Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia

Candidate number: 22

Advisor: Dr. Lee Bygrave

Deadline for submission: ….. (09/15/2009)

Number of words: 15,076

Thesis submitted in partial fulfillment of the requirement for the Degree of Master of Laws in Information and Communication Technology law, University of Oslo, 2009

UNIVERSITY OF OSLO

Faculty of Law

Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia

Submitted by

Alebachew B. Enyew

Submitted in partial fulfillment of the requirement for Masters Degree in Information and Communication Technology Law

Advisor: Dr. Lee Bygrave

Norwegian Research Center for Computers and Law (NRCCL)

Law Faculty

University of Oslo

September 2009

Acknowledgement

Thanks to God for letting me go through this! I would like to extend my heart-felt gratitude to my advisor Dr. Lee Bygrave for his scholarly and constructive comments in the course of writing. I would also like to thank all people who have directly or indirectly made my stay in Oslo bearable.

Table of Content

Acronyms

ECT-Ethiopian Telecommunication Corporation

ETA-Ethiopian Telecommunication Agency

EU-European Union

FDRE-Federal Democratic Republic of Ethiopia

FEAC-Federal Ethics and Anti-Corruption Commission

ICCPR-International Covenant on Civil and Political Rights

ICT-Information and Communication Technology

OECD-Organization for Economic Co-operation and Development

PET-Privacy Enhancing Technology

UDHR-Universal Declaration of Human Rights

Chapter one

1 The background of the study

1.1 Introduction

The right to privacy has been guaranteed in various human rights instruments, including in the International Covenant on Civil and Political Rights as fundamental right. As a state party to the Covenant, Ethiopia has constitutionally given recognition to the right. Nonetheless, the country does not have a specific privacy law to enforce the constitutionally guaranteed right. However, one can still find privacy related provisions in various branch of laws of the country, mainly in the constitution itself, Criminal Procedure Code, Law of Extra-contractual liability and Mass Media law. In this thesis, we are going to focus on examining how and to what extent privacy right is protected within the existing legal framework of the country.

Regardless of its constitutional guarantee and recognition under international human rights instruments, the right to privacy has been increasingly threatened owing to technological advancements. The global nature of the internet and the advancement of information technologies have enhanced the flow of information through out the world. Nowadays personal information can be collected and processed easily through the use of sophisticated means and implemented in various ways. The information appetite of both public and private sectors can also result in a wide and uncontrolled flow of information which can negatively affect the fundamental human rights and freedoms in particular the right to privacy. In short, recent developments can give rise to an inappropriate imbalance between the public interest for surveillance and the competing individual interest for privacy. And hence the flow of information has to be carefully scrutinized from personal data protection perspective.

Having known the ongoing situation, notably European countries and USA have begun to promulgate piece of legislation to protect personal information since 1970s. On the other hand, countries like Ethiopia have still tried to regulate privacy concerns by the virtue of the already existing law, without having specific law. Undeniably, the legal response of countries can be dependent upon their level of information and communication technology development. For instance, in most developing countries, information and communication technology is still lagging behind both in terms of quality and area of coverage. Such countries may take time to feel the repercussion of the new technology, and come up with the appropriate respective legal response. However, personal information could still be collected, processed and transferred even in those countries in which ICT is at the very early stage of development. Globalization and international trade have played a great role for the flow of personal data within and outside of those countries.

This being so, the central aim of this thesis is to probe the legal protection accorded to privacy by the already existing law of Ethiopia. For the purpose of this thesis, the terminologies “privacy law” and “data protection law” are used interchangeably. Besides, privacy is intended to refer all aspects of the term (physical privacy, information privacy, communication privacy and territorial privacy). The thesis is divided into four chapters. The first chapter presents background of the study, statement of the problem, scope of the study, and the methodology. By so doing, the chapter is hoped to provide the skeleton of the thesis. In chapter two, it is sought to discuss the concept of privacy, the scope and limitation of privacy as a human rights. This chapter will try to touch upon the definitional difficulty of privacy and the problem of balancing countervailing interests against privacy. It will also unpack the impact information technologies on the notion of privacy and explicate the evolution of privacy laws. Chapter three will be devoted to canvass the legal framework of Ethiopia to protect privacy and personal information in light of information technologies development. This chapter will also examine whether the existing law provides sufficient protection for privacy. Finally, whether or not Ethiopia needs to have a codified privacy law will be dealt in chapter four.

1.2 Statement of the problem

According to its Information and Communication Technology (ICT) Policy, the Ethiopian government has made the development of information and communication technology one of its strategic priorities as an industry and as an enabler of socio-economic transformation. Even though, still in its infancy, ICT in Ethiopia has developed rapidly in recent years. Apart from the positive contribution, this technological development has, will have negative repercussion on the right to privacy if it is not regulated. The exploitation and application of ICT generally requires an appropriate legal and regulatory environment in every sphere including personal data protection. In spite of lack of codified privacy law to protect privacy and personal information in the country, one can find scattered privacy provisions in various branches of law. This being so, the writer is intending to address the following issues: what are the relevant provisions within the legal framework of Ethiopia to protect privacy and personal information? To what extent those provisions can protect privacy and personal information in light of ICT development? Do they satisfy the requirement of the EU 'adequacy test' for transnational data flow? And does the country need to take measures to bring its privacy law in line with EU adequacy standards?

1.3 Scope of the study

The study is limited to unpack the most relevant privacy provisions within the legal framework of Ethiopia in light of the ICT development. Since Ethiopia does not have a comprehensive codified law (which can be applicable for the protection of privacy), the writer will try to identify the said provisions from different legislations, namely the constitution, law extra-contractual liability, criminal procedure code, mass media law and other branches of law of the country. In order to examine those provisions in light of privacy protections, a comparison will seldom be made with other jurisdictions' privacy laws such as EU Data protection Directives and OECD Privacy Guidelines. For better

understanding of the notion of privacy, the study will also explicate the meaning and scope of privacy based on human rights instruments and academic literatures.

1.4 Methodology

The study is methodologically designed to be carried out from the perspective of legal analysis. In respect to the application of primary source materials, international treaties, domestic laws and cases will be used. Secondary sources like books, journals and articles will also be consulted. Besides, policies, preparatory works, statements, declarations and soft laws will be taken in account to understand the historical and political context in the interpretation of laws if need be.

Since there is no legal literature on the notion of privacy from information technologies perspective in Ethiopia, the study will mainly be carried out by consulting and analyzing the existing laws of the country. Bearing in mind that there could be a huge gap between Ethiopia as developing country and developed countries in various ways, the study will adopt a comparative approach if a need arises.

The Ethiopian law belongs to the continental legal system, the primary feature of which is that laws are written into codified or systematically arranged document. Decision is given based on codified law concerning particular subject matter, not based on precedence. The statutes of Ethiopia have been written in Amharic (the working language of the federal government as per article 5(2) of the constitution) and English languages. In case of contradiction between the Amharic and English versions, the former has final legal authority. Each federal law has stipulated a provision to that effect. In this study, the writer will use the English version of the law insofar as there is no discrepancy between the meanings of the law in the two languages.

Chapter Two

2 The Concept of Privacy

2.1 Definition

This chapter primarily tends to explore the double challenge that the notion of privacy has been facing: lack of a satisfactory definition and difficulty in balancing privacy against countervailing values. The concept of privacy has been the subject of academic and public controversy for generations. Many literatures (be it legal or philosophical) tell us that there is no consensus on the meaning of privacy. The concept is too elusive to define it clearly and precisely. Many controversies regarding privacy are conceptual in nature which concern the meaning of privacy and analytic basis of distinguishing privacy right from other kinds of rights recognized within moral, political or legal theories.[1] Concomitantly, other disagreements stems from the question of how to balance privacy rights against the rights and interests of others.

Although defining privacy has proven to be quite complicated, and many commentators have expressed great difficulty in defining precisely what privacy is, many attempts have been made to define the concept. These attempts range from providing broad definition down to doubting privacy as a distinct concept. In this regard, there are two conceptual approaches which are known in literatures as anti-reductionism and reductionism.[2] Proponents of anti-reductionism claim that a divers set of invasions or interferences with personal information, secrecy, repose, reserve, peace of mind, bodily integrity,

[1] Madison Powers, A Cognitive Access Definition of Privacy, Law and philosophy, vol.15, iss: 4, (1996) p.369.

[2] Ibid p. 370.

anonymity, solitude, seclusion, sanctuary, intimacy or intimate relationships, and decisional autonomy should be understood under the generic heading of privacy.[3]

Advocates of reductionism do not accept the seemingly all inclusive conceptions of privacy saying that the more expansive conceptions of privacy are vague, ambiguous and indeterminate.[4] They assert that privacy can be reduced to other concepts and rights. In this connection, Judith J. Thomson contends that:

> *there is nothing particularly distinctive about privacy and to talk about things as violating the 'right to privacy' is not all that useful. Privacy is a cluster of other rights such as the right to liberty, property right, and the right not to be injured. The 'right to privacy' is everywhere overlapped by other rights. Is there something distinctive about privacy? What does privacy capture that these other rights and interests (autonomy, property, liberty etc) do not?*[5]

The quotation conveys that the conceptual distinctiveness of privacy is doubtful. The concept is regarded as parasitic in a sense that its protection can be secured by safeguarding other primary interests (property rights, human dignity, bodily integrity, preventing or compensating emotional distress, etc).[6]

As has been expounded above, the gulf of disagreement between the two approaches is huge, ranging from the extreme forms of anti-reductionism treating privacy as a large family of loosely related concepts without any common denominators, to the extreme version of reductionism advocating the elimination of privacy altogether on

---

[3] Ibid p. 370-71.

[4] Ibid p.371.

[5] Daniel J. Solove and Marc Rotenberg, Information Privacy Law, Aspen publishers, New York (2003), p.40.

[6] Raymond Wacks, Personal Information: Privacy and Law, Oxford, Clarendon Press, (1989), p.18.

the ground that privacy is nothing but some other concept.[7] A wide range of intermediate views are possible as well. Various writers have defined the term privacy in their own ways. However, none of them has been able to provide a satisfactory and universally accepted definition. Any how, it may be helpful for further analysis of the concept to examine the suggested definitions at this juncture.

