Safeguards of the Right to Privacy in Ethiopia: A Critique of Laws and Practices

Kinfe Micheal Yilma* and Alebachew Birhanu **

"Without Privacy, we lose our very integrity as persons"

Charles Fried, Privacy, 77 Yale L. J. 475, 1968

Introduction

Privacy as a modern concept is largely a recent phenomenon dating back to a seminal law review article authored by Samuel Warren and Louis Brandeis in 1890. Claims for privacy nevertheless are essentially part of our human desire to seek seclusion with regard to a range of individual, family and community activities. Sociologists and anthropologists have also read claims of privacy into numerous primitive societies. Modern societies embody more refined and broader privacy demands and trends. The surge of new technologies and, very recently, the digital revolution have presented both challenges and opportunities to privacy claims of individuals, family and the community at large. With ever increasing capacity of digital storage and retrieval, individuals and organizations are increasingly losing control of their private and intimate information. Indeed, technology has equally enhanced the capacity of individuals to remain anonymous in their digital persona.

Ethiopia has recognized right to privacy throughout its brief constitutional history, albeit to a different degree. The first written constitution of 1931 explicitly recognized the right of Ethiopian subjects not to be subjected to domiciliary searches and the right to confidentiality of correspondences

except in cases provided by law.[1] These rights were also incorporated with more amplified tone in the revised constitution of 1955.[2] The 1987 Constitution did guarantee Ethiopians the right to the inviolability of their persons and home along with secrecy of correspondences.[3] The Transitional Government Charter didn't make a specific reference to privacy safeguards; but it did state that all rights provided for under the Universal Declaration of Human Rights (UDHR) shall be fully respected, and without any limitation whatsoever.[4] A more comprehensive privacy safeguard is introduced by the 1995 Federal Democratic Republic of Ethiopia Constitution (FDRE constitution) which protects privacy of persons, their home and correspondences. The privacy provision of the FDRE Constitution is apparently informed by the privacy provisions of the UDHR and the International Covenant on Civil Political Rights (ICCPR) to which Ethiopia is a party.

Yet, despite relatively longer constitutional recognition of the right to privacy, little has been written to illuminate the scope and the extent of the right. This article has two main aims. First, it aims at lessening this gap by presenting a firsthand critique on the privacy implication of laws enacted in the aftermath of the FDRE Constitution, and certain practices with potential

---

* Lecturer, Hawassa University Law School, LL.B. (Addis Ababa University), LL.M. (University of Oslo). The author also studied Internet Privacy at Oxford Internet Institute, University of Oxford.

** Lecturer, Bahir Dar University Law School, LL.B. (Addis Ababa University), LL.M. and MPhil (University of Oslo).

[1] The Ethiopian Constitution of 1931, Established in the Reign of His Majesty Haile Sillassie I, 1th July 1931, Arts 25 and 26.

[2] The Revised Constitution of the Empire of Ethiopia of 1955, Established in the Reign of His Majesty Haile Sillassie I, 4th November 1955, Arts 42 and 61.

[3] The Constitution of the People's Democratic Republic of Ethiopia, Proclamation No. 1, Negarit Gazetta, Vol. 47, No. 1, 12 September 1987, Arts 43 and 49.

[4] The Transition Period Charter of Ethiopia, No. 1, Negarit Gazeta, 50th Year, No. 1, 22nd July 1991, Art 1.

privacy ramification. A closer scrutiny of these legislations throws light on the scope of the right to privacy under the FDRE constitution. Legislators and executive authorities might also draw relevant insight in understanding the impacts of their proposals against privacy rights. The second and related aim is to set a research agenda for further extensive studies on the subject.

The article is organized as follows. The first section deals with background issues on privacy such as its origin, its place in primitive and modern societies, and the various conceptualization of privacy. The second section presents privacy as human right. In so doing, it describes privacy provisions of major international human rights instruments along with relevant case law. The privacy provision of the FRDE Constitution is also described. The third section is devoted to examine the privacy implications of various laws and practices ranging from tax seizure rules, new telecom fraud offenses law, anti-terrorism and anti-corruption proclamations and rules on unsolicited communications to evolving privacy invasive media practices. Ongoing legislative initiatives are also addressed in passing. Finally, conclusions and suggestions are offered.

1. Conceptual Background of Claims to Privacy[5]

1.1 Privacy in Primitive Societies

The claims for privacy had long been regarded as the value of the modern world absent from the social fabric of primitive societies of the past and present. Nevertheless, anthropological and sociological studies conducted decades back revealed that needs for privacy for individuals and groups are present in virtually every society. And, privacy norms for a society are

[5] Discussions under section 1.1-1.3 are partly adapted from A. Westin's, *Privacy and Freedom* (Atheneum: New York, 1967).

established at the levels of individuals, family as well as the community as a whole. According to these studies, individuals in virtually every society engage in a continuous personal process by which s/he seeks privacy at some times and disclosure or companionship at other times.[6] The reason for the universality of this process is that individuals have conflicting roles to play in any society; to play these different roles with different persons, the individual must present a different self at various times.

The claims to individual privacy gave rise to some other limits on inter-personal disclosure. The individual's moments of birth, illness and death are considered taboo and are secluded from the general view in many societies. Needs for privacy do appear in the intimacy of sexual relations, the par-territory as some call it. Norms of privacy are also to be found in the family-household settings of primitive life. Whether the household is nuclear or extended, most societies have rules limiting free entry into the house by non-residents, as well as rules governing the outsider's conduct once s/he enters. Even in those societies where entry is fairly free, there will usually be rules limiting what a person may touch or where s/he may go within the house. There will also be norms limiting family conversations or acts performed while outsiders are present.

Privacy for certain group ceremonies is another characteristic of primitive societies. One major example involves the rites of passage, by which girls and boys, as they come of age, are withdrawn from the whole group, go into seclusion, participate in special ceremonies, and then reenter as 'adults'. Universality of privacy claims is also manifested during times of spiritual connection with gods. Whatever the manner in which the individual

[6] Ibid, p. 13.

establishes initial contact with the spirits or gods, s/he will seek privacy in order to communicate with his/her guardian spirits. When man/woman seeks to reach his/her guardian spirit, s/he seeks privacy-usually by physical solitude in a deserted place or church but also by psychological isolation through self-induced trance or reverie if the individual cannot escape the physical presence of others.

1.2. Privacy in Modern Societies

There are variations on the attitude towards privacy and freedom in modern societies. This is basically reflected in the political ideology and systems that a society adopts or is ruled by. Westin eloquently compares the privacy tendencies of modern democratic and totalitarian systems as: [7]

> Totalitarian states rely on secrecy for the regime, but high surveillance and disclosure for all other groups. With their demand for a complete commitment of loyalties to the regime, the literature of both fascism and communism traditionally attacks the idea of privacy as 'immoral', 'antisocial', and part of the cult of individualism.
>
> ....
>
> Liberal democratic theory assumes that a good life for the individual must have substantial areas of interest apart from political participation. Personal retreats for securing perspective and critical judgment are also significant for democratic life.

Nevertheless, the explosion of information and communication technologies and the ensuing comprehensive digital storage present privacy concerns to all political systems. In the face of the ever increasing capacity of digital storage and retrieval, online activities mainly through social networking sites are

[7] Ibid, p. 24.

easily recorded and hence become publicly available. Crawling search engines index the World Wide Web, making information accessible to all of us by merely typing a word or two into a search field.[8] Already a number of cell phones sport GPS receivers making it possible to locate us and take our movements with precision.[9] In line with these developments, various regulatory measures have so far been adopted both by public authorities and the private sector. The recently proposed right to be forgotten in the European Union by which individuals could seek deletion of personal data in the hands of data controllers is a good case in point.[10] The private sector is also piggybacking such legislative measures with technical means of enabling individuals to gain control of their personal information.[11]

1.3. Conceptualizations of Privacy

Privacy as a concept is regarded as a slippery notion, one that is often and easily used but with imprecise meaning.[12] The difficulty in defining privacy lies in it being a value so complex, so entangled in competing and

---

[8] V.Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009), p. 6.

[9] Ibid, p. 9.

[10] Regulation of the European Union Parliament and of the Council on the Protection of Individuals with regards to the Processing of Personal Data and on the Movement of Such Data, COM (2012) 11 final, Art 17.

