab region is mainly formulated of developing countries. The adoption of technology in these countries has increased dramatically despite the fact that the number of internet users is still restricted to a certain subset of the population.[70] A first glance at the Arab countries reveals that these countries, with the exception of Lebanon, do not generally have telecommunication interception and access statutes, and that there is no refined writing on this issue. Also, there seems to be a lack of critical analysis on this topic in specific. Lebanon might be recorded as the first Arab country to enact an interception law in 2009.

The Arab region is largely comprised of Muslims. Islam stresses the holiness of private life for all individuals.[71] It cherishes the importance of the intimate secrets of people as a reflection of what Allah has said in the Holy *Qur'an* in *Surah Al-Hujurat*: "O you who believe! Avoid much suspicion, indeed some suspicions are sins. And spy not, neither backbite one another. Would one of you like to eat the flesh of his dead brother? You would hate it (so hate backbiting)."[72] This verse from the Holy Qur'an evidences that telecommunication interception would be a severe violation of Islamic *Sharia* by being an interception of the most private aspects of an individual's life.

Another test of Islamic reluctance to allow interception and wiretapping is what the Prophet Mohammad (Peace be Upon Him) has said: "Those who eavesdrop, a pure liquid lead shall be poured in his ears."[73] This is to show how severe the punishment is in the afterlife in case of such violation. Further, Al-Bukhari stated that: "I passed by Ali Bin Omar while a man was talking. As soon as I approached him, he slapped my chest and said: If you find two people talking, do not approach them

[66] *Id.* at 107.
[67] *Id.*
[68] Anthony S. Blunn, Report of the Review of the Regulation of Access to Communications. Public Affairs Unit Australian Government Attorney-General's Department, (2005).
[69] For a general overview on the regulation of telecommunications and interception in the Middle East, *see* Nassal M. Kisswani, *Telecommunication (Interception and Access) and its Regulation in Arab Countries*, 5 J. Int'l Com. L. & Tech 225 (2010).
[70] *See e.g.*, Jordan Department of Statistics, *Information Technology Use at Home Survey (2007-12)* http://www.dos.gov.jo/owa-user/owa/techno.list_tables (accessed March 15, 2013).
[71] For an overview of an Islamic Perspective of this issue *see*: Khaled Hroub, 2009. Supra note 27.
[72] Qur'an 49: 12, Surah Al-Hujurat.
[73] Mohammed Laarusi, M. [*Phone Calls System in Criminal Procedure law of Morocco*], 5 Morocco Legal and Politics Journal, 151(2005) (In Arabic).

or sit with them unless you ask for their permission to do so; have you not you heard the Prophet's words?" (If two people are talking in private, no one should interfere unless they ask for the permission to do so).[74]

In scrutiny, Islamic *Sharia* does not seem to make this prohibition in an unqualified manner. Circumstances may require that such exception may be imposed in accordance with the infamous fundamental rule: 'Necessities render prohibitions justified'. As such, interception of telecommunications becomes allowed based on the necessity that justifies recourse to such exception. Yet, this necessity has to be allowed only against another fundamental rule that says: 'Necessity is to be valued as is', meaning in accordance with the real value of the necessity.[75]

4.1. Dictums of the 'Right to Privacy' in telecommunication from the Arab Region

Article (18) of the 1952 Jordanian Constitution 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".[76] 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.[77] Similarly, the Jordanian Telecommunication Law no. (13) provides that "telephone calls and private telecommunications shall be considered confidential matters that shall not be violated"[78], and that "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".[79] Also, 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".[80] 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".[81]

In Bahrain, Article (26) of its Constitution singled a provision on communication, stating that "the freedom of postal, telegraphic, telephonic and electronic communication is safeguarded and its confidentiality is guaranteed. Communications shall not be censored or their confidentiality breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by law". Such exigencies found way in the subsequent 2002 Telecommunication Law of the Kingdom of Bahrain no. (48) which makes a hesitant reference to the privacy of individuals in Article (3/b/1) and authorizes the telecommunication authority to carry out its duties in a manner best calculated to protect "personal particulars and privacy of services", whereas Article (78) stresses the authority's competence to have access to the network for fulfilling the requirements of national security.[82]

A similar constitutional protection for the right to privacy in telecommunication seems to be lacking altogether from the Lebanese Constitution. The Lebanese Constitution does not mention of the 'Right to Privacy' in telecommunication nor does its Telecommunication law no. (431) of 2002. In Lebanon, however, and despite being the first Arab state to enact an interception law in 1999, they have succeeded in enforcing it ten years later, in 2009. This Law prevents misuse of the freedom of private citizens. Article (1) of this Act provides that "all postal, telegraphic and telephonic communications

[74]Fath Al-Bari Sharh Sahih Albukhari, Vol. 11, p. 70, (In Arabic).