According to Lee Bygrave, the definitions of privacy can be categorized into four major ways, albeit non-exhaustive.[8] The first group of definitions views privacy in terms of non-interference, a definition attributed to Samual Warren and Louis Brandeis who saw privacy as "a right to be let alone."[9] Most literatures indicate that the conception of Warren and Brandeis has profoundly shaped the development of the law of privacy. However, such definitions have been criticized for being over inclusive without some clear criterion for deciding when interference counts as a loss of privacy. Critics further contend that there are innumerable ways of failing to let a person alone which arguably have nothing to do with privacy or its loss, for instance hitting someone over the head with a brick is a clear case of not letting someone alone, and yet it is not reasonable to view it as an interference with privacy.[10]

The second group of theorists conceives privacy a form of control over personal information. Put differently, privacy is the control an individual has over information about the self. Charles fried explains that privacy is not simply the absence of information about the self in the mind of others; rather it is the control over the knowledge about oneself.[11] Alan Westin has also defined privacy as "claims of individuals, groups, or institutions to determine themselves when, how and to what

---

[7] Madison Powers , Supra note 1, P.371-72.

[8] Lee A.Bygrave, Data Protection law: Approaching its Rationale, Logic and Limits, (2002), p. 128-29.

[9] Samual D. Warren and Louis D. Brandeis, The Right to Privacy, Harvard Law Review, Vol. IV, No.5 (1809), P.193-96.

[10] Madison Powers, Supra note 1, p.374.

[11] Daniel J. Solove and Marc Rotenberg, supra note 5, p.31.

extent information about them is communicated to others."[12] Privacy is considered as an instrument for achieving individual goals of self-realization.[13] At this juncture, one may wonder whether or not this is a compelling definition of privacy. Critics of information control theorists argue that the condition of privacy may be obtained without control, and that one might exercise control without having privacy.[14] There is also uncertainty about the status of privacy whether it is a situation, a psychological state, a form of control, a right, a claim, or value. An assumption behind the rejection of information control definitions is that privacy can be defined as a condition or state of affairs such that it is possible to describe the changes in that condition which count as losses of privacy.[15]

The third group of definitions links privacy with intimacy. Some argue that intimacy appropriately defines what information or matters are private, for it is a common denominator in all the matters that people claim to be private.[16] For example, Julie Inness explains that privacy is the state of the agent having control over decisions (these decisions includes choices on the agent part about access to oneself, the dissemination of information about oneself, and one's actions) concerning matters that draw their meaning and value from the agent's love, caring, or liking.[17] Like other ways of definitions, linking privacy closely to intimate or sensitive aspects of one's life has suffered from criticism. The criticism springs from its failure to anticipate and capture the process by which detailed personal profiles are created.[18]

---

[12] Daniel Solove and Marc Rotenberg, Supra note 5, p.28.

[13] Bert-Jaap Koops and Ronald Leenes, 'Code' and the Slow Erosion of Privacy, 12 Mich. Telecom., Tech. L. Rev. 115 (2005), available at http://www.mttlr.org/voltwelve/koops and leenes.pdf, p.124.

[14] Madison Powers, Supra note 1, p.373.

[15] Ruth Gavison, Privacy and the Limits of Law, the Yale Law Journal, Vol.89, No.3, (1980), p. 425-27.

[16] Daniel Solove and Marc Rotenberg, supra note 5, p.32.

[17] Ibid.

[18] Lee Bygrave, Supra note 8, p.131.

The fourth group of theorists views privacy as a form of limited access to the self. Ruth Gavison has given an influential and multidimensional definition in this category. According to Gavison, our interest in privacy is related to our concern over our accessibility to others: the extent to which we are known to others (secrecy), the extent which others have physical access to us (solitude), and the extent to which we are the subject of others' attention (anonymity).[19] She argues that the three forms of privacy are independent, irreducible and distinct in the sense that a loss of privacy may occur through a change in any one of the three, without a necessary loss in either of the other two.[20] According to her, the concept is coherent because the three elements are all part of the same notion of accessibility, and are related in many important ways. Advocates of reductionism objected her on the ground that the two elements (secrecy and anonymity) can be reduced into one, and thus they are not distinct senses of privacy.[21]

Such a diversity of definitions tells us the battle over the concept of privacy seems to continue unabated. The problem of the definition by no stretch of imagination implies that the concept lacks importance. The quest and need for privacy is a natural one. In fact, the absence of a uniform definition of privacy may not always be a weakness, for it provides room for flexibility in its implementation and for balancing the amorphous concept with large counter claim.[22] And yet the prospects for its satisfactory legal recognition and application are bound to be poor unless the concept is sufficiently distinctive to facilitate coherent analytical identification and description.[23]

---

[19] Ruth Gavison, Supra note 15, p.423.

[20] Ibid p.428.

[21] Madison Powers, supra note 1, p. 383.

[22] Lee Bygrave, Supra note 8, p. 127.

[23] Raymond Wacks, Supra note 6, p.19.

As discussed, privacy is defined differently by various scholars: as a right to be let alone, control over information, intimacy and limited access to the self. It is of the opinion of this writer that the definition of privacy should not be confined to one aspect of the notion. To put differently, the definition should be broad enough to cover the essence of the concept or the multidimensional aspects of privacy. According to David Banisar there are the following four separate but related aspects of privacy.

> *Information privacy: which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";*
> *Bodily privacy: which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;*
> *Privacy of communications: which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and*
> *Territorial privacy: which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.*[24]

For example, informational control definition seems to this writer that it overlooks two or more aspects of privacy. The concept of privacy should be understood to refer the aforementioned dimensions. In being multidimensional, this writer finds that Ruth Gavison's definition is the most compelling to be upheld.

2.2 Privacy as a Human Right

Modern international human rights law is a post World War II phenomenon since its development can be attributed to the monstrous human rights violations during the war.[25]

---

[24] David Banisar, Privacy and Human Rights, Electronic Privacy Information Centre, Washington, DC, (2000), p.3.

With the establishment of the United Nations in 1945, the international community pursued a goal of "promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language or religion."[26] In this respect, the first remarkable step taken by the UN was the adoption of the Universal Declaration of Human Rights by the General Assembly on 10 December 1948. The Declaration has become to be recognized as a common standard for all peoples and nations towards the promotion human dignity. The standard setting gave way to the promulgation of legally binding international human rights instruments of the 1966: the Covenant on Civil and Political Rights, and the Covenant on Economic, Social and Cultural Rights. These instruments are subsequently supplemented by various conventions dealing with specific human rights violations.

Privacy is internationally recognized as a fundamental human right under the Universal Declaration of Human Rights (article 12), the International Covenant on Civil and political Rights (ICCPR article 17), the UN Convention on Migrant Workers (article 14), and the UN Convention on the Protection of the Child (article 16). These international human rights documents have embodied privacy in more or less the same wording. For instance, Article 17(1) of the International Covenant on Civil and Political Rights states: "no one shall be subjected to arbitrary or unlawful interferences with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." According to the Human Rights Committee, this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons[27]. State parties are required to adopt legislative and other measures to give

---

[25] Thomas Buergenthal *et.al*. International Human Rights Law in a nutshell, 3rd ed., west Group, (2004), p.27.

[26] Charter of the United Nations, (26 June, 1947), chapter I, art.1, Para. 3.

[27] The Human Rights Committee General Comment No.16, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc. HRC/08/04/88 (1988), Para. 1.

effect to the prohibition against such interferences and attacks as well as to the protection of this right.[28]

Article 17(1) has four elements: privacy, family, home, and correspondence. The term privacy in the heading and privacy in the wording of this article are different in their scope. The former is broad enough to consist of the four elements whereas the latter is to mean private life in the narrow sense. Privacy in the narrow sense includes all manifestations of privacy that do not fall under other categories: family, home and correspondence. Private life includes autonomy, physical and moral integrity, the right to determine personal identity (including sexual identity) and sexual orientation and relations.[29] Regarding the term family, the Human Rights Committee has stressed that the objectives of the Covenant require a broad interpretation of the family in the sense of the respective cultural understanding of the various State Parties.[30] In its General Comment No.16 paragraph 5, the Committee has also noted that home has to be understood to indicate a place where a person resides or carries out his usual occupation. Finally, communication under article 17(1) covers a wide range of communications including post, telephone, telex, fax, and email.

Furthermore, regional human rights instruments (save African Charter on Human and Peoples' Rights) have expressly given recognition to privacy as one of the fundamental rights in human rights catalogue. Although the African Charter on Human and Peoples' Rights does not explicitly say anything about the right to privacy, this writer believes that some aspect of privacy is impliedly enshrined in it when the Charter stipulates that "every individual shall have the right to respect of the dignity inherent in a human being and to the recognition of his legal status. All forms of exploitation and degradation of man particularly

---

[28] General Assembly Res. 2200(XXI) of 16 December 1966, International Covenant on Civil and Political Rights, Article 17(2).

[29] Manfred Nowak, UN Convention on Civil and Political Rights: CCPR Commentary, N.P. Engel, publisher Kehl, Strasbourg, Arlington, (1993), p.294-98.

See also Philip Leach, Taking a Case to the European Court of Human Rights, Blackstone Press Limited, (2001), p.150

[30] The Human Rights Committee General Comment No.16, supra note 27, Para. 5.

slavery, slave trade, torture, cruel and inhuman or degrading punishment and treatment shall be prohibited." [31] In Africa, there is little development towards privacy laws despite the fact that almost all African countries have ratified the ICCPR. The possible reason may relate to the lack of technological advancements, political and cultural differences. Some people might think of privacy as no more than a luxury for the better-off in developed countries.