[11] A software called *"X-Pire"* which enables social networking site users to set expiry dates to data (be photos, status updates or comments) they put online. TigerText, named after the Tiger Woods SMS scandals, is also another example by which one can fix expiry dates to SMS and MMS that s/he sends out. See, J. Rosen, ''Free Speech, Privacy, And The Web That Never Forgets (Keynote Address)'', *Journal on Telecommunication and High Technology Law*, Vol. 9, 2011, p.353. While this article is in the process of publication, the State of California has passed a law that gives a right to under 18 internet users the right to delete their internet contents such as facebook status updates, comments, posts, tweets etc from social networking sites also called web 2.0 platforms. See, Californian Law Gives Teens Right to Delete Web Posts, BBC News, Technology, 24 September 2013. Available at <http://www.bbc.co.uk/news/technology-24227095> [Accessed on September 27/2013]

[12] B. Koops and R. Leenes, "Code and the Slow Erosion of Privacy", *Mich. Telecomm. Tech. L. Rev.*, Vol. 12, 2005, p. 123.

contradictory dimensions, so engorged with various and distinct meanings.[13]As Judith Thomson writes, 'nobody seems to have a clear idea of what it is'.[14] Despite the uncertainty on the exact meaning of the value-laden concepts of privacy, privacy experts proffered varying explanations within the ambit of their discussions in particular contexts.

In discussing values and interests safeguarded by data protection law, Lee Bygrave identifies four major conceptualizations of privacy. Privacy as non-interference as advanced by Samuel Warren and Louise Brandeis is the first conception of privacy. According to Warren and Brandeis, the right to privacy forms part of right to be let alone such as the right not be photographed without one's will. [15] Clinton Rossiter's description of privacy as a 'special kind of independence that seeks to erect an unreachable wall of dignity and reserve against the entire world' also squarely falls in this category.[16] The second category describes privacy as inaccessibility in terms of informational secrecy, physical solitude and anonymity in the crowd.[17]

Westin's informational control definition of privacy as: 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'

---

[13] R. Post, "Three Concepts of Privacy", *The Georgetown Law Journal*, Vol. 89, 2001, p. 2087. Post writes elsewhere that 'privacy is a value asserted by individuals against the demand of a curious and intrusive society'. See, R. Post, "The Social Foundations of Privacy: Community and Self in Common Law Tort", California Law Review, Vol. 77, No. 5, 1989, p. 958.

[14] J. Thomson, "The Right to Privacy" in F. Schoeman (ed.), *Philosophical Dimension of Privacy: An Anthology* (Cambridge University Press1984), pp. 272, 286.

[15] L. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002), pp. 128-131.

[16] C. Rossiter, "The Pattern of Liberty", in M. Konvitz and C. Rossiter (eds.), *Aspects of Liberty: Essays Presented to Robert Cushman,* (Cornel University Press, 1958), pp. 15-17.

[17] In describing privacy as a limitation of other's access to an individual, Ruth Gavison gave an influential and popular definition representing the second category. See, R. Gavison, "Privacy and the Limits of Law", Yale Law Journal, Vol. 89, No. 3, 1980, p. 428.

represents the third group.[18] James Rachel and Lawrence Lessig's definitions of privacy as 'the control we have over information about ourselves'[19] and 'our ability to control'[20] respectively fall within this category. The fourth category relates privacy exclusively to those aspects of person's lives that are 'intimate' and/or 'sensitive'.[21] According to this view, a loss of privacy occurs only when sensitive and/or intimate personal information is disclosed.[22]

Jeffery Rosen identifies three distinct concepts of privacy: privacy as knowledge, privacy as dignity and privacy as freedom.[23] In the first case, privacy blocks flow of information that would otherwise create misconception or misrepresentation by the public.[24] It helps to clog creation of superficial public knowledge about oneself that would create misrepresentation and distress to the individual. In so doing, privacy prevents disclosure of the kind of information that cannot be adequately understood in the absence of special circumstances like intimacy.[25] Hence, it protects the right to define oneself as something more than stereotype. This conception of privacy is however criticized as the public defines persons for its own purposes and in its own ways, and these public definitions almost always constitute stereotypes and generalizations. [26]

---

[18] Westin, supra note 5, p. 7.
[19] J. Rachels, ''Why Privacy Is Important'', *Philosophy and Public Affairs*, Vol. 4, No. 4, 1975, p. 323 *et seq.*
[20] L. Lessig, *Code Version 2.0* (Basic Books, 2002), p. 200 *et seq.*
[21] Bygrave, supra note 15, p. 129, citing JC Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press, 1997), p. 140.
[22] Ibid.
[23] J. Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, 2000), p. 8 *et seq.*
[24] Ibid, p. 10.
[25] Ibid.
[26] Post, supra note 13, p. 2090.

Privacy as a safeguard of dignity is the second privacy notion identified by Jeffery Rosen. According to him, invasion of privacy can constitute an intrinsic offense against individual dignity, and such offenses cause harms irrespective of contingent consequences such as public misconceptions.[27] The third concept of privacy identified by Jeffery Rosen defines privacy as freedom. According to this view, privacy protects a space for negotiating legitimately different views of good life, freeing themselves from the constant burden of justifying their differences.[28] Privacy as freedom carves out a space in which individuals can be allowed to define themselves.[29] Privacy interjects in preserving private spaces for those activities about which there are legitimately varying views, activities no one in a civilized society should be forced to submit similarly.

As can easily be gleaned from the foregoing, privacy is apparently value-laden concept and therefore any effort to give a single comprehensive definition is bound to cause contextual incongruity. Nevertheless, for the purpose of this article privacy is meant to represent the syndicate of the four variants of definitions noted at the outset. Depending on the circumstances of a case, privacy includes the right to be let alone from interference, the right to control flow of one personal information, the right to keep the level of accessibility to ones domains and the right to decide who has access to ones intimate spheres. Besides this, the article doesn't make a distinction between privacy and personal data protection and both are used interchangeably as the case may be.[30]

---

[27] Rosen, supra note 23, p. 19.
[28] Ibid, p. 24.
[29] Ibid, p. 233.
[30] Indeed, as shall be noted later in this article, the right to privacy under Art 26(1) of FDRE Constitution is stipulated broadly, and illustratively so as to allow one to invoke

2. Right to Privacy Safeguards in International, Regional and National Instruments

This section presents the right to privacy as envisaged in major international and regional instruments along with a discussion on the nature and scope of right to privacy under the FDRE Constitution.

2.1 International Human Rights Instruments

In foregoing discussion, we have shown the definitional problem of privacy. Irrespective of the definitional hassle, the quest and need of privacy is a natural and imperative one. This being so, privacy is listed in the catalogue of human rights. At the international level, privacy is explicitly recognized as a fundamental right under the Universal Declaration of Human Rights, the International Covenant on Civil and political Rights, the Convention on Migrant Workers, and the Convention on the Protection of the Child.[31] The right to privacy forms the foundations of various rights espoused throughout human rights treaties.[32] These rights may, for example, include the privilege against self-incrimination, the right to remain silent upon arrest and the right to be free from unreasonable search and seizure.

---

protection of personal data, a protection elsewhere granted to personal data of persons under data protection law.

[31] The Universal Declaration of Human Rights, GA Res. 217A (III), 10 Dec. 1948, Art 12; the International Covenant on Civil and Political Rights, GA Res. 2200A (XXI), 16 Dec. 1966, Art 17; The Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, GA Res.45/158, 18 Dec. 1990, Art 14; and the Convention on the Rights of the Child, GA Res. 44/252, 20 November 1989, Art 16.

[32] A. Conte and R. Burchill (2nd ed.), *Defining Civil and Political Rights: The Jurisprudence of Human Rights Committee* (Ashgate, 2009), p. 201, see further D. Solove and M. Rotenberg, *Information Privacy Law* (Aspen Publishers: New York, 2003), p. 40, where privacy is considered as 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.

The ICCPR guarantees privacy as a right, the scope of which is detailed under the Article 17 of the Covenant as follows:

> Article 17(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.

Article 17 imposes on states parties an obligation to respect (not to interfere), and an obligation to protect. In this regard, the Human Rights Committee, in its General Comment No. 16, specified that the right to privacy must be guaranteed against all arbitrary or unlawful interferences and attacks, whether they emanate from state authorities or from natural person or legal person.[33] Moreover, states parties have an obligation to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as for the protection of this right.[34] Therefore, the nature of state obligation towards the right to privacy under Article 17 is both positive and negative kind.