[75]*See*, analysis of the concept of necessity in Islam in: A. B. Abdullatif, [*The Jurisprudential Elements in Explaining the Holy Quran*], Phd Thesis, The Islamic University Press, 2003, p. 79 (In Arabic).

[76]Jordan Const., art. 18 available at: http://www.kinghussein.gov.jo/constitution_jo.html (Accessed March 5, 2013).

[77]U.S. Dept. of State, Bureau of Democracy, Human Rights, and Labor, *Jordan*, Sec. 1 f, (2006) (available: http://www.state.gov/g/drl/rls/hrrpt/2006/78855.htm) (accessed October 22, 2013).

[78]Jordanian Telecommunication Law (1995) art. 56, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=25&lang=english (accessed October 22, 2013).

[79]*Id.* at art. 76.

[80]*Id.* at art. 71.

[81]*Id.* at art. 77.

[82]The Telecommunication Law of the Kingdom of Bahrain no. 48 of 2002, http://tra.org.bh/en/pdf/Telecom_Law_final.pdf (accessed March 12, 2013).

shall be treated as secret and as such shall not be subject to intercept or suspension except in circumstances prescribed by law".[83]

In Morocco, the issue of the right to privacy in telecommunication seems to be controversial. The 1996 Constitution provides that the "the secrecy of corresponding must not be violated", whereas Article (108) of the criminal procedural law was made to add telecommunication interception provisions in an attempt to balance the control of illegal activities, whilst at the same time attempting to protect the national security. Amendments were enacted by adding eight provisions in regulation of the interception of telecommunication as well as the entities that should provide them. These entities are required to obtain permission before intercepting or accessing telecommunications. The crimes that are allowed to be investigated should be of a serious type.[84] The unconstitutionality of these provisions were often stressed by Moroccan scholars.[85]

In Egypt, there seems to be considerable controversy about the issue of privacy in telecommunication interception. Prior to the Arab Spring, Dr. Tariq Kamel, who then acted as the Egyptian Minister of Communication, passed an official note that his office would allow official security agencies to intercept people's telecommunications.[86] This announcement in itself provoked a degree of unrest. Opponents have noted that article (64/2) of the Telecommunications Act in Egypt authorizes the interception of telecommunications, only if approved by a competent court. Accordingly, the job of the Public Prosecutor in Egypt should be to protect privacy in general and achieve a degree of balance with the required national security. This realization has now been made a constitutional right under Article (38) of the new Egyptian Constitution of 2012, as a natural conclusion of the Arab Spring.

4.2. Telecommunication interception and access jurisprudence in the Arab World

The integration of modern technologies in maintaining national security has attracted the concerns of many intellectuals, and their varying opinions on the legitimacy of telecommunications interception. Attitudes are characterized by three positions: one allows superiority to private interest over public interest by considering that interception should be invalidated even if permitted by a competent court. This attitude is made on the basis of several considerations:

- If the technology pursued in criminal substantiation falls within the ambit of the 'freedom for proof' principle, as is prevalent in criminal proceedings, exploitation should not then be set in absence of the risks of violation of values protected by the Constitutions, specifically the right to private life and its sanctity.[87]
- Phone call interceptions are no more than deception of suspects, and is similar to forcing suspects to sniff or drink a substance that eventually will make them lose control of their senses or actions, and therefore allows the judicial authority to obtain certain confession.[88]
- One of the prerequisites for a fair trial is to allow the submission of evidence, pre-trial, to allow both parties to discuss their content face-to-face, and enable then to produce counter evidence, if possible. This criteria is missing altogether in the case of using intercepted phone calls.
- The fear that interception through wiretapping could become the only procedure in the investigation process that might affect the judges beliefs and would render any other evidence inconsequential.[89]

[83]Lebanon Telecommunication Interception Act no. (140) of 1999, sec. 1 (Arabic version) at: http://www.penallebanon.org/Publications.aspx?code=34; *See* Alsadeq Bogzol, [*Article 108 of Criminal Procedure Act is Unconstitutional*], AlMaghress Magazine (28 January 2011), http://www.maghress.com/assabah/4757 (accessed March 12, 2013) (In Arabic).