In the Inter-American human rights system, the right to privacy has been embodied in the 1948 the American Declaration of the Rights and Duties of Man. This regional declaration has been reinforced by the American Convention on Human Rights of 1969. Article 11 of this Convention envisages:

> *(1)Every one has the right to have his honor respected and his dignity recognized. (2)No one may be the subject of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.(3)Every one has the right to protection of the law against such interference or attacks.*

The American Convention on Human Rights sets out the right to privacy in similar terms (save sub article 1) to the International Covenant on Civil and Political Rights.

The 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms has also enshrined the right to privacy in different formulation and content as compared to the above discussed human rights instruments. The difference lies on the qualifications made in sub article 2 of article 8 of the Convention. Article 8 of this Convention reads:

> *(1) Everyone has the right to respect for his private life and family life, his home and his correspondence. (2) There shall be no interference by a public authority*

[31] African Charter on Human and Peoples' Rights, (1981), article 5.

with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

Like the Covenant on Civil and Political Rights, this article protects four different interests (private and family life, home and correspondence) which embrace a variety of matters, some of which are connected one another, some of which overlap with others.[32] The first paragraph defines protected right, the second lays down the condition upon which a state might legitimately interfere with the enjoyment of the right. In other words, the European Convention expressly stipulates the competing interests protected and limitations. So far we have seen how the right to privacy is incorporated in the international and regional human rights instruments. Like most human rights, the right to privacy is not an absolute one. It has its own limitations. Now we are going to comment on the limitations of the right to privacy.

2.3 Limitations of Privacy

According to international human rights law, countries can generally limit or restrict the scope of obligations in different ways: express limitations to the rights, derogations from the rights, and reservations to treaties. In this section, we are not interested in discussing derogations and reservations. Rather we are going to probe the limitations to the right of privacy. A restriction of rights is stipulated in human rights documents in order to strike a balance between competing interests/values.

[32] DJ Harris, M O'Boyle and C Warbrick, Law of the European Convention on Human Rights, Butterworth, London, (1995), P.302.

As discussed, the right to privacy is guaranteed in the UDHR, ICCPR and the American and European human rights system. Of these human rights instruments, the European Convention on Human Rights has explicitly provided an exception to the right to privacy. To the contrary, as one can understand from the cursory reading of article 17 of the ICCPR, there is no express legal proviso allowing for restriction in the interest of public or similar purposes. Nonetheless, one can logically infer the existence of permissible interference with privacy from the phrases "arbitrary or unlawful interference." However, the terms arbitrary and unlawful are in need of interpretation. According to the Human Rights Committee, the term unlawful means no interference except in cases envisaged by law, and the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[33] The converse reading of article 17(1) reveals that interference with the privacy, family, home and correspondence is permissible so long as the interference is neither unlawful nor arbitrary. And hence limitation of the right for the sake of other interests is permitted insofar as such limitation is made lawfully and reasonably. There is no wrong to restrict right to privacy in accordance with the law and in a reasonable manner. The essence of each restriction is that the interest of the society as whole overrides the interest of individuals.

By the same token, under the European Convention on Human Rights, the right to privacy can be limited where certain qualifying conditions are satisfied. Those conditions (under which limitations are permissible) are clearly envisaged under article 8 (2) of the Convention. As per paragraph 2 of article 8 of the Convention, limitations are allowed if they are in accordance with the law and are necessary in a democratic society for the protection of one of objectives set out therein. In order to strike a balance between human rights enshrined in the Convention from articles 8-11 and their respective limitations, the European Court of Human Rights has used the same criteria: whether the interference is prescribed by the law, whether the interference pursues a legitimate aim, and whether the

[33] Human Right Committee General Comment No.16, Supra note 27, para.3-4.

interference is necessary in a democratic society and proportionate to the legitimate aim pursued.[34] These criteria have been advanced and made clear by decision of the Court at Strasbourg.[35] Therefore, any countervailing values/interests against the right to privacy will be examined based on those criteria at least in Europe.

The European Court of Human Rights has been using the "balancing test" based on those criteria to lawfully justify the limitations to the right of privacy. One the other hand, in the U.S context, the test of "reasonable expectation of privacy" has been introduced in case law to canvass whether there is a breach of privacy.[36] Actually, the transatlantic difference regarding privacy is not only limited to using different parameters to offset other values against privacy, but there is also a divergence of view on value protected by privacy: liberty or dignity? The cleavage between 'libertarian' and 'dignitarian' is considered as a reflection of the underlying neo-liberal and social democratic theories of human rights.[37] The transatlantic clash on privacy is described:

> *Privacy protections in Europe are, at their core, a form of protection of a right to respect and personal dignity…By contrast, America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: it is the right to freedom from intrusions by the state, especially in one's own home.*[38]

---

[34] Francis G. Jacobs and Robin C.A. White, the European Convention on Human Rights, Oxford University press, 4th ed, (2006), p.223-40.

[35] See *Malone v United Kingdom* (1984) 7 EHRR 14, *Silver et.al. v United Kingdom* (1983) 5EHRR 347, and *Salov v. Ukraine*, European Court of Human Rights, Strasbourg, (2005).

[36] Bert-Jaap Koops and Ronald Leenes, supra note 13, p.128.

[37] Katja S. Ziegler, Human Rights and Private Law-Privacy as Autonomy, Oxford and Portland, Hart Publishing, (2007), p.1-2.

[38] James Q. Whiteman, the Two Western Cultures of Privacy: Dignity versus Liberty, Yale Law Journal, Vol.113, (2004), p.1151.

2.4 The Impact of Technology on Privacy

We live in a society in which information technology is accelerating rapidly. Because of the technology there has been steady growth in the use and manipulation of vast quantities and varieties of personal data. Extensive details concerning the most trivial actions undertaken are recorded. This offers almost unlimited possibilities to facilitate surveillance and monitoring, thereby invading privacy.[39]As the information based societies have gradually become more dependent on computers and new technologies of communication, privacy has been at stake more than ever. Audio and video surveillance technologies, identification and tracking technologies, data processing technologies, internet and computer technologies (privacy invasive technologies) have been offering many new opportunities for capturing and processing data. While the growth of information technologies is critical to governments, public services, business, and the livelihood of many individuals, it can also facilitate unobtrusive access to, manipulation of, and presentation of private data of individuals.[40] In this regard, one commentator pointed out the seriousness of the matter when he said: both government and business are using information technologies to monitor individuals "to a degree that no keystroke goes uncounted, and no pause for breath goes unmetered."[41] Wherever we go, whatever we do, we could easily leave behind a trail of data that is recorded and gathered together.[42] And hence, the information technologies have created a big forum for them to pry deeper into the personal sphere, often invisibly and from a safe distance.

---

[39] Bert J. Koops and Ronald Leenes, supra note 13 p. 118.

[40] Victoria Bellotti, Design for Privacy in Multimedia Computing and Communications Environments, in Philip E. Agre and Marc Rotenberg, Technology and Privacy: the New Landscape, The MIT Press, Cambridge, Massachusetts, (1998), p.64.

[41] David Brin, Transparent Society-Will Technology Force Us to Choose Between Privacy and Freedom?, Addison-Wesely, Reading/Massachusetts, (1998), p.81.

[42] Daniel Solove and Marc Rotenberg, Supra note 5, p.1.

Privacy erosion is the counter product of the rapid growth of information and communication technology. In relation to the impact of the information technologies on privacy, it was said that:

> *one of the less welcoming consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.*[43]

According to David Banisar, along with technological advancements there are three important trends that contribute to the erosion of privacy: globalization (which removes geographical limitations to the flow of data-internet), convergence (which leads to the elimination of technological barriers between systems for interoperability) and multimedia (which fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms).[44]

The increasing sophistication of information and communication technologies, coupled with the increasing use of personal information by business and government,

---

[43] Ian J. Lioyd, Information Technology Law, Oxford University press, 4th ed., (2004), p.52

[44] David Banisar, Supra note 24, p.18

has posed great challenges for the protection of privacy. However, it is equally good to remember that technologies are not always privacy invasive. In fact, there are some privacy enhancing technologies (PETs) like encryption and anonymizing technologies. But still information technologies are more privacy invasive than privacy enhancing. The growing dependency of the society on novel and constantly evolving technologies has introduced a sense of urgency to the demand for the legal applications and implications of these new technologies. In the next section, we are going to elucidate the evolution of privacy laws.

2.5 The Evolution of Privacy Law

As discussed in the forgoing section, there have been rapid information technology developments which in turn spawn the growth in the amount of data stored and the data-sharing along organizational and national boundaries. Concerns about the potential effect of automatic data processing upon the right to privacy began to grow during the late 1960s and the early 1970s with the advent of information technology.[45] These concerns about the possible use and misuse of data through sophisticated technologies gave rise to a growing call for legislative intervention. In response to this call, US has exhibited a propensity to enact a range of statutes to regulate specific forms of information handling (sectoral approach), whereas a different approach has prevailed within Europe in which the tendency has been to enact omnibus data protection statutes (comprehensive laws) to regulate almost all instances regarding personal data.[46] So the development of privacy law in United States is typically described as sectoral in a sense that privacy legislation focuses on specific sectors of the economy, while European privacy law is often characterized as omnibus, for it is generally applied to all entities that collect personally identifiable information

[45] James Michael, Privacy and Human Rights: an International and Comparative Study, with Special Reference to Developments in Information Technology, Dartmouth, UNESCO Publishing, (1994), p. 32.

[46] Ian Lioyd, Supra note 43, p.61.

regardless of the nature of the business or the technology involved.[47] Beyond the comprehensive and sectroral laws, there are two more approaches for privacy protection which can be complementary or contradictory depending on their application.[48] One of the approaches is self-regulation. At least theoretically privacy protection can be achieved through various forms of regulation, in which companies and industry bodies establish codes of practice and engage in self policing, thereby enabling data subjects and other entities to enforce the codes against themselves.[49] Self regulation, which is currently the policy promoted by USA, Japan and Singapore, has tended to provide only weak protections and lack enforcement.[50] The other approach is using privacy enhancing technologies. Individuals and institutions have sought to develop cryptographic techniques of data protection that provide varying degrees of privacy and security of communications.[51]

Beyond Europe and USA, other countries are also moving toward adopting privacy laws. According to David Banisar, there are three major reasons for the movement towards comprehensive privacy laws. These are:

> *To remedy past injustices- many countries, especially in Central Europe, South America and South Africa, are adopting laws to remedy privacy violations that occurred under previous authoritarian regimes.*
> *To promote electronic commerce- many countries, especially in Asia, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal*

---

[47] Daniel Solove and Marc Rotenberg, Supra note 5, p.687.