Article 17 of the ICCPR provides for the protection of a wide range of rights. The rights – the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation – embrace a variety of matters , some of which are connected with one another, some of which overlap with others. None of the rights referred to under Article 17 is entirely self-explanatory in meaning. In effect, a question of what is the scope of the protected right (e.g. what is privacy of the person or home) may be raised in the course of the application of the provision in a case. Since

---

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

[34] Ibid.

Article 17 protects the right to respect for privacy of a person, family, home and correspondence, it is necessary to first determine the content of each right.

A) Privacy of a Person

According to Article 17(1) of the ICCPR, the first category of prohibited unlawful or arbitrary interference is that of one's 'privacy', the privacy of a person. Privacy of a person relates to various aspects of one's private life: from one's personal and sexual identity, to one's freedom from personal search or the collection of personal information.[35] Private life of an individual includes autonomy, physical and moral integrity, the right to determine personal identity (including sexual identity) and sexual orientation and relations.[36]

The fundamental interest within the sphere of private life is the capacity of the individual to determine his identity: to decide and then to be what he wants to be, to have his choice of name, his mode of dress, his sexual identity, and to choose how he is to be regarded by the state and how to present himself to others.[37]

In *Toonen v Australia*[38], the UN Human Rights Committee gave some guidance as to the meaning or ambit of 'private life' and other aspects of it. In *Toonen v Australia*, the author challenges the Tasmanian (one of

---

[35] Conte and Burchill, supra note 32, p.205.

[36] M. Nowak, *UN Convention on Civil and Political Rights: CCPR Commentary* (N.P. Engel, Kehl: Strasbourg, Arlington, 1993), pp. 294-98. See also P. Leach, *Taking a Case to the European Court of Human Rights* (Blackstone Press Limited, 2001), p.150.

[37] D. Harris, M. O'Boyle and C. Warbrick, *Law of the European Convention on Human Rights* (Butterworths, 1995), p. 305.

[38] *Toonen v Australia*, UN Human Rights Committee Communication No. 488/1992, UN Doc CCPR/C/50/D/488, (1994), para 6.5.

Australia's constitutive states) Criminal Code which criminalizes various forms of sexual contacts between men, including all forms of sexual contacts between consenting adult homosexual men in private. Mr. Toonen argued that the criminalization of homosexuality in private is breach of Article 17 (1) of the ICCPR: unlawful interference with one's privacy. In determining whether Mr Toonen has been a victim of an unlawful or arbitrary interference with his private life contrary to Article 17 of the ICCPR, the Human Rights Committee noted that it was undisputed that adult consensual sexual activity in private is covered by the concept of '*privacy*'. This implies that private life embraces not only individuals, personal choices but choices about relationships with others. Thus one's sexual relations fall within the sphere of private life.

Personal information such as fingerprints, medical records, photography is also within the orbit of privacy of person. The collection of such information by officials of states without the consent of the individual will interfere with his privacy. States parties to the ICCPR are obliged to regulate, by law, the gathering and holding of personal information on computers such as data banks and other devices, by public authorities or private individuals or bodies.[39] They must also take effective measures to ensure that information concerning a person's private life does not reach the hands of unauthorized persons, and to ensure that personal information is never used for purposes incompatible with the ICCPR.[40] Protection of one's private life requires an individual to have the ability to ascertain whether, and if so what, personal data is stored about him or her and for what purpose, with a right to request

[39] The Human Rights Committee General Comment No.16, supra note 33, para 10.
[40] Ibid.

rectification or elimination of information that the individual believes is incorrect.[41]

B) Family

Article 17 of the ICCPR prohibits unlawful or arbitrary interference with one's 'family', but does not define what the term 'family' constitutes. The understanding of what constitutes a family ranges from monogamous marriage and the traditional nuclear family to polygamous marriage and extended family units.[42] In its General Comment No.16 paragraph 5, the Human Rights Committee has noted that the objectives of the ICCPR require a broad interpretation of the family in the sense of the respective cultural understanding of the various state parties. In *Ngambi v France*[43], the Human Rights Committee has stressed:

> [T]he term 'family', for purposes of the Covenant, must be understood broadly as to include all those comprising a family as understood in the society concerned. The protection of such family is not necessarily obviated, in any particular case, by the absence of formal marriage bonds, especially where there is a local practice of customary or common law marriage. Nor is the right to protection of family life necessarily displaced by geographical separation, infidelity, or the absence of conjugal relations. However, there must first be a family bond to protect.

According to the Human Rights Committee, family life is understood as extending beyond formal relationships and legitimate arrangements.

C) **Home**

Freedom from arbitrary or unlawful interference with one's home is one further aspect of the right to privacy as enshrined under Article 17 of the ICCPR. In general, 'home' is understood to indicate the place where a person

---

[41] Ibid.

[42] A. Conte and R. Burchill, supra note 32, p.222.

[43] *Ngambi v France*, Communication 1179/2003, UN Doc CCPR/C/81/D/1179/2003 (2004), Para 6.4.

resides or lives on a settled basis. The Human Rights Committee has noted that home is a place where a person resides or carries out his usual occupation.[44]

It may be the case that not all living places are 'home'.[45] In *Stewart v Canada*[46], the author argued that the term 'home' should be interpreted even more broadly to encompass the entire community of which an individual is a part. The author claimed that his 'home' was Canada and that it was therefore

---

[44] The Human Rights Committee General Comment No.16, supra note 33, Para. 5. See also *Société Colas Est and Others v. France* (Decision of 16 July 2002), the Court stated that: "building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises".

[45] *United States v. Ruckman*, 806 F.2d 1471 (10th Cir. 1986) as cited in G. Arco, "United States v. Ruckman: The Scope of the Fourth Amendment When a Man's Cave is Not His Castle", J. Marshall L. Rev., Vol. 20, 1986/87. In the Ruchman case, the United States Court of Appeals for the Tenth Circuit noted 'home' does not include a cave. Frank Ruckman had been living in a natural cave on government land for approximately eight months. After the government issued a warrant for his arrest in 1985, six local police officers proceeded to the cave site. At the cave site the officers found a closed, but unlocked, door at the entrance of the cave. Ruckman was not in the vicinity. The officers entered the cave without a search warrant and seized several weapons. Upon his arrival at the cave, the police arrested and jailed Ruckman. Ruckman was subsequently charged with possession of an unregistered firearm. Before trial, the defendant moved to suppress the evidence seized in the warrantless search of his 'home'. The trial court denied the motion and Ruckman was convicted of the charge. The Appellate Court affirmed the conviction. In its analysis of whether the government-owned cave fell within the ambit of the fourth amendment's protections against unreasonable searches and seizures, the court refused to consider the cave a 'home' for purposes of protection under the fourth amendment. Rather, the court focused its attention on Ruckman's status as a trespasser and on the government's regulatory power over its land. Because Ruckman's living arrangements were tentative, and because the government had the power to oust Ruckman at any time, the court concluded that Ruckman did not have a reasonable expectation of privacy. See also the fourth amendment: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized.'

[46] *Stewart v Canada*, Communication 538/1993, UN Doc. CCPR/C/58/D/538/1993, (1996), Para. 3.3.

an interference with his home for Canadian authorities to deport him. The Human Rights Committee did not address that submission.

D) Correspondence

Freedom from arbitrary or unlawful interference with one's correspondence is a right to uninterrupted and uncensored communications with others. Within the framework of Article 17, correspondence covers a wide range of communications including post, telephone, telex, fax, and email. The Human Rights Committee explained this as follows:[47]

> Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

It seems to follow that the writer of a letter does not retain the right to non-interference with his correspondence once the letter is in the hands of the addressee.

2.2 Regional Human Rights Instruments

At regional level, the right to privacy is expressly recognized as one of the fundamental rights under the European Convention on Human Rights, and the American Convention on Human Rights.[48] Although the African Charter on Human and Peoples' Rights (hereinafter the African Charter) does not explicitly say anything about the right to privacy, one may argue that some

---

[47] The Human Rights Committee General Comment No.16, supra note 33, Para. 8.

[48] The Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, Art 8; The American Convention on Human Rights, San Jose, 22 November 1969, Art 11.

aspect of privacy is impliedly enshrined in it when the Charter stipulates that:[49]

> 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 slavery, slave trade, torture, cruel and inhuman or degrading punishment and treatment shall be prohibited.