[84][The new code of Criminal Procedural Law 2011], Articles (108–116) (2012) at: http://www.slideshare.net/sirajj/ss-12639559 (accessed March 12, 2013) (In Arabic).

[85]Alsadeq Bogzol, [*Article 108 of Criminal Procedure Act is Unconstitutional*], AlMaghress Magazine (28 January 2011), http://www.maghress.com/assabah/4757 (accessed October 22, 2013) (In Arabic).

[86]Jalal Amin, [*Interception of telecommunication and foreign investment*] AlShorouq Newspaper (15 February 2009), http://shorouknews.com/columns/view.aspx?cdate=15022009&id=72ced48f-4187-4337-985f-da374804401e (accessed October 22, 2013) (In Arabic).

[87]Abdelsalam Bihiddo. [*Summary on Interpretation the Criminal Procedural Law of Morocco*], Dar Lyila 291 (1997) (In Arabic).

[88]Mohammed Al-Mashishi, [New Techniques in Criminal Substantiation; Proceedings of the Studying Day Organized by the House of Representatives on 29/03/2002], 146, (In Arabic).

[89]Zain Alabden Salem & Mohammed Ibrahim, [*Modern Scientific Techniques in Combating Crimes*]. Arab Magazine for Social Defense, 15, 72, (1983) (In Arabic).

— The dependence on interception of phone calls may adversely affect the 'presumption of innocence' doctrine as a principle set forth in international conventions.[90]

Another trend to legitimise intercepting telecommunications is for the following reasons:

— It is legitimate in achieving criminal justice to refer to novel science and technological progress.
— Interception of phone calls, or any other audio recordings, does not constitute a violation of privacy as long as it is done voluntarily, and in reference to the prescribed laws and regulations.

However, one could envisage a third trend that adopts a middle ground and considers the most vital interest of a state, and therefore allows the public authorities a right to carry out a degree of interception and access so as to safeguard national interests. However, these obligations must establish clear limits for the interception and guarantee for individuals the security necessary from any violations that might occur, whether of an administrative or judicial nature.[91]

It is to be noted that in criminal proceedings, it is generally acceptable to use all possible evidence to conclude a judgement. Therefore, the use of telecommunication interception and access is essentially substantial in criminal materials to maintain the interests of the state in serious crimes that pose serious public threats. This type of crime cannot generally be proven by the use of traditional means, and instead relies heavily on telecommunication interception and access. Accordingly, the exclusion of these modern techniques would leave such crimes unpunished. However, to alleviate the illegal use of such means would be to subject their use to certain qualifications that guarantee the inviolability of individuals' privacy.

Therefore, to achieve harmony between the contents of the constitutions that provide for the confidentiality of correspondence on one hand, and the criminal procedural laws in the Arab countries that is grounded in the principles of 'prevention' and the exception based on 'necessity', which grant the public prosecutor a summary action, a decision must be made based on necessity.[92]

4.3. The right to privacy v. telecommunication interception and access laws in the Arab Region

The purpose of this section is to examine the operation of the telecommunication interception and access laws by Arab countries, specifically in relation to the degree of proportionality that these laws are able to maintain the pillar of privacy as a human right, as opposed to a more policing state.

4.3.1. The Hashemite Kingdom of Jordan

Jordan has witnessed a flourishing technological boom and increase in the use of the internet in the recent years. Subsequent governments made it a key objective to overhaul the technology sector in the hope that it would make Jordan an attractive region for investment in these fields. To achieve this objective, Jordan has taken numerous measures, the most important of which was the establishment of the 1995 'Communication Regulatory Commission', and the subsequent promulgation of the 2002 Law on Telecommunications No. (8), amending its 1995 predecessor. This showed that Jordan strived to develop its own laws and regulations in relation to the communication sector whilst attempting to keep up with the concurrent factual developments.

Yet, there is no legislative order in Jordan that regulates the issue of telecommunications interception and access. Since interception poses the issue of achieving a balance between individual's rights to privacy unless permission is duly granted, and the State's authority and right to maintain internal and external security and hence monitor all that might prejudice its components, the intellectual positions on recognising the legitimacy of intercepting telecommunications fluctuate on legislative, jurisprudence and judiciary levels.