[48] David Banisar, Supra note 24, p.3.

[49] David Bender and Larry Ponemon, Binding Corporate Rules for Cross-Border Data Transfer, Rutgers Journal of Law and Urban Policy, Vol.3:2, (2006), p.161.

[50] David Baisar, Supra note 24, p. 4.

[51] David J.Phillips, Cryptography, Secrets, and Structuring of Trust, in Philip E. Agre and Marc Rotenberg, Technology and Privacy: the New Landscape, Cambridge, The MIT Press, (1998), p243.

information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

To ensure laws are consistent with pan-European laws- most countries in Central and Eastern Europe are adopting new laws based on the Council of Europe Convention and the European Union Data Protection Directive. Many countries hope to join the European Union in the near future. Countries in other regions, such as Canada, are adopting new laws to ensure that trade will not be affected by the requirements of the EU Directive.[52]

The origin of modern privacy laws (commonly known data protection laws in Europe) can be traced to the first data protection law in the world enacted in the state of Hesse in Germany in 1970, with the first national statute being the Swedish Data Protection Act 1973.[53] Indeed, it was inevitable, as society increasingly dependent on novel and constantly evolving technologies, that the legislatures would be compelled to enact laws in order to regulate the new situation. According to Bygrave, there are three important catalysts for the emergency of data protection laws, which can be termed technological and institutional developments, public fears about these developments, and legal factors[54]

As has been said in section 2.2, the formal normative source of privacy laws derives from human rights instruments, mainly from Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, Convention on Child Rights, Convention on Migrant Workers, and the two regional (European and American) human rights instruments. These human rights instruments have firmly established privacy protection as fundamental human rights claim, and thereby shaped privacy laws. Although the first privacy laws were enacted at national level, there had been

---

[52] David Banisar, Supra note 24, P.9.

[53] Ian Lioyd, Supra note 43, p.62.

[54] Lee Bygrave,Supra note 8, p.93.

international data protection initiatives pursued within the Council of Europe and the Organization for Economic Cooperation and Development (OECD).[55] These initiatives resulted in the adoption of the Council of Europe's Convention on data protection and the OECD Guidelines. The former came into effect in 1985, and is now legally binding among the member states, whereas the latter is not in the language of obligation, rather recommendation. The Council's Convention has established basic rules for data protection measures to be adopted by adhering states, and has set out special rules about trans-border data flows.[56] The 1980 OECD guidelines, which carry heavy political and economical weight, have also stipulated the fundamental principles for personal data protection.[57] The privacy guidelines of OECD represent a consensus position of countries from North America, Europe, and East Asia as to the basic structure of privacy law. Beyond this, there are guidelines at the United Nations level regarding Computerized Personal Data Files which are intended to encourage enactment of privacy laws in UN member states, and to encourage international organization to process personal data in a responsible, fair and privacy-friendly manner.[58]

In Europe, apart from the Council of Europe's Convention on Data Protection, the 1995 EU Data Protection Directive is the central focus of European Privacy law. The EU Data Protection Directive has had a profound effect on the development of privacy law, not only in Europe but also around the world.[59] The importance of this Directive stems from its status as a legally binding instrument. Beyond the Directive, the

---

[55] Ian Lioyd, supra note 43, p.62-63.

[56] Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series No. 108, /1981), articles 5 & 12.

[57] Lee A. Bygrave, Privacy Protection in a Global Context- A Comparative Overview, in Peter Wahlgren(ed.), IT law, Scandinavian Studies in Law Vol.47, Stockholm Institute for Scandinavian Law,(2004) p.334.

[58] Ibid, p.335.

[59] Daniel Solove and Marc Rotenberg, Supra note 5, p.688.

European Court of Human Rights has also played a great role for the development of privacy laws by giving a binding decision pursuant to article 8 of the European human rights convention.

The Organization for Economic Cooperation and Development (OECD) privacy guidelines set out eight key principles for the protection of personal data which have shaped national privacy laws around the globe. These basic principles for personal data protection are summed up in terms of collection limitation, purpose specification, information quality, individual participation, use limitation, information security safeguards, openness and accountability.[60] The Council of Europe Convention on privacy protection has much in common with the Guidelines. It is also a truism in EU Data Protection Directive even though the last two basic principles are not included.

[60] OECD Guidelines on the Protection of Privacy and Transborder flows of Personal Data, (1980), articles 7-14.

Chapter Three

3 The Legal Framework for Privacy Protection in Ethiopia

3.1 ICT in Ethiopia at Glance

Before we proceed to probe the privacy law of Ethiopia, it is very important at this point to give an overview about the status of information and communication in the country, for information technology has a great impact on privacy. The introduction of telecommunication in Ethiopia dates back to 1894.[61] Established over a century ago, the Ethiopian Telecommunication Corporation (ETC) is the oldest public telecommunication operator in Africa. ETC operates as a public enterprise under the supervision of the Ethiopian Telecommunication Agency (ETA)[62], with the principal duty of maintaining and expanding telecommunication services in the country and providing domestic and international telephone, telex, facsimile, telegraph and other communication services. In this respect, ETC has been made the "sole telecommunication service (including the provision of internet service) provider."[63] Despite the recent liberalization and privatization measures in different sectors, the telecommunication industry has remained under the control of the government. So ETC is the incumbent public telecommunication operator and has a monopoly over all telecommunication services in the country (fixed, mobile, internet and other communication services).

---

[61] Access on June 24, 2009, Ethiopian Telecommunication web site http://www.telecom.net.et/aboutETC/history.html.

[62] Proclamation No.49/1996, A proclamation to Provide for the Regulation of Telecommunications, *Negarit Gazeta*, (1996), article 3 and 6.

[63] Proclamation No. 281/2002, A Proclamation to Provide for the Amendment of Telecommunication Proclamation, Negarit Gazeta (2002), article 2(1).

In 1993, the use of the internet was introduced in Ethiopia when the UN Economic Commission for Africa (whose head quarter is in Addis Ababa) established a store-and-forward email service called PADISNet (Pan African Documentation and Information Service Network).[64] The introduction of the internet has increased access to the global knowledge resources. Especially since 1997 it has been observed considerable growth of information technology use in Ethiopia - proliferation of private companies that provide value added services in information technology, training centers and the establishment of a computer science unit in Universities, efforts towards standardizing Ethiopic software, etc.[65] Concomitantly, infrastructure is being put in place in various line ministries and regional states through funds from development assistance. Given the wide range of needs and enormous poverty, efforts to date are virtually insignificant.

As a developing country, Ethiopia has taken many efforts to improve the existing socio-economic conditions. ICT is believed to provide opportunities to support in the sustainable development of the socio-economic conditions, thereby enabling poverty eradication. The country has considered ICT as a major enabler of developmental efforts. This being so, the National ICT Policy was formulated in 2001. The National ICT Policy is a comprehensive document that articulates policy guidelines and describes critical areas for the development of ICT in Ethiopia. The strategic focus areas of this document include, among other things, the legal and regulatory environment. However, E-commerce related laws and regulations such as privacy protection and digital signature have yet to be promulgated. For the purpose of the thesis, we are going to examine as to how privacy is protected within the purview of the Ethiopian legal system. Therefore, the following sections are devoted to discuss the legal regimes of Ethiopia which are capable of protecting privacy right.

---

[64] International Telecommunication Union, Internet from the Horn of Africa: Ethiopia case study, Geneva (2002), p.18.

[65] Lishan Adam, Information and Communication in Ethiopia: Past, Present and Future Potential for Social and Economic Development, Ethiopian Information Technology Professional Association Workshop, Addis Ababa, (1999).

3.2 Privacy laws

3.2.1 The FDRE Constitution

As pointed out in section 2.2, privacy is a fundamental human right recognized in most major international treaties and agreements on human rights. Moreover, the constitutions of most countries of the world guarantee this right. So does the Ethiopian constitution. The Federal Democratic Republic of Ethiopia (hereinafter FDRE) Constitution consists of a comprehensive bill of rights including civil, political, economical, social and cultural rights as well as the right to development and environmental rights. Almost one-thirds of the constitution is devoted to human rights (chapter three of the constitution, articles 13-44). In respect of privacy, Article 26 of the constitution guarantees the right in the following terms:

1. *Everyone has the right to privacy. This right shall include the right not to be subjected to searches of his home, person or property, or the seizure of any property under his personal possession.*
2. *Everyone has the right to inviolability of his notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices.*
3. *Public officials shall respect and protect these rights. No restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others*.

The FDRE constitution further provides: “All international agreements ratified by Ethiopia are an integral part of the law of the land”, and that: “The fundamental rights and freedoms specified in this chapter [chapter 3 of the constitution on fundamental rights and freedoms] shall be interpreted in a manner conforming to the principles of the Universal Declaration of Human Rights, International Covenant on Human Rights

and international instruments adopted by Ethiopia."[66] Accordingly, as Ethiopia is a party to the Covenant on Civil and Political Rights, article 17 of the Covenant should be deemed to be an integral part of the privacy law of the country. And if the privacy provision of the constitution is vague, ambiguous or needs interpretation, it will be construed in light of article 12 of UDHR and article 17 of ICCPR. However, individuals are not entitled to communicate human rights violations to the Human Rights Committee, since Ethiopia has yet to ratify the first optional protocol of the ICCPR.[67]

As we can understand from the cursory reading of article 26 of the FDRE constitution, the right to privacy of the individual is defined in terms of one's person, home and property. The right to inviolability of one's correspondence and communication with others is also made part and parcel of the right to privacy. And yet this article does not seem exhaustive about what the right to privacy consists of. It simply puts indicative list by giving examples. Article 26 the constitution and article 17 of the ICCPR are different in their wording in sense that the former prohibits searches of one's home, person or property, and seizure of one's property whereas the latter prohibits the unlawful or arbitrary interference with private life, home, family and correspondence. It seems to this writer that unlawful or arbitrary interference is broader than unlawful or arbitrary searches and seizures. Unlike the ICCPR and UDHR, the constitution has extended privacy protection to property under one's personal possession; it is silent about protection of family though. Nonetheless, it is still possible to argue the element

---

[66] Proclamation No. 1/1995, the Constitution of the Federal Democratic Republic of Ethiopia, *Negarit Gazeta*, (1995), Articles 9(4) and 13(2).