The African Charter guarantees the respect of dignity of human beings and freedom from all forms of exploitation and degradation, including torture. The respect one's dignity and the freedom from torture carry protection of one's autonomy, physical and moral integrity. As pointed out earlier, a private life of a person includes, among others, his autonomy, physical and moral integrity. And hence, such aspect of privacy can be inferred from the African Charter.

There is little development towards privacy laws in Africa, 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. The absence of express stipulation about the right to privacy in the African Charter might also be another reason. 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 American Declaration of the Rights and Duties of Man. This regional declaration has been reinforced by the American Convention on Human Rights of 1969(American Convention). Article 11 of the American Convention envisages:

---

[49] The African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev.5, 27 June 1981, Art 5.

> (1) Everyone 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)Everyone 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 to the ICCPR. Article 11 of the American Convention prohibits all arbitrary or abusive interference in the private life of individuals, the privacy of their families, their home or their correspondence. In this regard, the Inter-American Court of Human Rights has stated that "the sphere of privacy is characterized by being exempt and immune from abusive and arbitrary invasion by third parties or public authorities."[50]

The 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention) 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 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.

---

[50] Case of *Escher et al. v. Brazil*, Preliminary Objection, Merits, Reparations and Costs, Judgment of July 6, 2009, Series C No. 158, para 113; Case of the *Ituango Massacres v. Colombia*, Preliminary objection, merits, reparations and costs, Judgment of July 1, 2006, Series C No. 148, para. 194; Case of *Escué Zapata v. Colombia*, Merits, reparations and costs, Judgment of July 4, 2007, Series C No. 165, para. 95; and Case of *Tristán Donoso v. Panama*, Preliminary Objection, Merits, Reparations and Costs, Judgment of January 27, 2009, Series C No. 193, para. 55.

Like the ICCPR, the above article protects four different interests: private life, family life, home and correspondence. Article 8(1) of the European Convention outlines protected interests without determining their scope. The jurisprudence of the European Court of Human Rights guides to ascertain the scope of those interests. For instance, in relation to the scope of 'private life', the Court held that: [51]

> ...it would be too restrictive to limit the notion of private life to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings

The European Court extended the concept of private life beyond the narrower confines on secrecy of personal information and seclusion without giving an exhaustive definition of private life, or even to isolate the values it protects. The European Court also extended the notion of 'home' to cover some business premises when it decided that home may extend, for example, to a professional person's office.[52]

---

[51] *Niemietz v Germany,* A 251-B, (1992), para 29; see also *Peck v UK* where the Court stressed that private life is a broad term not susceptible to exhaustive definition. The Court held that elements such as gender identification, name, sexual orientation and sexual life, identity and personal development, establishing and developing relationships with other human being and the outside world are important elements of the personal sphere protected by article 8 of the European human rights convention. There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life.'

[52] Ibid; the Court held 'home' includes business premises, since this was consonant with the object of Article 8 to protect against arbitrary interference by the authorities. Because 'activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises, it may not always be possible to draw precise distinction.'

Article 8(2) of the European Convention 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 the content of the right to privacy as embodied 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. The next section is devoted to discuss these limitations.

2.3 Limitations on the Right to Privacy

According to international human rights law, the guarantee of rights and freedoms incorporates a level of flexibility. This allows States to give effect to those rights and freedoms, while at the same time pursue important democratic objectives designed to protect society (such as national security) and to maintain a balance between conflicting rights (such as freedom of expression, balanced against privacy or the right to a fair hearing).[53] A restriction of rights is stipulated in human rights documents in order to strike a balance between competing interests/values. This accommodation is effected through limitations which are permitted by virtue of the particular expression of the right or freedom.

As discussed above, the right to privacy is guaranteed in the UDHR, ICCPR, and the American and European human rights instruments. Of these human rights instruments, the European Convention on Human Rights has explicitly provided an exception to the right to privacy. To the contrary, Article 17 of the ICCPR does not contain an express legal proviso allowing for restriction

[53] A. Conte and R. Burchill, supra note 32, p. 39.

on the right to privacy. 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' need clarification.

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 reasonable in the particular circumstances.[54] The converse reading of Article 17(1) of the ICCPR reveals that interference with privacy, family, home and correspondence is permissible so long as the interference is neither unlawful nor arbitrary. The essence of restriction of the right to privacy is that the interest of the society as a whole overrides the interest of individuals.

Like the ICCPR, the American Convention does not explicitly stipulate limitations on the right to privacy. Nevertheless, as the converse reading of Article 11(2) of the American Convention makes clear, the right to privacy is not an absolute right and can be restricted by the states parties, provided interference is not abusive or arbitrary. An interference with one's private life, his family, home or correspondence is permissible so long as it is not abusive or arbitrary. To this end, the interference must be established by law, pursue a legitimate purpose and be necessary in a democratic society.[55]

[54] The Human Rights Committee General Comment No.16, supra note 33, para 3-4.
[55] Case of *Escher et al. v. Brazil*, supra note 50, para 116.

By the same token, under the European Convention, 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 Article 8-11 of the Convention 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 interference is necessary in a democratic society and proportionate to the legitimate aim pursued.[56] These criteria have been advanced and made clear by decisions of the Court.[57]

The European Court of Human Rights has been using the 'balancing test'[58] based on the above criteria to justify the limitations on the right of privacy. The Court had to balance the interest of the right holder, and the interest of

---

[56] F. Jacobs and R. White (4th ed.), *The European Convention on Human Rights* (Oxford University press, 2006), pp. 223-40.

[57] 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).

[58] 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. 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. *See also*, J. Whiteman, "The Two Western Cultures of Privacy: Dignity versus Liberty", Yale Law Journal, Vol.113, 2004, p.1151; 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.

the public or other individuals. The right holder has an interest to control a state's capacity to interfere in central matters of interpersonal relationships, including consensual sexual activities, parent-child relations, and conversation while a state is required to protect individuals from harm inflicted by others such as exploitive sexual conduct, abuse of children by parents, and communications which harass the recipient.[59]

2.4 The FDRE Constitution

Article 26 of the FDRE Constitution guarantees the right to privacy 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 first sentence of Article 26(1) of the Constitution recognizes the right to privacy in general terms. Article 26 sub-article (1) in its second sentence and sub-article (2) further defined the right to privacy in terms of one's person, home, property, correspondence and communication. However, it is good to note that the list of protected interests under Article 26 sub-article (1) second sentence and sub-article (2) is just illustrative.[60] This is to say that the right to

---

[59] Harris, O'Boyle and Warbrick, supra note 37, p.353.

[60] Since that the right is so broadly and illustratively defined, it may legitimately be extended to protect data privacy, or data protection right as it is called in European law. As a result, the right to privacy can be understood to embrace the right not to be

privacy is broad enough to include other interests, including non-interference with one's family. As a rule, the FDRE Constitution prohibits the search of an individual's home, person (giving individuals a sphere of personal autonomy), seizure of property, and interception of individual's correspondence. Yet again, it must be noted that privacy protection under the FDRE Constitution is not limited to the prohibition of searches of one's home, person or property, seizure of one's property, and interception of one's correspondence, but rather includes the prohibition of unlawful or arbitrary interference with any of the protected interests.[61]

The FDRE Constitution requires public officials not only to refrain from interferences with individual privacy, but also to prevent private persons or entities that would impair the right. However, the right to privacy is not absolute. The FDRE Constitution under Article 26(3) puts a limitation clause on the right to privacy. Limitation on the right to privacy is allowed only when three important elements are satisfied together: (1) there must be

---

subjected to storage, processing and disclosure of personal details or data without express consent save limitations set out under Art 26(3) of the constitution. Accordingly, discussions in the third section assess some laws in light of this sense of the scope of right to privacy.

[61] A question might arise whether the right to privacy as regulated Art 26 applies to legal or juridical persons. While one might plausibly argue that right to privacy is an individual human right and hence excluding legal persons, there appears to be a convincing reason to stretch the applicability of the right to legal persons. Similarly with individuals, legal persons do have values that the right to privacy aims to protect. One example in this regard is that searches and seizures could be made against the business premises of corporations and unless such acts are conducted in line with legally set requirements, they may cause non-negligible damage to the entity and its human members as well. In other words, intrusions into the confidential sphere of companies would no less intrusion against the right to privacy of its members. To be added to this is that despite the general heading of Part One of the Constitution (Human Rights), Art 26 on its own right is broader and is likely to protect entities in addition to individual persons. In *Société Colas Est and Others v. France* (decision of 16 July 2002) case, the European Court of Human Rights held that warrantless entry into business premises of a corporation violates Art 8 of the European Convention on Human Rights (ECHRt), a provision that regulates right to privacy.

compelling circumstances; (2) restriction must be in accordance with specific laws; and (3) there must be legitimate aim.