It has been mentioned that Article (18) of the Constitution Law 1952 of Jordan provides for the privacy in telecommunications. Further, Article (88) of the Jordanian Criminal Procedural Law 1961 provides that "The public prosecutor may censor all letters, correspondence, newspapers, publications and parcels at post offices, and all wireless letters at the telegraph offices; further, he may also intercept

[90]Abdelsalam Shaweesh, [*Technological Means and the Effect thereof on the Guarantees of Fair Trials*]. Al-Munatharah Magazine, 9, 131 (2004)(In Arabic).

[91]Yousef Wahabi, [*Problems of Wiretapping and Phone Harassment in Moroccan and Comparative Criminal Legislation*], 6 Almalf Journal, 136 (2005) (In Arabic).

[92]Supra note 73.

phone calls if the same is beneficial for demonstrating truth". Hence, one can see that the legislator permits the public prosecutor to intercept telecommunications in the service of justice, and in light of a warrant provided to authorize such interception.[93]

The above provision may not fit with the general rule, and does not provide for any substantive legal guarantees for those who are merely dubbed as suspects without any reasonable grounds for that suspicion. As a result, it is possible to impose interception without obtaining approval from a competent court of law.[94]

It is obvious here, the Jordanian legislator did not observe Jordan's international obligations stemming from the various international declarations and conventions, that guarantee an equivocal right to privacy of all individuals unless a legal necessity for securing the society is made prevalent. Even here, the interception entities of the state should be subjected to the supervision and control of the judiciary.[95]

In order to permit interception of phone calls through issuing court orders, the existence of solid, tangible evidence indicating a serious crime is required. Another pre-requisite would be to allow interception and access only for a certain period of time, and therefore should end upon submitting the needed information to a competent court.[96]

In accordance with the Anti-Terrorism Law 2006, authority was extended to the public prosecutor enabling him to intercept suspect's communications, whilst preserving all personal data of suspects.[97] Indeed, due to the rapid development of communication tools, the legislator in Jordan should interfere to provide definite powers for the executive authority and design articulate procedures to allow the state agencies with the capacity to disclose individual's privacy, and balance the due respect and legal protection for their private lives. Violation of such powers and procedures of interception should be punished, with the resulting invalidation of cases violating the procedures.[98]

The issue of making a subtle balance between two contradicting interests has, however, been realised in Jordanian judicial practice. A case that was based wholly on the interpretation of the provisions of the 1995 Telecommunication Law No. (13) was presented, which seemingly presents two contradictory inclusions in both Article (56) and (29).[99]

According to an interpretation by the 'Bureau of Interpretation of Laws of the Court of Cassation', presented in relation to the ability of Jordanian Police Force Directorate (through its Emergency Communication Centre, which is connected to all telecommunication companies), a right was conferred to this Centre to request data on the identity of the phone subscriber and their geographic positioning, as well as any other information related to manifesting the duties of the Emergency Communication Centre.

In applying the provisions of Article (29) and Article (56) of the Telecommunication Law, it may be realized that the Jordanian legislator, under Article (56) of the Telecommunication Law, had deemed phone calls and private telecommunication as confidential matters that should not be violated, and is therefore subjected to legal liability.[100] However, the legislator in Article (29/g) seems to allow the request of certain information for security reasons, and in the process of the implementation of judicial

[93]Sami Al-Rawashdeh, The Jordan Prevention of Terrorism Act 2006: A Proportionate Response to Amman Terrorist Attacks? 17 *European Journal of Social Sciences*, 316 (2010).

[94]Hassan AlMersafawi, [*Personal Freedom Guarantees under Exceptional Laws*], 2 The Egyptian Lawyers Journal, 32–361967 [In Arabic].

[95]*Id*, pp. 32–36.

[96]Ahmad Bilal, [*Admissibility of Evidence Obtained Illegally*], (Dar Al-Nahtha Al-Arabia, Cario 1995) (In Arabic).

[97]Mohammed Abu Amer, [*Criminal Law: Private Part*] (Tewiany for Publication,1989), (In Arabic).

[98]Fathi Wahidi, [Negative Impact of Technology Development on Personal Freedoms], 13 The Spirit of Law Journal, (1997) (In Arabic).