[67] The First Optional Protocol to the International Covenant on Civil and Political Rights was adopted in 1966 by the UN General Assembly in order to establish internationally an individual complaint mechanism for the ICCPR. According to article 1 of the Protocol, state parties have agreed to recognize the competence of the UN Human Rights Committee to consider complaints from individuals who claim their rights under the Covenant have been violated. To take the case to the Committee, complainants must have exhausted all domestic remedies, and complaints should not be anonymous. The Committee must bring complaints to the attention of the relevant party, which must respond within six months. Following consideration, the Committee must forward its conclusions/views to the party and the complainant. However, its conclusion won't have a binding effect. See articles 2-5 of the protocol.

family is protected within the purview of privacy in Ethiopia for two reasons: first, the list of protected elements under article 26 is open-ended to include family; second the ICCPR is the integral part of the law of the country by the virtue of article 9(4) of the constitution.

Despite the otherwise argument of the Human Rights Committee, the obligation owed to the right to privacy under ICCPR has traditionally been viewed as an obligation to abstain from arbitrary or unlawful interferences with the right. This obligation of negative kind stems from the wording of the article 17 which does not expressly impose positive obligation as well on adherent states. In this regard, even the European Human Rights Convention seems to impose negative obligation. In particular, if we see the language of article 8(2) of the European Human Rights Convention ("there shall be no interference by a *public authority* with the exercise of this right…"), the obligations on state parties appears a negative one, the right to be left alone by public authority. However, the European Court of Human Rights has not perceived the right to privacy in wholly negative terms; instead it has expanded the duties to positive obligation by using the wording 'respect for' under article 8(1).[68] As opposed to this, the first limb of article 26 (3) of the FDRE constitution solves such ambiguity when it explicitly says "public officials shall *respect* and *protect* [the right to privacy]." This sub article conveys that public officials are required not only to refrain themselves from interferences with individual privacy, but also to prevent private persons or entities that would impair the right.

The right to privacy in the constitution is not unfettered right. It may be limited by rights of others and interests of the society. However, the mere benefit of others and general welfare should not be enough to justify an infringement as limitation of the right.[69] Pursuant to article 26(3) of the FDRE constitution, limitations to the right are permissible under the fulfillment of certain cumulative requirements. Limitation to the

[68] D J Harris, M O'Boyle and C Warbrick, supra note 32, p. 303.

[69] Rakebe Messele, Enforcement of Human Rights in Ethiopia, unpublished, Addis Ababa, (2002), p.13.

right to privacy is allowed only when the three important elements are satisfied together. These are: (1) there must be compelling circumstances; (2) interference must be in accordance with specific laws; and (3) there must be legitimate aims. Under article 26(3) of the FDRE constitution, six legitimate objectives are enumerated: national security, public peace, the prevention of crimes, the protection of health, public morality, and the rights and freedoms of others). National security is an amorphous concept at the core of which lies the survival of the state, whereas public safety, the prevention of crime, the protection of health, and public morality reflect society's interest from different angles.[70] The constitutional requirements set to limit privacy right are more or less similar to the requirements stipulated in the European Convention for Protection of Fundamental Rights and Freedoms. The only difference is that the constitution puts the requirement of "compelling circumstances" in lieu of the requirement of "necessary in the democratic society." [71]

Whether or not an interference with privacy is justifiable based on the constitution, the three issues (is there a compelling circumstance to interfere? is the interference based on a specific law? and is the interference for one of the purposes set out in sub article 3?) are sine quo non elements to be addressed. The parameter of "compelling circumstances" may be difficult to define it in the abstract. In any event, the prevailing situation should appear compelling to a reasonable degree to interfere with the right to privacy for one of the legitimate aims. It is also important to consider to what extent the compelling situation limits the right, test of proportionality. And the limitation should be by the virtue of specific law which can be laid down for the purpose of safeguarding national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others. In such situations, the privacy right may be overridden by other values/ public interests.

---

[70] Fasil Nahum, Constitution for a Nation of Nations: the Ethiopian Prospect, Lawrenceville N.J., Red Sea Press, (1997), p. 124.

[71] Article 26(3) of the FDRE Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms, (1950), article 8(2).

Succinctly, interference with privacy right is permissible upon the fulfillment of the aforementioned requirements. Any limitation other than the constitutionally stipulated ones is by no means permissible, and is tantamount to constitutional violation. In this connection, article 9(1) of the constitution is very relevant when it declares that "the constitution is the supreme law of the land; and any law, customary practice or a decision of an organ of state or a public official which contravenes this constitution shall be of no effect." According to Articles 62 and 83 of the FDRE constitution, the power to interpret the constitution and decide constitutional dispute is given to the second chamber, the House Federation. Unlike second chamber of other federations, House of Federation has no or little law-making functions; instead it reviews the constitutionality of laws.[72] This is to say the House Federation can strike any governmental legislation down on the ground that the legislation breaches the constitution.[73] Therefore, any law or decision of government officials which goes against the constitutionally guaranteed right to privacy will be rendered null and void.

3.2.2 Subsidiary laws

In the foregoing section, we have tried to unpack privacy protection at the constitutional level. Normally, constitution of any country consists of general

[72] Assefa Fiseha, Constitutional Adjudication in Ethiopia: Exploring the Experience of the House of Federation (HoF), a paper presented at African Network of Constitutional Law Conference on Fostering Constitutionalism in Africa, Nairobi, (2007), p.9.

[73] Ethiopia has structurally a bicameral parliament, but functionally a unicameral since the upper house (House of Federation) does not involve in law making process. Instead it is empowered to interpret the constitution and decide constitutional disputes. The House of Federation is assisted by an expert body called 'Council of Constitutional Inquiry (CCI)', which examines each case upon which constitutional interpretation is requested and submits its recommendations to the House, which then makes a final binding decision upon cases (Articles 82-84 of the FDRE constitution). The rationale for vesting power of constitutional interpretation in the House of Federation and not in the regular judiciary is that the constitution is considered as the reflection of the 'free will' and 'consent' of nationalities, and therefore the nationalities should be the ones to be vested that power. To this effect, House of Federation, which is composed of the representatives of "nations, nationalities and peoples" of Ethiopia pursuant to article 61(1) of the constitution, is granted the power to review the constitutionality of laws. Constitutional interpretation in Ethiopia is not purely a legal matter, for it is given for a political body believing that the constitution is mainly a political document. See also Assefa Fiseha, Ibid, p. 9-10.

provisions dealing about government structures or organs and their respective powers, and human rights. These constitutionally framed provisions needs subsidiary specific laws for their proper implementation before court of law. Although the right to privacy is guaranteed in the FDRE constitution, Ethiopia does not have still a codified legislation on privacy protection. However, apart from the constitution, one can find scattered privacy provisions in Criminal Procedure Code, Civil Code, and Freedom of Mass Media & Access to Information Proclamation. In this particular section, we are going to discuss what privacy protections are provided by the existing array of laws. To this effect, privacy related provisions in various branches of law will be under our scrutiny.

3.2.2.1 Criminal Procedure law

As has been pointed out earlier, privacy may be limited in accordance with a specific law under compelling circumstances for legitimate aims. Crime prevention is one of the grounds by which the law enforcer can interfere with the privacy of individuals. However, the police officer can not interfere with individuals' privacy arbitrarily under the guise of law enforcement. In this respect, the 1957 Criminal Procedure Code of Ethiopia provides:

Art. 32. - Searches and seizures.

Any investigating police officer or member of the police may make searches or seizures in accordance with the provisions which follow: (1) No arrested person shall be searched except where it is reasonably suspected that he has about his person any articles which may be material as evidence in respect of the offence with which he is accused or is suspected to have committed. A search shall be made by a person of the same sex as the arrested person. (2) No premises may be searched unless the police officer or member of the police is in possession of a

search warrant in the form prescribed in the Third Schedule to this Code except where: (a) an offender is followed in hot pursuit and enters premises or disposes of articles the subject matter of an offence in premises ;(b) information is given to an investigating police officer or member of the police that there is reasonable cause for suspecting that articles which may be material as evidence in respect of an offence in respect of which an accusation or complaint has been made under Art. 14 of this Code and the offence is punishable with more than three years imprisonment, are concealed or lodged in any place and he has good grounds for believing that by reason of the delay in obtaining a search warrant such articles are likely to be removed.

The interests protected under article 32 are body, premises and property of a person against arbitrary searches and seizures respectively. The protection of the individual's person is one of the fundamental aspects of privacy, without such protection there is the threat of physical violence and assaults. As a rule, neither the body of a person nor the premises may be searched. However, this rule may be derogated when the exceptional conditions stated under article 32 (1) & (2) are met. Exceptionally, a police officer can lawfully interfere with the bodily privacy or territorial privacy of individuals as per article 32 of the Criminal Procedure Code in order to prevent crimes (legitimate aim of the interference). And hence, the Criminal Procedure Code of Ethiopia has stipulated the conditions under which searches and seizures are permissible in line with the FDRE constitution.