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. But what constitutes violation of legitimate objectives such as 'public morality' or '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.[62]

The standards set to limit privacy right under the FDRE Constitution are more or less similar to the requirements stipulated under the European Convention on Human Rights. The difference is that the FDRE Constitution puts the requirement of "compelling circumstances" in lieu of the requirement of "necessary in the democratic society" under the European Convention on Human Rights.[63] The test of "compelling circumstances" may be difficult to define in the abstract. In any event, the prevailing situation should appear compelling to a reasonable degree to interfere with the right to privacy. It is also important to consider to what extent the compelling situation requires limitation on the right. The limitation should also be made by a specific law[64] which can be laid down for the purpose of safeguarding

---

[62] F. Nahum, *Constitution for a Nation of Nations: The Ethiopian Prospect* (Red Sea Press, 1997), p. 124.

[63] The Constitution of the Federal Democratic Republic of Ethiopia, Proclamation No. 1/1995, Negarit Gazeta, 1st Year, No. 1, Art 26(3), and the European Convention for the Protection of Human Rights and Fundamental Freedoms, supra note 51, Art 8(2).

[64] The Human Rights Committee, in its General Comment 16 (supra note 33), para 8 stated that no interference can take place except in cases envisaged by specific law which

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.

Succinctly, interference with privacy right is permissible under the FDRE Constitution upon the fulfillment of the aforementioned requirements. Any limitation other than the constitutionally stipulated ones is not permissible, and is tantamount to a violation of the constitution.

3. Laws and Practices in Ethiopia with implications on the Right to Privacy

This section closely examines some of the major laws and practices which are likely to pose threat to the constitutional right to privacy.

3.1 Criminal Procedure Laws and the Right to Privacy

As we have previously underlined in the discussion of the FDRE Constitution, privacy can only be limited under compelling circumstances in accordance with specific laws and in pursuit of legitimate aims. Crime prevention and national security are, as per Article 26 (3) of the FDRE Constitution, some of the legitimate aims which enable the law enforcer to lawfully interfere with the privacy of individuals in accordance with specific laws. In the Ethiopian legal system, we have some laws including the Criminal Procedure Code, the Anti-Corruption Proclamation and the Anti-Terrorism Proclamation that impose restriction on the right to privacy.

---

in turn specify in detail the precise circumstances in which interference is permitted and must designate an authority, on case by case basis, to determine such authorizations.

The 1957 Criminal Procedure Code of Ethiopia provides protection to body, premises and property of a person against arbitrary searches and seizures respectively.[65] The protection of the individual's person is one of the fundamental aspects of privacy, without which there would be threats of physical violence. 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) and (2) of the Criminal Procedure Code are met. For example, an arrested person can be searched when there is a 'reasonable suspicion'[66] that he possesses any articles serving as a material evidence for the offence he is suspected to have committed. Here the difficulty lies on deciding whether all facts and circumstances that are known to the police officer establish a 'reasonable suspicion.' Premises can also be searched with a search warrant. Of course, there are circumstances where premises can be searched without even a search warrant. Such is the case when an offender is followed in hot pursuit and enters premises or disposes of articles, and a police officer is informed and reasonably suspects that the articles serving as material evidence are concealed or lodged in a place and

---

[65] Article 32 of the Criminal Procedure Code provides: "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".

[66] The term reasonable suspicion is incorporated in our legal system without any definition, and may open a room for abuses of individuals' rights.

he has good grounds to believe that delay in obtaining a search warrant will lead to the articles to be removed.

The Anti-Terrorism Proclamation[67] (hereinafter ATP) provides limitations on the constitutional right to privacy in order to prevent crimes of terrorism and maintain national security. The ATP expands both police and prosecution powers in significant ways. The ATP under Article 14 gives powers to the National Intelligence and Security Service (hereinafter NISS) to intercept or conduct electronic surveillance of telecommunications including Internet communications so as to prevent and control a terrorist act. The power to gather information through surveillance for the same purpose is also granted under sub-article 4 of Article 14 of the ATP. An interception or surveillance on the communications privacy under Article 14 of the ATP is to be made only with court warrant. However, it is not clear whether the court has the power to reject an application for a warrant.

The ATP outlines two types of searches: covert search under Article 17 and sudden search under Article 16. A covert search requires a court-approved search warrant if a police officer has reasonable grounds to believe that a terrorist act has been or is likely to be committed or that a resident or a possessor of a house to be searched has made preparations or plans to commit a terrorist act.[68] As per Article 17 of the ATP, the fulfillment of two conditions is sought for a covert search. First, a police officer must have a reasonable ground to believe that a terrorist act has been or is likely to be committed, or that a resident to be searched has made a plan to commit a terrorist act. Second, the officer must have reasonable grounds to believe that

[67] A Proclamation on Anti-Terrorism, Proclamation No.652/2009, Federal Negarit Gazeta, 15th year, No. 57.
[68] Ibid, Art 17.

covert search is essential to prevent or to take action against a terrorist act or suspected terrorist activity.[69] As opposed to Article 14 of the ATP (a court warrant for interception or conducting electronic surveillance by NISS), the court may either deny or grant a warrant to conduct covert search based on the information presented to it by having into account the nature or gravity of the terrorist act or suspected terrorist act, and the importance of the warrant in preventing the act of terrorism.[70]

However, a sudden search of body and property can be conducted by a police officer with authorization of the director general of the Federal Police or his designee, without judicial oversight, if a police officer has reasonable suspicion that a terrorist act will be committed and deems it necessary to make a sudden search.[71] To conduct a sudden search, a police officer is required to have a reasonable suspicion that a terrorist act will be committed and to believe that a sudden search prevents the act. Article 16 of the ATP, grants the police officer exclusive discretion to carry out search and seizure solely on the basis of reasonable belief that a terrorist act may be committed. Article 21 of the ATP also empowers the police officer to take samples of handwriting, hair, voice, fingerprint, photograph, blood, saliva and other fluids of a person suspected of acts of terrorism for investigation. The powers of the police granted by virtue of Article 16 and Article 21 of the ATP may pose a threat to the constitutional right to privacy.

Another specific legislation which restricts the right to privacy is the Anti-Corruption Proclamation. As seen in the earlier discussion, the FDRE Constitution guarantees the right to the inviolability of one's notes and correspondence (communications privacy) including postal letters, and

[69] Ibid, Art 17(3).
[70] Ibid, Art 18 (1).
[71] Ibid, Art 16.

communications made by means of telephone, telecommunications and electronic devices. However, this aspect of privacy can also 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 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.

The 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.[72] The FEAC can order the interception of one's correspondence if it is necessary for investigation of corruption offences. The interception cannot however be made for indefinite period. In the absence of a decision by the investigating organ, the duration of interception should not be longer than four months. The provision gives the FEAC an exclusive discretion without court warrant to intercept the communications of individuals. Hence, such a discretionary power may undermine the constitutional right to privacy.

3.2 Mass Media Law and Right to Privacy

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

Privacy of individuals and freedom of expression may stand in direct conflict. These two fundamental rights serve important functions: the first, protecting the individual from unlawful or arbitrary intrusion; the second, communicating information deemed to be in the public interest.[73] The FDRE Constitution guarantees freedom of expression, opinion and thought under Article 29. Freedom of expression as recognized in the FDRE Constitution consists of the right to seek, receive and impart information and ideas. Freedom of information (the right to access information) is the crucial aspect of freedom of press or other media. Accordingly, individuals are at liberty to receive information about the government representing them. Concomitantly, press and other mass media are entitled to gather information in the process of seeking information and disseminating them to the public. This means that the government is duty bound to be transparent and make its documents accessible to the press so long as it is for public interest. These rights can only be limited through laws based on the principle that freedom of information and expression cannot be limited on account of the content or effect of the point of views expressed.[74] The limitation can be laid down for the purpose of protecting the well being of the youth, and the honor and reputation of individuals.[75]

The Proclamation on Freedom of Mass Media and Access to Information (hereinafter Proclamation on Mass Media) provides that all persons have the right to seek, obtain and communicate any information held by public bodies, except exempted information therein.[76] The exempted information from

---

[73] L. Pyk, "Putting the Brakes on Paparazzi: State and Federal Legislators Propose Privacy Protection Bills", DePaul J. Art & Ent. Law, Vol. IX: 187, 1999, p.187.