[99]The Jordan Court of Cassation Judgment No 5 of 2008, http:/www.lob.gov.jo/ui/laws/discussarticle_descr.jsp (accessed March 25, 2013) (In Arabic). Article (29/f) of the 1995 Telecommunication Law No. (13) that "The Licensee's undertaking to provide free-of-charge emergency telecommunications services to the Beneficiaries in accordance with the arrangements and limits to be determined by the Commission in cooperation with the concerned parties"; Article (29/g) provides that "The Licensee's commitment to offer the necessary facilities to the competent bodies to implement the judicial and administrative orders related to tracing the telecommunications specified in those orders"; Whilst Article (29/h) provides that "The Licensee's undertaking to provide the service to applicants or Beneficiaries on equal basis and without discrimination, except for national security requirements or within what is considered as tolerance for operational, social or humanitarian reasons". Further, the amended Article (56) of the Telecommunication Law 1995 states that "Telephone calls and private telecommunications shall be considered confidential matters which may not be violated, under legal liability".

[100]Supra note 95.

and administrative orders. Also, the licensee is to provide variable service to applicants for reasons of national security.

One can conclude that the Jordanian legislator admitted the inviolability of private telecommunications as being confidential and subjected the violators to liability. However, the legislator in Article (29/f, g and h) obliged the licensee to facilitate the work of the Jordanian Police Force Directorate in enforcing the judicial and administrative orders that relate to tracing specified telecommunications. The legislator has also authorized to depart from the 'confidentiality principle' for as long as it serves the national security.[101]

Since the Jordanian Police Force Directorate is directly concerned with preserving the national security of Jordan, it is therefore excluded from the confidentiality principle. Hence, the Bureau on Law Interpretation had unanimously maintained that it is the right of the Jordanian Police Force Directorate to obtain all necessary information that enable it to perform effectively. Additionally, it is within the authority of the Jordanian Telecommunication Regulatory Commission to mandate telecommunication companies to provide the Emergency Telecommunication Centre of all necessary data that enables it to perform its security duties.[102]

Additionally, the Jordanian Telecommunication Law 1995 has provided for certain penalties in this respect. Article (71) makes spreading or disclosing the content of communications through public or private telecommunications networks punishable by imprisonment for a period between one and twelve months, or by a fine between 100 and 300 Jordanian Dinars (JOD), or by both penalties. Furthermore, Article (76) provides that "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 for a period not less than one month and not exceeding six months, or by a fine not more than (JOD 200), or by both penalties". Similarly, the Cyber Crimes Law of 2010, addresses the issue of interception of telecommunications in Article (5) and considers that "any person who wilfully intercepts or wiretaps without a reason, content sent via the internet or any information system shall be subject to imprisonment for a term not less than one month and not exceeding one year, by a penalty that is not less than (JOD 200) and not exceeding (JOD 1000), or by both penalties."

4.3.2. *Lebanon*

Lebanon was the first Arab state to enact a telecommunication interception law in 1999, although it did not come into force until 2009 once it was formally adopted by the Lebanese Cabinet under the title "the Lebanese Interception Law No. 140/ 99". This aimed at preventing abuse of the citizen's freedom of privacy. As such, Article (1) provides that "all postal, telegraphic and telephonic communications shall be treated as secret and as such shall not be subject to interception or suspension except in circumstances prescribed by law". In scrutiny, one can pinpoint that this law attempts to regulate the interception and access of telecommunications on the basis of both judicial or administrative decisions.

4.3.2.1. Judicial interception: This kind of interception refers to that which is carried out as a judicial procedure as an outcome of an express request made by a competent judicial authority. Such interception ought to be managed and supervised by this competent court. This simply aims at identifying the committed crimes and then identifying the perpetrators and accomplices.[103] Article (2) of the Lebanese Interception Law provides that:

> In extreme emergencies, senior magistrates in each governorate shall, either spontaneously or upon a written request made by the assigned examining magistrate, decide on interception of communications made by any of the communications means ... in any criminal prosecution penalised by deprivation of freedom for a period not less than one year, provided that the decision to be made is in writing and justified and unchallengeable by any of the challenge methods.

[101] *Id* at pp. 34–36.
[102] *Id* at pp. 34–36.
[103] Nadir Shafi, [*What are the Conditions of Telecommunication Interception and Access*] Journal of the Army (2007) http://www.lebarmy.gov.lb/article.asp?ln=ar&id=14395 (accessed January 15, 2013) (In Arabic).