Beyond bodily and territorial privacy, communications privacy can also be limited in accordance with the law for prevention of crime. As said above, article 26(2) of the FDRE constitution guarantees the right to the inviolability of one's notes and correspondence (communications privacy) including postal letters, and communications made by means of telephone, telecommunications and electronic devices. However, this aspect of privacy can be intercepted in order to investigate and prosecute corruption offences. In this regard, Article 46 of the Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation of Ethiopia states:

(1) Where it is necessary for the investigation of corruption offence, head of the appropriate organ, [an organ empowered to investigate and/or prosecute corruption offences], may order the interception of correspondence by telephone, telecommunications and electronic devices as well as by postal letters… (3) An order given in accordance with sub article (1) of this article shall indicate the offence which gives rise to the interception, and the duration of the interception, and, if it is a telephone or telecommunication, the link to be intercepted. Unless head of the appropriate organ decides otherwise, the duration of the interception may not exceed four months.

Federal Ethics and Anti-corruption Commission (FEAC) of Ethiopia is an independent federal government organ which has a full mandate to investigate and prosecute corruption offences.[74] The commission can order the interception of one's correspondence if it is necessary for investigation of corruption offences. The interception can not, however, be made for indefinite period. In the absence of otherwise decision by the investigating organ, the duration of interception should not be longer than four months.

3.2.2.2 Civil Law

In the 1960 Civil Code of Ethiopia, there are some provisions for protection of privacy. For instance regarding pictures, it is said that the photograph or the image of a person should not be exhibited in a public place, nor reproduced, nor offered for sale without the

[74] Proclamation No.433/2005, the Revised Federal Ethics and Anti-Corruption Commission Establishment, *Negarit Gazeta*, (2005), article 73(2) &(4), and Proclamation No. 434/2005, Revised Anti-Corruption Special Procedure and Rules of Evidence, *Negarit Gazeta*, (2005), article 2(3).

consent such person.[75] Consent is a requirement to display or disclose one's image. However, the consent of a person concerned may not be sought where the production of his image is required for justice, scientific or cultural interests, or public interests.[76] Similarly, in respect of correspondence, the Civil Code provides that "the addressee of a confidential letter may not divulge its contents without the consent of the author."[77] In both cases, consent is very important. The Civil Code entitles the person concerned to control the reproduction of his image or the disclosure of the contents of his letter. From this, one can safely infer the two basic principles of data processing (data subject's participation and disclosure limitation) which are enshrined in EU Data Protection Directive and OECD Privacy Guidelines.

The Civil Code has also protected bodily privacy by setting out that "a person commits a fault where he intentionally makes contact with the person of another against the latter's will."[78] However, as per article 2039(1) of the Civil Code, no fault is deemed to have been committed where the defendant could not reasonably have foreseen that the plaintiff would object to his act. The test of reasonable expectation of privacy seems to be introduced in this article. For instance, a person may touch another person against the latter's will in queue for public transport or in market places where the reasonable expectation of privacy is minimal. And the defendant may not reasonably expect the plaintiff would object the body contact in those places. Regarding bodily privacy, a person is also entitled to refuse at any time to submit himself to a medical or surgical examination or treatment.[79] Protection of bodily privacy pertains to the preservation of an individual's physical integrity. Consent to privacy invasive procedures (trespass against the person, forms of assaults in the medical environment) is normally required.

---

[75] Extraordinary Issue No. 2/1960, The Civil Code Proclamation of the Empire of Ethiopia, *Negarit Gazeta*, (1960), Article 27.

[76] Ibid Article 28.

[77] Ibid Article 31(1).

[78] Ibid Article 38 (1.)

[79] Ibid Article 20 (1).

Furthermore, the Civil Code has prohibited trespassing on the land or into the house of another, and taking the possession of property against the will of the lawful owner or possessor, without due legal authority.[80] In other words, in the absence due legal authority, one can not enter into the house of another person or seize the property of another or trespass on the land of another person unless the latter has consented to that effect. The Civil Code further sets out that a person is at fault when he (by his words, writings or by any other means) acts in such a way as to make another person detestable, contemptible or ridiculous and to jeopardize his credit, his reputation or his future.[81]

At this juncture, one may wonder the remedy available for individuals whose privacy is violated. Depending on the nature and type of the violation, the remedy can be of two fold: civil and criminal. In other words, violations may give rise to both civil and criminal liabilities. Putting aside the criminal liability, the victim can bring an action against the infringer by virtue of law of extra-contractual liability. In Ethiopia, extra-contractual liability is mainly established based on fault, and exceptionally based on strict and vicarious liability.[82] Generally, fault is deemed to have been committed when there is a breach of the usual standard of good conduct by act or forbearance.[83] Pursuant to article 2030(2) of the Civil Code, the standard of good conduct is closely tied up with concept of prudent and diligent person who never commits an act which is bad. The defendant's act is judged in reference to this reasonable man representing usual and good conduct i.e. what a reasonable man would have done in the same circumstances. If this reasonable man would have acted in the same way as the defendant, had he been placed in the shoe of the defendant, the latter is said to have committed no fault. Deviation from the usual standard of good conduct will put the defendant at fault.

Apart from the test of reasonable man standard, Articles 2038-2065 of the Civil Code define what types of conduct constitute fault, and if a person acts or omits in violation of

[80] Ibid Articles 2053 and 2054.

[81] Ibid Article 2044.

[82] Ibid Article 2027.

[83] Ibid Article 2030

one of these provisions, he will be considered as committing fault. Besides, violation of any specific provision of law is fault by virtue of article 2035 of the Civil Code. Therefore, deviation from the above discussed privacy laws (invasion of privacy) is tantamount to fault which may, in turn, spawn civil liability pursuant to article 2028 of the Civil Code ("whosoever causes damage to another by his fault shall make it good"). To conclude, one can bring a lawsuit based on law extra-contractual liability against another so long as the former sustains damage due to the latter's privacy invasive act.

3.2.2.3 Mass Media Law

The FDRE constitution guarantees freedom of expression, opinion and thought under article 29. The freedom of expression as recognized in the constitution consists of the right to seek, receive and impart information and ideas.[84] Accordingly the public is at liberty to receive information about the working of the government representing them. By the same token, press and other mass media are entitled to gather information in the process of seeking ideas and disseminating them to the public. This means that the government is duty bound to be transparent and let its documents accessible to the press so long as it is for public interest. These rights can only be limited through laws guided by the principle that freedom of information and expression can not be limited on account of the content or effect of the point of view expressed.[85] The legal limitation can be laid down for the purpose of protecting the well being of the youth, and the honour and reputation of individuals.[86]

In line with the constitutional provision, the Proclamation on Freedom of Mass Media and Access to Information (Mass Media Law) provides that all persons have the right to

[84] FDRE Constitution, supra note 66 Article 29(2), second limb.

[85] Ibid Article 29(6).

[86] Ibid.

seek, obtain and communicate any information held by public bodies, except exempted information therein.[87] The exempted information from disclosure is *inter alia* personal information. In this respect, article 16(1) of the Mass Media Law goes "Any public relation officer must reject a request for access to a record of the public body if its disclosure would involve the unreasonable disclosure of personal information about third party, including a deceased individual who has passed away before 20 years." Had it not been this provision, the personal information of a person would have been at risk in the course of seeking and disseminating information. However sub article 2 of the same article stipulates situations (including the consent of the person concerned) under which personal information may be disclosed.

At this juncture, it is very important to query what kind of information is considered as personal one, and is exempted from being disclosed. Fortunately, the Mass Media law of Ethiopia has clearly defined what personal information means. Pursuant to Article 2(8) of the Mass Media Proclamation,

> '*Personal information' means information about an identifiable individual, including but not limited to: (a) information relating to the medical or educational or the academic, employment, professional or criminal history, of the individual or information relating financial transactions in which the individual has been involved; (b) information relating to the ethnic, national or social origin, age, pregnancy, marital status, colour, sexual orientation, physical or mental health, wellbeing, disability, religion, belief, conscience, culture, language or birth of the individual; (c)information relating to any identifying number, symbol or other particular assigned to the individual, the address, fingerprints or blood type of the individual; (d) the personal opinions, views or preferences of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual; (e) the views or opinions of another individuals about a proposal for a grant, an award or a prize to be made to the*

[87] Proclamation No.590/2008, Freedom of Mass Media and Access to Information, *Negarit Gazeta*, (2008), Article 12(1) and Article 15.

individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; (f) the views or opinions of another individual; or (h) the name of the individuals where it appears with other personal information relating to the individual or where the disclosing of the name itself would reveal information about the individual; but excluding information about a person who has passed away before 20 years.

In short, personal information is any information about an identifiable individual. This provision has attempted to list examples of personal information without being exhaustive. To the best knowledge of this writer, it is very difficult to see a reason why the legislature goes to such a long list insofar as the list is illustrative. If it were to make the list exhaustive, it would be sensible. Unlike the definition of EU Data Protection Directive, this definition expressly include biological material of an individual when article 2 (8) (c) refers "information relating to any identifying number, symbol or other particular assigned to the individual, the address, fingerprints or blood type of the individual" to be personal information. Indeed, the definition is broad enough to include any information about identifiable person, but is muted about information relating to an identified person. One may wonder at this point that what if the information is related to an identified person. This writer believes that if information about an identifiable person (who is going to be identified through the use of one or the combination of such information) is treated personal information, information about an identified person must be personal one for stronger reason. In this regard, the EU Data Protection Directive has made it clear by saying personal data means any information related to an identified or identifiable individual.[88]

As has expressly been stipulated under article 16 of the Mass Media Law, personal information held by public body should not be disclosed under the guise of access to the records of the latter. This article contains one of the basic principles of personal data processing i.e. disclosure limitation. However, its scope is limited in the sense

[88] Directive 95/46/EC of the European Parliament and of the Council, the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, (1995), Article 2(a).

that it refers to personal information held by only public body. This provision does not say any thing about personal information held by private sectors.

3.3 Inadequacy of Privacy Protection Laws

In the preceding discussion, we have examined the relevant provisions for privacy protection within the purview of Ethiopian legal system. In this particular section, we will indulge into areas that are not provided protection by those provisions. As has been indicated in section 2.1, privacy has several dimensions – territorial privacy, bodily privacy, privacy of communications, and information privacy. The ICCPR and the FDRE constitution have given recognition for the right to privacy, which needs specific laws for its effective enforcement. The above discussed provisions of the Criminal Procedure Code, Mass Media Law and the Civil Code mainly focus on some aspects of privacy: bodily, territorial and communications privacy. Information privacy appears less protected.