[74] FDRE Constitution, supra note 63, Art 29(6).

[75] Ibid.

[76] Freedom of Mass Media and Access to Information Proclamation, Proclamation No.590/2008, Federal Negarit Gazeta 14th Year, No. 64. Arts 12(1) and 15.

disclosure is *inter alia* personal information. In this respect, Article 16(1) of the Proclamation on Mass Media provides "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 for 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 Article 16(1) of the same proclamation stipulates situations where personal information may be disclosed with the consent of the person concerned.

The Proclamation on Mass Media has clearly defined personal information means as information about an identifiable individual, including information relating to one's medical history, ethnic or national origin, identifying numbers, personal references, views or opinions, blood type etc. [77] The Proclamation on Mass Media lays down examples of personal information

[77] Art 2(8) of the Freedom of Mass Media and Access to Information Proclamation defines 'personal information' as '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 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.'

without being exhaustive. Unlike the definition of European Union (EU) Data Protection Directive, the Proclamation on Mass Media 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. We believe that information about an identifiable person should be treated personal information. In this regard, the EU Data Protection Directive has made it clear that personal data means any information related to an identified or identifiable individual.[78]

As per Article 16 of the Proclamation on Mass Media, personal information held by public body should not be disclosed under the guise of access to the records. The provision contains one of the basic principles of personal data processing i.e. disclosure limitation. However, its scope is limited in the sense that it refers to personal information held by only public body. The provision does not say anything about personal information held by private sectors. Private sectors may gather, process, and transfer personal information in a way that undermines the constitutional right to privacy.

3.3 Tax Seizure Rules and Right to Privacy

The Ethiopian law of tax embraces tax seizure rules as new tools of tax enforcement. A peculiar feature of these seizure rules is that the tax authority is empowered to unilaterally seize and sell delinquent taxpayers property

[78] 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, Directive 95/46/EC (1995), Art 2(a).

should the latter fall in default of paying taxes due.[79] Unlike the pre-2002 collection schemes, the authority no more resort to courts to demand execution against defaulting taxpayers as the so called tax foreclosure rules enable self-execution by the tax authority.

Nevertheless, that tax seizures are enforceable by tax authorities unilaterally without any judicial oversight inevitably become a cause for concern particularly in relation to the rights of taxpayers. This is because such procedures give unfettered latitude to authorities thereby putting rights and interests of allegedly delinquent taxpayers at stake. More particularly, the constitutional rights to privacy might be at stake as the right to privacy guaranteed under the FDRE Constitution includes the right not to be subjected to seizure. That the bureaucracy is hardly mature, prone to impropriety and less synchronized to win the confidence of taxpayers compounds the concern.

The right to privacy under the FDRE Constitution, as noted earlier, can be restricted only if the three cumulative conditions are met; i.e. first, there must be compelling reasons necessitating the seizure, second, there must be specific laws authorizing such restrictions, and third, there must be legitimate objectives such as crime prevention, national security, public peace and morality. It transpires from the above proviso that on top of having tax laws authorizing seizure it is highly necessary seizures must be made only in those circumstances compelling the action. Compelling circumstances perhaps include those cases jeopardizing the collection of taxes. In line with this understanding, a sheer existence of tax laws authorizing seizure, and a mere default on the part of taxpayers cannot itself warrant the constitutionality of

[79] For details see, K. Yilma, infra note 82.

the seizure. Seizure should be undertaken only when delinquent taxes[80] cannot be recovered in any other possible means without affecting the fiscal interest of the government.

The UN Human Rights Committee has, as pointed out earlier, given authoritative insights on whether a mere existence of a law authorizing interference (seizure in our case) justifies any interference with one's right to privacy. The Committee held that the term 'unlawful' means that no interference can take place except in cases envisaged by law, which in itself must comply with the provisions, aims and objectives of the ICCPR.[81] It further stated that an arbitrary interference might take place even in cases where the interference is provided under the law. It flows from this that arbitrary tax seizure that runs over other fundamental rights such as the right to property of taxpayers although mandated under the law might be in breach of Article 17 of the ICCPR.

In mitigating the privacy implications of the tax seizure rules, we suggested elsewhere the issue of requiring judicial warrant before any act of seizure as it is the case in criminal matters.[82] The very fact that the tax authority is the sole decision maker on whether there is a 'compelling circumstance' warranting seizure of property is a cause for concern. In dealing with such situation requiring prior tax seizure warrant would be perhaps befitting. Requirements of prior tax seizure warrants are also common in countries

[80] Delinquent taxes are taxes already due but not yet paid by the taxpayer; the defaulting taxpayer is referred to as a delinquent taxpayer.

[81] General Comment No. 16, supra note 33, Para 1.

[82] K. Yilma, "On Tax Foreclosure Rules and Taxpayers' Rights to Privacy and of Access to Justice in Ethiopia", *Ethiopian Journal of Human Rights*, Vol.1, 2013, pp.195 *et seq.*

where the tax system is remarkably developed, and where regard to basic rights of taxpayers is a paramount priority.[83]

The tax foreclosure regime also entails other features with privacy invasive penchant. For instance, tax authorities are exempted from issuing a notice of seizure to the taxpayer when they found out that collection of taxes is in jeopardy. All what is required of the tax authority is to make a demand for 'immediate payment of the tax'; upon failure or refusal, seizure without notification would be lawful.[84] This provision stands in contradistinction with the rule in Canada, for example, where the tax authority is required to obtain judicial warrant even in cases where 'collection is in jeopardy.[85] In so doing, the tax authorities would be required to demonstrate the existence of urgency justifying abrupt collection action. The provision in the Ethiopian tax law appears to negatively affective the due process of law.

There is also a related privacy invasive procedure called jeopardy assessment whereby the tax authority may order the immediate blockage of taxpayer's bank account and have access to information thereof where it believes that

---

[83] In the US, for instance, seizure of taxpayers' property violates right to privacy unless the tax authority (IRS) obtains a prior judicial warrant save the exception when seizure is made at public places. See, *2nd American Jurisprudence: Federal Tax Enforcement*, Vol. 35, (Cooperative Lawyers Publishing Company, 2001), p. 20; see also, E. Enright, "Probable Cause for Tax Seizure Warrant", *The University of Chicago Law Review,* Vol. 55, No. 1, 1988, pp. 210-211. A slightly similar rule applies in Canada. To give an authorization of seizure, the Minister of National Revenue must certify that all or part of an amount payable has not been paid and register a certificate in the Federal Court of Canada. See, J. Li, infra note 85, p.115; see also Sections 222-225 of Consolidated Canadian Income Tax Act of 1985, infra note 85.

[84] See Income Tax Proclamation, Proclamation No. 286/2002, Federal Negarit Gazeta, 8th Year, No. 34, Art 77(5).

[85] J. Li, ''Taxpayers' Rights in Canada'', Revenue Law Journal, Vol. 7, Issue 1, 1997, p. 115; see also Sections 222-225 of Consolidated Canadian Income Tax Act of 1985, available at <http://laws-lois.justice.gc.ca/eng/acts/I-3.3/page-365.html#docCont.> [Accessed on September 27/2013]

the collection of the tax is in jeopardy to make immediate assessment of the tax for the current period.[86] It must then obtain a court authorization within 10 days from giving the administrative order. As it can readily be noted, the tax authority has to obtain judicial authorization *ex post* after having blocked the bank account and accessed personal data of the taxpayer.

The purpose of the judicial authorization is not clear as it will be obtained after the damage is done to the privacy of the taxpayer; nor is it clear what remedies are available to the taxpayer should the court reject the administrative order whose effect has already taken place. It would have been in line with the constitutional right to privacy if the judicial authorization was required before the administrative order is given by the tax authority.