Furthermore, interception will be deemed as invalid if made by any agent of the Prosecuting Agency and in absence of a decision produced by the competent court magistrate.[104] The legal system of Lebanon, so closely intertwined with the French system, usually makes reference to the French Court of Cassation which holds that interception is deemed illegitimate unless necessitated by a crime committed prior to the interception process, and only in respect of interception managed and supervised by the Judge himself.[105]

Moreover, the Lebanese Interception Law No. 140/99 specifies few important procedures and conditions for judicial interception. Article (3) makes it clear that the Judge is enabled to decide on the kind of interception needed to obtain evidence for prosecution or investigation. He is also empowered to allow for no more than two months of interception for that purpose. This period is not extendable except under the same principles and conditions. On the other hand, Article (4) states that "Interception of communications, recording and executing a record of the content thereof shall be made by the duly assigned judicial police office under the authority, supervision and control of the judge who issues the decision". All staff members of the concerned agencies must assist in implementing the judicial decisions of interception.[106]

Furthermore, in accordance with Article (6), the judge who issues the decision of interception, or the assigned judicial prosecuting officer, shall organise the minutes on the interception process, and must contain the date and time of the commencement and the end of interception. The minutes shall be directly related only to the information required, and the recordings shall be kept maintained in a sealed envelope by the competent judge.[107] Finally, according to Article (7), all recordings shall be destroyed following a decision made by the general attorney at the Court of Cassation once the prescribed limitation period has lapsed.[108]

Furthermore, Article (8) of the Lebanese Interception Law provides that all communications made by lawyers may be intercepted but only after notifying the Chair of the Law Association Bureau so as to confirm that the concerned lawyer has committed or participated in committing a felony or misdemeanour.[109] This provision has been invalidated by a Constitutional Council resolution no. (24/11/1999), where it was decided that this provision is in direct contradiction of the principle of equality before the law, as it discriminates between the lawyers without a sound justification, and because wiretapping does not target them in their capacity as lawyers, but as citizens.[110]

4.3.2.2 Administrative interception: This refers to interception made by administrative or political authorities aiming to assemble specific information related to national security, or in the process of safeguarding vital national resources. The prevention of the risk of terrorism falls within the limits of this kind of control. It simply encounters any danger that threatens the state and the society.[111]

To many, this type of interception clearly violates human rights standards as embedded in major international conventions. It is therefore unwanted for national security entities to tap the communications of citizens for the protection of national security of the homeland or its constitutional or political institutions, except where danger is real and only in extraordinary cases as provided for by the laws and regulations and in express, clear and objective conditions.[112]

It should be indicated here that Article (2) of the National Defence Law of Lebanon, as promulgated by the Decree-Law No. 102/83, states that in cases where the homeland, or any part of the territories of Lebanon, or even a public sector or a group of the population, is subject to any danger, will allow for the possibility to declare the state's full or partial emergency. Measures thereof shall only be made possible by decrees made by the Council of Ministers and in submission made by the Higher Defence Council. Here, special provision that might aim at organising the control of transport, movement, transportations and communications are to be made. Hence, one can conclude that the rights of the

[104] *Id* at paragraph 7.
[105] *Id* at paragraph 7.
[106] Interception Law 140/99 (Lebanese), Article (5).
[107] *Id.* Article (6).
[108] *Id.* Article (7).
[109] *Supra*, note 104, at paragraph 12.
[110] Interception Law 140/99 (Lebanese), Article (8).
[111] *Supra*, note 104, at paragraph 14.H
[112] *Id.*

state during particular circumstances may be extended to allow interception of communications, provided that this is adopted only for a limited time and in extraordinary cases.

4.3.3. *Morocco*

The State of Morocco has made substantial amendments to its criminal law in adding eight articles related to the issue of telecommunication interception. These were made in an attempt to achieve a balance between the prescribed individuals rights and the national interest of the State, by means of controlling offensive activities while protecting national security. Hence, the amendments were produced to the effect of requiring governmental entities to obtain permission to intercept or access telecommunications, as well as prescribing the time limit for the actual interception. Furthermore, these amendments only allow the right of interception by governmental agencies for the most serious offences or crimes.