Information privacy concerns the collection, use and disclosure of personal information. The regulation of information privacy is to protect private information about an individual which is not intended by the individual to make public or over which the individual wishes to retain control. In view of this, EU Data Protection Directive has enshrined the core principles for protection of personal information, which can be expressed in terms of lawful and fair data processing, minimality, purpose specification, data quality, data subject participation and control, disclosure limitation, information security and sensitivity.[89] These principles are also reflected in the national laws of EU countries. As seen in section 2.4, the OECD guidelines too have contained those basic principles which highly influence the national laws of member states.

[89] Ibid, Articles 5-8.

Turning to the Ethiopian legal system, there are no laws which explicitly deal with the core principles of personal data processing. Nonetheless, one can safely conclude from the foregoing discussion that the principles of disclosure limitation and data subject participation (consent) are embodied in the Ethiopian privacy protection provisions. However, the two principles are applicable to a limited degree. For instance, the non-disclosure principle in Mass Media law is confined to personal information held by public organ, not by private sectors. As has been explained in section 3.1, information and communication technology is growing steadfastly which in turn let a wide and uncontrolled personal data processing and dissemination by both public and private sectors. To the dismay of individual's privacy right, the existing provisions related to privacy do not suffice to regulate personal data collection, processing, and flow across institutional as well as national boundaries. This is the reason why this writer believes that the personal information aspect of privacy has received little protection by the existing law of Ethiopia.

Chapter Four

4 The Need for Privacy Law

As we can understand from the previous discussion, the existing laws within the legal framework are not capable to protect privacy to its fullest. In other words, privacy related provisions incorporated in various branch of laws of the country do not suffice to provide protection for manifold aspects of privacy, particularly information privacy. This being so, this writer would like to recommend the enactment of a comprehensive piece of legislation for the following compelling reasons: to protect human rights, to promote e-commerce, and to govern technological advancements. Let us see the compelling reasons one by one.

4.1 Human Rights Protection

States establish legally binding obligations among themselves by entering into an international agreement or through wide accepted state practice of a rule as customary international law.[90] As treaties under international law, the Covenants and other human rights instruments create legally binding obligations for states that have ratified the instruments. Regarding the obligation of state parties, the ICCPR provides that every state party to the Covenant should respect and ensure to all individual within its territory the rights recognized therein[91]. Article 2(2) of the ICCPR further stipulates that each state party is under obligation to enact legislation and create the framework to give effect the rights enshrined in the Covenant.

---

[90] Richard B. Bilder, An Overview of International Human Rights Law, in Hurst Hannum (ed.), Guide to International Human Rights Practice, (2nd ed.), University of Pennsylvania Press, (1992), p.9.

[91] General Assembly Res. 2200A (XXI), supra note 28, Article 2(1).

In the international human rights law, privacy is clearly and unequivocally established as a fundamental right to be protected. Accordingly, states are duty bound to respect and protect the right to privacy within their jurisdiction. The degree of obligations range from abstaining from interference with privacy to protecting individual's right from being infringed by other. As a state party to ICCPR, Ethiopia must, therefore, comply with the international obligations undertaken at the international level. Not only should the country refrain from interference with privacy of individual, but also should take some positive measures including enacting piece of legislation for effective implementation of the right. Given the growth of the gathering and holding of personal information on computers, data banks and other devices by public authorities or private sectors, failure to have legislation is tantamount to non-compliance with international obligations, which renders human rights particularly privacy right ineffective. Information concerning a person's private life may reach the hands of persons who are not authorized by law to receive, process, and use it, which, in effect, threatens the privacy of individual.

Apart from international obligation, Ethiopia has a national obligation to take the necessary measures for the effective enforcement of human rights enshrined in the FDRE constitution. In this connection, the constitution says "All Federal and State legislative, executive and judicial organs at all levels shall have the responsibility and duty to respect and enforce the provisions of [human rights]."[92] As per this provision, federal and state legislatives should exercise their power for the effective implementation of human rights, including privacy right. The inherent power of legislative organ is, obviously, to make laws. Accordingly, the federal and state law making organs are obliged to enact laws for protection of privacy as guaranteed in the constitution and in the Covenant. To put succinctly, the enactment of piece legislation for privacy protection is very indispensable to discharge international as well as national obligations owed to human rights. The main purpose of having such law is to protect the fundamental human rights, in particular the right to privacy.

[92] FDRE Constitution, supra note 66, Article 13 (1).

4.2 Electronic Commerce Promotion

The global economy has increasingly become dependent upon information technology which has enabled a growth of international communication and commerce.[93] Commerce now requires the transfer of huge quantities of personal data, largely relating to employees and customers.[94] Thus, personal information increasingly flows across the borders of different nations around the world. As pointed out in section 2.5, privacy laws and regulations have evolved in various nations. However, this raises two difficulties: (1) differing level of protection might interfere with the smooth and efficient flow of personal information between countries, (2) countries seeking to protect the privacy of their citizens must depend upon the protections accorded by other countries.[95] There is thus a need for harmonization or convergence of approaches to regulating the processing of personal information.

In view of this, both the OECD Guidelines and the EU Data Protection Directive contain rules for trans-border data flows – the flow of information between different countries.[96] The OECD guidelines 15-18 regulate trans-border data flows among member states, but the guidelines are silent about the flow of data outside member states. On the other hand, the EU Data Protection Directive regulates the transfer of data across national borders in two ways: letting the flow of information free within the community as indicated in article 1(1) of the Directive, and putting the requirement of adequacy test for transfer of data outside Europe as envisaged article 25 and 26 of the Directive. The EU makes the flow of information within the community free by increasing the level of harmonization, and puts pressure on other countries to adopt legislation satisfying adequate protection.

---

[93] Daniel J. Solove and Marc Rotenberg, supra note 5, p.735.

[94] David Bender and Larry Ponemon, supra note 49, P. 154.

[95] Daniel J. Solove and Marc Rotenberg, supra note 5, p.735.

[96] Supra note 60, OECD Guidelines 15-18 and EU Data Protection Directive, supra note 88, Articles 25 and 26.

As per article 25(1) of the EU Data Protection Directive, member states are required to ensure that personal data, that are undergoing processing or are intended for processing after transfer, are not transferred outside the EU or European Economic Area to a third country unless that third country has put in place adequate level of protection. As indicated in paragraph 2 of article 25 of the Directive, whether that third party has put in place adequate level of protection for personal data processing, it must be examined in light "all the circumstances surrounding a data transfer operation or set of data transfer operations," in particular the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law in force both general and sectoral, the professional rules and security measures.

Pursuant to article 26 of the Directive, where a third country fails to fulfill the requirement of adequate level of protection, personal information can be transferred on the following conditions: (1) the data subject has given unambiguous consent to the proposed transfer; (2) the transfer is necessary for the performance of a contract between the data subject and the controller of the data, or for one of several other specific purposes; (3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; (4) the transfer involves data that is essentially public; (5) the transfer is necessary to the vital interests of the data subject; or (6) a contract is in place between data exporter and importer, that requires adequate safeguards by the importer. Accordingly, United States (whose privacy law fails to provide adequate level of protection in the eyes of EU) has responded to the EU Directive by putting safe harbor arrangement which provides adequate protection for personal data transferred from the EU.

Turning to Ethiopia, the country is not an exception. The country is required to satisfy the adequate level of protection for transfer of personal data from Europe. Ethiopia has, wants to have extensive trade relations with European countries as well as other foreign countries. It has also attempted to privatize many sectors so that foreign investors can participate in the economy. The existence of appropriate and efficient law is very

important to regulate and promote investment. So long as the Ethiopian law is found to lack of adequate protection of privacy, it will encounter limits on the transfers of personal information. Limitations on the flow of personal information discourage investment and commerce. Beyond trans-border data flow, the enactment of privacy law is equally important to put the legal framework in place for e-commerce within the country. Thus, the enactment of privacy law is very essential to facilitate e-commerce (which the country will introduce it in the future), international trade and investment.

4.3 Technological Developments Regulation

The recognition of privacy as a concept worthy of distinct treatment by the law dates back to an article called "The Right to Privacy" in the 1890 Harvard Law Review, which was inspired by the rise of newspapers, photography and other technologies with the potential to expose people's images and personal information to the public.[97] Recently, fresh privacy concerns again arose as a result of technological developments, notably the spectacular growth of automatic data processing made possible by the computer revolution.[98] The modern world is a time of telephoto lenses, long-range parabolic microphones, and mobile phone cameras, as well as other technological advances such as the internet that provide easy means of dissemination of information to a world wide audience.[99] These advances mean that there is now nowhere on earth that a person may retreat with an absolute assurance of being left alone. The public concern is focused on the impact of information revolution upon our lives, in particular where this interface impacts upon our ability to lead a private life.

---

[97] Gehan Gunasekara, The 'Final' Privacy Frontier? Regulating Trans-border Data Flows, International Journal of Law and Information Technology, Vol.15, No.3, Oxford University Press, (2006), p. 365.

[98] Ibid.

[99] Des Butler, A Tort of Invasion of Privacy in Australia, an article available at http://www.austlii.edu.au/au/journals/MULR/2005/11.html#Heading345, visited on 26/07/2009.

Currently, information and communication technologies have been increasingly developed in Ethiopia. Access to means of widespread publicity is now at the fingertips of government institutions as well as private sectors. This may in turn let public and private sectors to collect, process, and transfer personal data. And hence there is a need for law to accommodate developments in technology and changes in attitudes, practices and values in the society.

Conclusion

Different authors have defined privacy differently. Privacy has been described as the right to be left alone, the right to exercise control over one's personal information, limited accessibility, or intimacy. Nonetheless, there is no universally accepted definition of privacy. Defining the concept has been found complicated and a difficult task. Regardless the absence of a universally accepted definition of privacy, the quest and need of privacy is natural and a real one. The protection of privacy is very essential to safeguard personhood, autonomy, integrity and dignity of human being. The term should be understood to include all aspects of privacy, namely bodily privacy, information privacy, communication privacy and territorial privacy. And privacy laws should provide protection to every aspect of privacy.