3.4 Telecom Fraud Offence Law, Deep Packet Inspection and Unsolicited Communications

3.4.1. Telecom Fraud Offences Law

The recently adopted Telecom Fraud Offense (TFO) proclamation No. 761/2012 is the other legislative instrument with potential threats to right to privacy. Few recent legislative initiatives of the Ethiopian government received as much attention and criticisms as the TFO. Apart from the usual human rights whistle-blowers, it has been a point of discussion in mainstream international media such as Al-Jazeera[87] and the BBC.[88] The issues and concerns that the bill gives rise to are twofold. Whilst criticisms over the

---

[86] See Income Tax Proclamation, supra note 84, Art 81.

[87] Aljazeera held a special program on the alleged ban of Skype. See, Skype Me May Be, The Stream, Aljazeera, June 14, 2012; available at < http://stream.aljazeera.com/story/ethiopia-skype-me-maybe-0022243> [Accessed on September 27/2013].

[88] K. Moskvitch, Ethiopia Clamps Down on Skype and other Internet Use on Tor, BBC News, Technology, June 15, 2012; available at <http://www.bbc.com/news/technology-18461292> [Accessed on September 27/2013].

alleged ban of Voice Over Internet Protocol (VOIP) call dominated the discussion, few have quipped on the potential privacy implications of the law. A local English weekly, Addis Fortune, slammed the proposal in livid terms that 'there seems to be an inherent interest to put every beast under control; no matter how harmless it is'.[89] In its editorial, Addis Fortune stated: [90]

> Worse, the bill transcends the Constitution by violating the right to individual privacy with a long list of admissible evidence. Although individual notes and communications are protected by the Constitution, the new bill makes digital evidence collected through unlawful interference admissible in a court of law. No matter how infant the debate over privacy is, closer, there is no worse situation than providing the state with the power to interfere with individual communications.

The above concern relates to the power of covert search bestowed to the police under the the TFO proclamation. According Article 14 of the TFO proclamation, a police officer may request a court in writing for a covert search warrant 'where he has reasonable grounds to believe that a telecom fraud offence has been committed or is likely to be committed.' This provision legalizes secrete surveillance by the police upon suspicion that a telecom fraud offense has been or is likely to be committed. It, however, blends it with judicial oversight by requiring prior judicial warrant which is commendable on its own.

What remains unclear, however, is the discretion of courts in reviewing the request for a search warrant. Are courts at liberty to reject requests should there appear not to exist a reasonable ground to believe the commission or

---

[89] Editor's Note, Addis Fortune, Volume 13, Number 632, Published on June 10, 2012, available at <http://www.addisfortune.net/fortune_editors_note.htm.> [Accessed on September 29/2013].

[90] Ibid.

likelihood of commission of an offense? Or is it just a formal requirement whereby the police just go to receive the imprimatur of the court? What if the police overstep the warrant and seize properties of the person under surveillance? At the most basic level, one might even ask what 'search' refers to within the meaning of the provision. While it might be thought to embrace surveillance, it is ambiguous whether it also includes interception of communications or eavesdropping. In the absence of clearly articulated powers of surveillance or interception, it would be hard to justify the latter as having been carried out in compliance with the constitutional right to privacy.

The drafters of the law regrettably missed valuable examples from the Ethiopian Criminal Procedure Code on the conditions and discretion of courts in entertaining requests for search warrant. The Code states that no search warrant shall be issued unless the court is satisfied that purposes of justices will be served by the issuance of the warrant.[91] More interestingly, the law sets out important elements that any search warrant must incorporate. For instance, it provides that the warrant shall clearly specify the property to be searched and goes to set the time when searches have to be undertaken, between 6 A.M. and 6 P.M.[92] The later aspects of the Code are apparently privacy friendly and has the potential to mitigate extreme cases of *ultra vires* by authorities in charge of covert searches.

Given that limitation to the right to privacy are possible in very exceptional circumstances, it is also doubtful if the proviso on covert search by the police is clear enough to qualify to the 'specific law' requirements of Article 26(3)

---

[91] The Criminal Procedure Code of Imperial Ethiopian Government, Negarit Gazeta, Proclamation No.185 of 1961, Art 33(1).

[92] Ibid, Arts 33(2) and 33(5) respectively.

of FDRE Constitution. The jurisprudence on the legality of interception and secret surveillance in other jurisdiction offers valuable insight on this. For instance, the European Court of Human Rights (ECHR) held that the mere fact that there is law authorizing (telephone) interception doesn't warrant the legality of the interception unless the law in question indicates with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities to give the individual adequate protection against arbitrary interference.[93] In another case, the ECHR noted that powers of secret surveillance are often tolerable in so far it is strictly necessary for safeguarding democratic institutions.[94] The TFO proclamation seems to fail short of these privacy-friendly standards with vague and crude formulation of police surveillance powers.

A troubling side of the surveillance is that any evidence obtained through surveillance or interception shall be admissible in court proceedings.[95] Apparently, Article 15 of the TFO proclamation concerns admissibility of evidences obtained based on the covert police search carried out under Article 14 of the same law.[96] This is particularly worrying because rules of evidence admissibility, if any, don't regulate exclusion of certain illegally

---

[93]See, European Court of Human Rights, *Kruslin v. France*, 24-04-1990, available at <http://sim.law.uu.nl/sim/caselaw/Hof.nsf/e4ca7ef017f8c045c1256849004787f5/340529db2776b38dc1256640004c1cf2?OpenDocument. > [Accessed on September 27/2013].

[94]See, European Court of Human Rights, *Klass v. Germany*, 1978, available at <http://www.hrcr.org/safrica/limitations/klass_germany.html.> [Accessed on September 27/2013]

[95]See Art 15 of Telecom Fraud Offense Proclamation, Proclamation No. 761/2012, Federal Negarit Gazeta, 18th year, No. 61. Note that Reporters without Borders similarly states 'it also allows evidence gathered through such (covert search) interception or surveillance to be admissible'. See, Reporters without Borders for Freedom of Information, Although Still At Draft Stage, New Telecoms Rules Give Cause For Concern, July 6, 2012, available at <http://en.rsf.org/ethiopie-although-still-at-draft-stage-new-06-07-2012,42957.html.> [Accessed on September 27/2013].

[96] This can also readily be gleaned from the consecutive arrangement of the provisions.

obtained evidences.[97] In other countries such as the USA, the exclusionary rule allows exclusion of evidences obtained by any illegal means. As TFO proclamation stands, it is uncertain what kinds of evidences are admissible, leaving many open questions. Is any evidence collected by (any) means admissible as long as there is a search warrant? One plausible line of interpretation is that only evidences collected through warrantless searches or surveillance are to be rendered inadmissible before courts. Yet, the provision leaves a room for unbridled arbitrary search in the name of having judicial warrant.

3.4.2. Deep Packet Inspection and Privacy of Communications

A report on the recent installation of Deep Packet Inspection (DPI) technologies by the Ethio-telecom, in concert with Information Network Security Agency (INSA), indicates the potential of the practice in threatening privacy in Ethiopia.[98] DPI is a computer network packet filtering technique that involves inspection of contents of packets as they are transmitted across the network.[99] Since most of the internet traffic is unencrypted, DPI enables Internet Service Providers (ISPs) to intercept virtually all of their customers' internet activity, including web surfing data, email, and peer-to-peer

---

[97] The only relevant provision in this regard is Art 19(5) of the FDRE Constitution which provides that any evidence obtained from an arrested person through coercion shall be inadmissible. In this context, some constitutional law lawyers, in informal conversations, tended to argue that the scope of application of the constitutional provision is so broad enough to be extended even in cases of evidences obtained through secret surveillance under the TFO.

[98] Tor Project, a virtual tunnel that enables online anonymity, reported on 31st of May 2012 that the then Ethiopian Telecommunications Corporation (now Ethio-Telecom) has deployed or begun testing Deep Packet Inspection of all internet traffic. See, Tor, Ethiopia Introduces Deep Packet Inspection, May 31, 2012, available at < https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection.> [Accessed on September 27/2013]

[99] Electronic Privacy Information Center, Deep Packet Inspection and Privacy, available at <http://epic.org/privacy/dpi/.> [Accessed on September 27/2013]

downloads.[100] The uses of DPI seem to generate *prima facie* privacy concerns, as data about users' behavior on the internet (which could also include sensitive data) is being monitored and used for various purposes.[101] The danger with widespread use of DPI is that it may be abused in certain circumstances for purposes that violate end users privacy.[102]

The DPI technologies would practically enable the sole state-owned ISP, Ethio-Telecom, to intercept and survey almost every communication over the net. In the absence of a law authorizing the use of such technologies in circumstances set out under Article 26(3) of the FDRE Constitution, the surreptitious use of DPI would violate the right of persons to inviolability of their communication through the internet guaranteed under Article 26(2) of the FDRE Constitution. Although there might exist compelling circumstances necessitating using tools such as the DPI, the easy way forward would be to set forth a clear framework within which the incumbent telecom company may interfere with the private communications of right-holders.