Also, in accordance with Article (108) of the 2003 Criminal Procedural Law, the attorney general may appeal to the Chief of the Court of Appeal to obtain an order of interception of telecommunications tools, only if the investigation requires it. This jurisdiction is confined to certain specific crimes, and does not entail the appeal to the Chief unless the matter is related to the crimes affecting the security of the state, or are related to combating terrorism.[113]

In cases of urgency, the general attorney may extraordinarily order, in writing, the interception of telecommunications tools without submitting an appeal to the Chief. For instance, when the investigation requires expedited action where there is a fear of evidence extinction, provided that an immediate notification is made to the chief of the competent court.[114] The chief of the court shall, within 24 hours, issue a decision on whether to confirm, adjust or cancel the decision of the attorney general.[115] In this case, the interception of phone calls shall be suspended and the adopted procedures in executing the cancelled order will be considered as extinguished.[116] The decision issued by the chief of the court is unchallengeable.[117]

It is noteworthy that the authority of the general attorney for intercepting telecommunications tools, is an exception to the general rule and may only be granted under the condition that the crime in question is of a collective organisation, and most importantly relates to matters of national security. These crimes are often penalised with capital punishment or life imprisonment.[118]

The judicial authority assigned with investigation is made of officers from the attorney directorate office. This excludes officers or employees that are not of this judicial capacity. This is in line with what has been mandated by Article (24) of the Criminal Law 1962 of Morocco, in stating that "The processes ... must indicate the ... has the judicial police officer capacity". Under Article (111), the officer who executes the interception must also produce a report of the minutes of the execution of interception and in respect of all and every interceptions of calls.[119] Generally, interception must be carried out under the supervision of the examining magistrate or the attorney general.

4.3.4. *Bahrain*

Bahrain's Telecommunication Regulatory Authority has issued a policy in relation to telecommunication interception and access. This policy aims to impose restrictions on companies maintaining records of all telephone calls and email communication, VoIP and all websites accessed by citizens and residents of Bahrain for the last three years on the basis of national security concerns. However, this policy from the Telecommunications Regulatory Authority was never submitted for due processing by the Bahraini Parliament. The policy has never even been discussed by members of the Parliament.[120]

[113]Criminal Procedural Law 2003 (Morocco), Articles (163–218).

[114]Abdullah Belhaj, [*Interception between privacy and the legality of criminal prosecution*], www.startimes.com/?t=22735957, (2009) (accessed January 20, 2013) (In Arabic).

[115]Criminal Procedural Law 2003 (Morocco), Article (108/5).

[116]*Id.*at Article (108/6).

[117]According to Article 108 of the Moroccan Criminal Procedural Law of 2003: The decision of the examining magistrate on the interception of the calls shall be deemed as jurisdictional rather than judicial; such interpretation is substantiated by the inability to challenge the decision.

[118]*Supra*, note 115 at paragraph 17.

[119]Supra note 73.

[120]Jameel Almahari, [*Correspondence and Telephone Calls Should be Confidential*], Al-Wasat (Manama), (10 March 2009) http://www.alwasatnews.com/2377/news/read/41299/1.html (accessed October 22, 2013) (In Arabic).

5. CONCLUSION

Privacy interests are as old as civil society. Yet, the concept of privacy in today's technological environment has become complex and is intertwined with the use of technology. Therefore, many Western governments have embarked on taking extreme measures to prevent the use of telecommunications for covert terrorist planning. In parallel, however, and irrespective of the different approaches to define the term, the right to privacy has also been recognised as one of the most fundamental human rights worldwide. International human rights laws acknowledge that states can and must take measures towards self-preservation when perceiving the threat of terrorist attack. What is emphasised, however, is that these measures must neither be excessively invasive nor entirely exclude human rights. The ECHR is the paradigm for an international treaty to protect human rights and fundamental freedoms in Europe. Article (8) of the Convention ensures the right to privacy and provides for the principle of proportionality that plays an important role in such cases.

After the 9/11 attacks, privacy has become not only complex, but also controversial, with governments attempting to defend their own right to invade the communication privacy of citizens while human rights groups advocate against this. From the government's viewpoint, complete privacy cannot be granted to citizens, considering that terrorist activity would then be allowed to thrive unabated. Indeed, it would seriously hamper the government's ability to protect its people from national security breaches. From the citizens' viewpoint, greater transparency from the government is desirable to protect their right to privacy.