Recently, privacy laws in many jurisdictions have emerged in order to protect privacy. Indeed, the evolution of privacy laws has been catalyzed by various factors. The first being, most major human rights instruments have recognized privacy as a fundamental human right. The vast majority of countries of the world are parties to those human rights documents which in turn require the contracting states to ensure that their domestic legal systems provide adequate protection against interference with privacy. Accordingly, despite differing level of protection accorded and cultural differences, the notion of privacy has already been introduced in many countries legal system. Secondly, the continued development of information technology has had a huge impact upon the right to privacy. In other words, the advancement of information technologies has increasingly

threatened the privacy of individuals, for the technologies have made the collection, processing and transfer of personal information easier. Conspicuously, most information technologies are privacy invasive. This being so, many countries have begun to regulate the adverse effect of information technologies on individual's privacy. The advancement of information technologies is, therefore, the other factor for the emergence of privacy laws such as Council of Europe Convention on Personal Data Protection, EU Data Protection Directive, national privacy laws of different countries and OECD Privacy Guidelines. In shaping the national laws of various countries, the EU Data Protection Directive and the OECD Privacy Guidelines have played a great role throughout the world.

As a party to the ICCPR, Ethiopia has undertaken an international obligation for the protection of privacy. In line with this obligation, the country has enshrined the right to privacy in its constitution. Despite the constitutional guarantee of privacy and the steadfast development of information technologies in the country, there is lack of specific piece of legislation for the full enforcement of the right. As discussed, we are, however, able to find some relevant provisions of different branches of the law for protection of privacy. And yet, those provisions are not sufficient enough to protect the multidimensional concept of privacy. For instance, the existing law does not sufficiently regulate how personal information can be collected, processed and transferred. They are also very limited in the scope of protection.

The need for privacy law is imperative. The reasons being: first, Ethiopia has internationally consented to protect and promote human rights recognized by international agreements. Over and above, the country has constitutionally recognized the right to privacy. And hence particular law is a must to implement the right incorporated in general terms. Secondly, the country has conducted international trade with foreign countries, which require the transfer of personal information. Knowing the absence of protection to personal information, foreign countries may withhold the flow of personal data, and thereby obstruct trade relations. Moreover, sooner or later, the country will certainly introduce e-payment which involves personal information. The enactment of

privacy law is, therefore, indispensable to foster international trade as well as to lay a legal foundation for e-commerce. Thirdly, the information technologies, which affect society in many ways, need to be regulated. The law may lag behind the technological advancements. This can seldom be inevitable, for there are difficult times for legislators to make laws before hand and regulate certain technological developments. In any event, the law should not remain behind indefinitely. The law should be dynamic to regulate technologies, and innovation. And hence, Ethiopia needs to promulgate privacy laws to cope up with the development of information technologies.

References

List of Judgments

Malone v United Kingdom, (1984), 7 EHRR14.

Silver v United Kingdom, (1983), 5 EHRR347.

Salov v. Ukraine, European Court of Human Rights, Strasbourg, (2005).

International/Regional Treaties

Directive 95/46/EC of the European Parliament and of the Council, the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, (1995).

General Assembly Res. 45/158 of 18 December 1990, International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families.

General Assembly Res. 44/25 of 20 November 1989, Convention on the Rights of the Child.

Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series No. 108, /1981).

African Charter on Human and Peoples' Rights, Nairobi, (1981).

OECD Guidelines on the Protection of Privacy and Trans-border flows of Personal Data, (1980).

OAS Treaty Series No. 36 of 1969, American Convention on Human Rights.

General Assembly Res. 2200(XXI) of 16 December 1966, International Covenant on Civil and Political Rights.

General Assembly Res. 2200A (XXI) of 1966, Optional Protocol to International Covenant on Civil and Political Rights.

OAS Res. XXX**,** American Declaration of the Rights and Duties of Man, (1948).

Charter of the United Nations, San Francisco, (1945).

National Laws

Proclamation No.590/2008, Freedom of Mass Media and Access to Information, *Negarit Gazeta*, (2008).

Proclamation No. 434/2005, the Revised Anti-Corruption Special Procedure and Rules of Evidence, *Negarit Gazeta*, (2005).

Proclamation No.433/2005, the Revised Federal Ethics and Anti-Corruption Commission Establishment, *Negarit Gazeta*, (2005).

Proclamation No. 281/2002, A Proclamation to Provide for the Amendment of Telecommunication Proclamation, *Negarit Gazeta*, (2002).

Proclamation No.49/1996, A proclamation to Provide for the Regulation of Telecommunications, *Negarit Gazeta*, (1996).

Proclamation No. 1/1995, the Constitution of the Federal Democratic Republic of Ethiopia, *Negarit Gazeta*, (1995).

Extraordinary Issue No. 2/1960, the Civil Code Proclamation of the Empire of Ethiopia, *Negarit Gazeta*, (1960).

Proclamation No. 185/1961, Criminal Procedure Code of Ethiopia, *Negarit Gazeta*, (1961).

Books and Articles

Agre, Philip E. and Rotenberg, Marc, Technology and Privacy: the New Landscape, the MIT Press, Cambridge, Massachusetts, (1998).

Banisar, David Privacy and Human Rights, Electronic Privacy Information Centre, Washington, DC, (2000).

Bender, David and Ponemon, Larry, Binding Corporate Rules for Cross-Border Data Transfer, Rutgers Journal of Law and Urban Policy, Vol.3:2, (2006).

Bert J. Koops, Bert J. and Leenes, Ronald, 'Code' and the Slow Erosion of Privacy, 12 Mich Telecomm, Tech.L.Rev. 115, (2005).

Bilder, Richard B., An Overview of International Human Rights Law, in Hurst Hannum (ed.), Guide to International Human Rights Practice, (2nd ed.), University of Pennsylvania Press, (1992).

Buergenthal, Thomas *et a*l, International Human Rights Law in a nutshell, 3rd ed., west Group, (2004).

Bygrave, Lee A., Data Protection law: Approaching its Rationale, Logic and Limits, (2002).

David Brin, Transparent Society-Will Technology Force Us to Choose Between Privacy and Freedom? Addison-Wesely, Reading/Massachusetts, (1998).

Gavison, Ruth, Privacy and the Limits of Law, the Yale Law Journal, Vol.89, No.3, (1980).

Gunasekara, Gehan, the 'Final' Privacy Frontier? Regulating Trans-border Data Flows, International Journal of Law and Information Technology, Vol.15, No.3, Oxford University Press, (2006).

Harris DJ, O'Boyle M and Warbrick C, Law of the European Convention on Human Rights, Butterworth, London, (1995).

International Telecommunication Union, Internet from the Horn of Africa: Ethiopia case study, Geneva (2002).

Jacobs Francis G. and White, Robin C.A., the European Convention on Human Rights, Oxford University press, 4th ed, (2006).

Koops, Bert-Jaap and Leenes, Ronald, 'Code' and the Slow Erosion of Privacy, 12 Mich. Telecom., Tech. L. Rev. 115 (2005).

Leach, Philip, Taking a Case to the European Court of Human Rights, Blackstone Press Limited, (2001).

Lioyd, Ian J., Information Technology Law, Oxford University press, 4th ed., (2004).

Michael, James, Privacy and Human Rights: an International and Comparative Study, with Special Reference to Developments in Information Technology, Dartmouth, UNESCO Publishing, (1994).

Nahum, Fasil, Constitution for a Nation of Nations: the Ethiopian Prospect, Lawrenceville N.J., Red Sea Press, (1997).

Nowak, Manfred, UN Convention on Civil and Political Rights: CCPR Commentary, N.P. Engel, publisher Kehl, Strasbourg, Arlington, (1993).

Phillips, David J., Cryptography, Secrets, and Structuring of Trust, in Philip E. Agre and Marc Rotenberg, Technology and Privacy: the New Landscape, Cambridge, the MIT Press, (1998).

Powers, Madison, A Cognitive Access Definition of Privacy, Law and philosophy, vol.15, iss: 4, (1996).

Solove, Daniel J. and Rotenberg, Marc Information Privacy Law, Aspen publishers, New York, (2003).

Wacks, Raymond, Personal Information: Privacy and Law, Oxford, Clarendon Press, (1989).

Wahlgren, Peter (ed.), IT law, Scandinavian Studies in Law Vol.47, Stockholm Institute for Scandinavian Law, (2004).

Warren, Samuel D. and Brandeis, Louis D., the Right to Privacy, Harvard Law Review, Vol. IV, No.5 (1809).

Whiteman, James Q., the Two Western Cultures of Privacy: Dignity versus Liberty, Yale Law Journal, Vol.113, (2004).

Ziegler, Katja S. Human Rights and Private Law-Privacy as Autonomy, Oxford and Portland, Hart Publishing, (2007).

Unpublished Materials

Adam, Lishan, Information and Communication in Ethiopia: Past, Present and Future Potential for Social and Economic Development, Ethiopian Information Technology Professional Association Workshop, Addis Ababa, (1999).

Des Butler, A Tort of Invasion of Privacy in Australia, an article available at http://www.austlii.edu.au/au/journals/MULR/2005/11.html#Heading345, visited on 26/07/2009.

Fiseha, Assefa, Constitutional Adjudication in Ethiopia: Exploring the Experience of the House of Federation (HoF), a paper presented at African Network of Constitutional Law Conference on Fostering Constitutionalism in Africa, Nairobi, (2007).

Ethiopian Telecommunication web site, http://www.ethionet.et/aboutus/historybackground.html, visited on 24 June 2009.

The Human Rights Committee, General Comment No.16, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc. HRC/08/04/88 (1988).

Messele, Rakebe, Enforcement of Human Rights in Ethiopia, unpublished, Addis Ababa, (2002).

A National Information and Communication Technologies Policy, Addis Ababa, (2001).