An increasing number of critics have begun to question the validity of such governments' approach, especially as it concerns privacy interests in communications along with concomitant human rights. Further, the concern is that any government's ability to intercept electronic communications systems would significantly hamper the free speech rights provided for in their constitutions'. Despite citizens' calls to protect their privacy rights from government intrusion, complete transparency would paralyse government planning and action. In contrast, complete opacity is not conducive to a functional citizen-government relationship. Privacy interests and security are both at risk should the government maintain complete secrecy from the people. Finding the right balance between citizens' privacy rights and national security interests is crucial where privacy is at issue, including the workplace and surveillance practices in professional environments.

As in Western states, some Arab states have also attempted to regulate telecommunication industries and have made amendments to particular legislations. However, a particular need to advance new high-tech systems, whilst attempting to govern the use of telecommunication tools, is most needed. These should be directed to securing a balanced approach between the rights of citizens with the most necessary security needs. This can be achieved through introducing access laws and regulations that aim at protecting the interests of national economy from any potential threats whether sourced internally or externally.

Some Arab states, like Lebanon, may have enacted interception and access laws, but only in an intermittent fashion, making it difficult to refer to it as a complete template for implementing an interception and access law. Arab states either still lack proper telecommunication legislations, or at least have not yet made the proper amendments to their current laws and regulations to include interception and access to telecommunication.

Overall, it is recommended that the interception and access of information regulation in the Arab region must be multifaceted, in that it would fight cybercrime, terrorism, and domestic crimes such as drug abuse, but also protect individuals'/groups' rights to privacy. Protection of individual/group rights to privacy comes in two forms; the law itself must show respect for individual rights, and secondly, it must shield individuals/groups from other parties wishing to violate their privacy. Adoption of regulation for telecommunication interception and access is beneficial since it avails necessary grounds for complete protection of the economy against dangers of financial crime. It would make investors and business people have confidence in the business environment, which has an overall effect of boosting investments. Therefore, it should be drafted with the help of experts and professionals from various fields, including law and business to ensure that it captures a sufficiently wide view.

Such a regulation must not only benefit the country for the purpose of ensuring proper security. It is recommended that the regulation recognises the importance and need for businesses to initiate investigations whenever they notice violation. However, such investigations need to be initially limited in order to avoid breaches of individual privacy through the execution of investigations by law

enforcement agencies and officials. Where private investigators are involved, the law must stipulate their authority and the limitations imposed on that authority. Extension of authority for investigation to individual businesses and private practitioners is important in the current environment because businesses may wish to open preliminary investigations before determining whether their rights have been breached or if there are any damages. This is necessary to avoid an accumulation of cases involving interception and access of information violations in courts.

Whilst this paper sought to outline the gaps in existing legislative order in Arab countries, it attempts to draw some guidelines 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 these countries could follow to achieve this objective:

1) A prompt conviction should be reached by the governments of the Arab states that privacy protection shall be a core consideration in all initiatives. The introduction of a legislation on interception and access to telecommunication for security, and a law of enforcement purposes, should be a priority and is aligned with the requirements and criteria of international law.
2) The implementation of telecommunication interception and access law should cover the most serious offences only, including organized crime and crimes connected to corruption.
3) In the process of granting licenses to carrier companies, the legislation should place strict requirements to prevent interception of signals and data; a license should be required by the law enforcement and national security agencies. Arab governments should develop standard procedures for carriers as to what is required under the licensing conditions applicable to government agencies.
4) Government officials must implement a writ requirement from a competent court before obtaining call data from carriers. A warrant should be required when government officials seek to store accessed communication data.
5) Close observation of international developments in encryption and its control is required by government officials, as monitoring the use of encryption by interception targets becomes vital.
6) Arab states should indulge in having a general role in organizing and addressing international considerations related to interception and access issues associated with new technology.
7) Arab states should ensure that they amend their telecommunication Acts to allow law enforcement agencies to obtain legal orders to intercept and access individual and group communications whenever they deem it necessary to investigate or prosecute criminals.
8) Carriers in the Arab region should be aware of the initial cost of obtaining an interception capacity. Arab governments should be aware of allowing 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.
9) Arab states should invite and encourage the telecommunications equipment suppliers to participate in consultations on new technology and its interception and access implications.
10) The legislation should place a condition on carriers that before any signals or data are intercepted; a license should be required by government agencies (law enforcement and national security agencies).