3.4.3. Unsolicited Communications[103] and Privacy of Communications

---

[100] Ibid.

[101] A. Daly, "The Legality of Deep Packet Inspection", 2010, First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade', University of Glasgow 17 June 2010, p. 7; available at < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024 .> [Accessed on September 27/2013].

[102] C. Hangey, "Deep Packet Inspection and Your Online Privacy: Constitutional Concerns and the Shortcomings of Federal Statutory Protection", 2008, available at <http://ssrn.com/abstract=1907078.> or http://dx.doi.org/10.2139/ssrn.1907078> [Accessed on September 27/2013].

[103] As can readily be gleaned from the phraseology "This right shall include(sic).." under Art 26(1) of the FDRE Constitution, the right to privacy is guaranteed broadly in that it possibly includes the right to be let alone. The latter includes the right to decide what kinds and forms of communications to receive. The electronic

Speaking of telecommunications and privacy, a recently adopted law on advertisements partly deals with unsolicited telecommunication advertisements. According to this law, unsolicited advertisements sent to subscribers' telephones shall be prohibited unless the subscriber consented in advance.[104] In effect, the law adopts what is elsewhere called 'opt-in' approach of communications by which electronic communications such as e-mail have to be addressed to individuals only after consent is secured. The law however carves out an exception to those advertisements addressed by the telecom provider, Ethio-telecom itself and public advertisements.[105] While the inclusion of opt-in approach is commendable measure in protecting the privacy of subscribers, the broader exception of advertisements by the Ethio-telecom may be called into question.

Given that most of the advertisements sent over to subscribers are from Ethio-telecom itself, we suggest that the exception should rather be restricted only to those relevant and perhaps mandatory service advertisements rather than commercial and sometimes political advertisements and communications. Moreover, there should be an option for a subscriber to 'opt-in' at the time of subscription or to 'opt-out' at a later stage. Also striking about the law on advertisement is its apparent failure to include unsolicited communication through electronic mail. Indeed, it includes 'internet website' (lets us assume that this is meant to include e-mail) in defining means of advertisement dissemination. In a country where the level

---

communications may be either unsolicited e-mails, also called spam, sent from botnets maintained abroad or mobile SMS/MMS or even cold phone calls.

[104] A Proclamation on Advertisement, Proclamation No. 759/2012, Federal Negarit Gazeta, 18th Year, No. 59, Art 22(2)..

[105] Ibid.

of internet penetration is close to 1.1%,[106] the omission might not come as a surprise. It must nevertheless be stressed that regulation shall envision future developments in ICT sector of our country so that legal protection of citizens would not be a piecemeal exercise.

At the time of writing of this article, a draft cybercrime law that, among others, criminalizes dissemination of commercial advertisements through e-mail — or spamming — has emerged.[107] The draft text of the law states that whosoever disseminates spam through e-mail accounts is criminally punishable.[108] The law further sets forth exceptional circumstances where spamming will not be punishable; these are:

i. There is prior consent from the recipient, or

ii. The primary purpose of the advertisement is to introduce existing users or subscribers with new products or services, or

iii. The advertisement contains valid identity and address of the sender, and valid and simple way for the recipient to reject or unsubscribe receipt of further advertisement from the same source.

---

[106] According to Internet World Stats 2012 report, the level of internet penetration in Ethiopia is 1.1%. See, Internet World Stats, Usage and Population Statistics, available at <http://www.internetworldstats.com/africa.htm#et.> [Accessed on September 27/2013]. In an interview with Ethiopian News Agency (ENA) on 13th June 2012, Minister of Communication and Information Technology and Deputy Prime Minister Dr. Debre-Tsion Gebre-Micael stated that the number of internet users have reached 2.5 million, which roughly would put the level of internet penetration 2.87 %. See, details about the news report at < http://danielberhane.com/2012/06/17/ethiopia-internet-users-no-reached-2-5-million-minister-says/ >. [Accessed on September 27/2013]

[107] Note that the authors of this article had the opportunity to take part in the workshop called on to comment on the draft text of the law drafted by the Information Network Secuirity Agency held at the Golf Club, Addis Ababa between July 22 – 23, 2013.

[108] See the Proclmation to Legislate,Prevent and Control Computer Crime (Draft), 2013, Art 14 available on file with the authors.

The initiative to regulate spam is commendable on its own though most spam destined to our e-mails are from overseas and indeed from those highly sophisticated spammers. The challenge ahead is thus formidable as policing and prosecuting such offenders would require significant technological and institutional readiness.

3.5 Few Words on Evolving Privacy Invasive Media Practices

On 25 January 1883 Samuel Warren married Mabel Bayard, a daughter of a United States Senator from Delaware and a candidate for President, Thomas Bayard.[109] The New York Times and the Washington Post shortly featured detailed and sensitive reportage of the wedding.[110] Furious about the details disclosed by the press, Warren and his colleague Lois Brandeis wrote one of the most widely cited law review article in 1890[111], an article tout to invent the 'right to privacy as we know it today'.[112] In the article, Warren and Brandeis attacked unethical and intrusive reporting practices of the press. They stated that 'the press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and the vicious, but has become a trade, which is pursued with industry as wells as effrontery'.[113]

Although not in a scale described by Warren and Brandeis a century ago, evolving media practices are posing real dangers to privacy in Ethiopia.

---

[109] A. Gajda, "What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering The Press Coverage That Led To 'The Right to Privacy'", *Michigan State Law Review,* 2008, Vol. 35, p. 36.

[110] Ibid, pp. 36-37.

[111] S. Warren and L. Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, 1890, available at < http://www.law.louisville.edu/library/collections/brandeis/node/225>. [Accessed on September 27/2013]

[112] D. Glancy, "The Invention of The Right to Privacy", *Arizona Law Review*, Vol. 21, No. 1, 1979, p. 1.

[113] Warren and Brandeis, supra note 111.

Following a slight liberalization of the media sector, private radio and television channels are increasingly becoming viable alternatives to state media. The peculiar feature of these channels is that the greater portion of the transmissions focuses on entertainment programs anchored almost in similar fashion. And, some of them heavily rely on disclosing very private information of celebrities or other eminent personalities. A few examples are in order.

A radio program called '*Ethiopica Link*', aired throughout the week except on Sundays on Fana FM 98.1, has a special program named *'ye Ethiopia mishit'* on air for three hours.[114] While the radio show is often penchant on disclosure of information about celebrities, foreign or local, the one hour program that it presents on Saturday nights raises questions of privacy. The program, dubbed '*wist awaki*', probably inspired by a US TV program called *'Insider'*, focuses on divulging very sensitive and intimate private information of individuals and families. There doesn't seem to exist a limit on what kind of personal information has to be disclosed. This is obviously due to the absence of any data protection law in Ethiopia that regulates processing of personal data by data controllers including the media. Lack of clear privacy regime has inextricably blurred the boundaries of freedom of expression and the right to privacy of citizens.

One might be struck that the said radio program has received a considerable attention from a good portion of the public. According to Warren and Brandeis, such attention should not come as a surprise as gossips are of easy

[114] Recently, this program has been forced to leave FM 98.1 and has started airing in another FM station called Zami FM 90.7. The structure of the program has however resumed as before, if not with more anti-privacy tendency.

comprehension and are appealing to the weak side of human nature.[115] Limitless engagement in sniffing around the private affairs of others is said to have serious social and psychological implications. Warren and Brandeis, for instance, argued that overly privacy invasive acts of the media have the potential to cause serious mental pain and distress whose harm may even be far reaching than physical injury.[116] In similar fashion, Westin associates numerous instances of suicide and nervous breakdown to unfettered exposure of individuals' private affairs.[117] Lowering moral and social standards are also possible results of unfettered curiosity and yearning for gossip. In the view of Warren and Brandeis, when personal gossip attains the dignity of (print), and crowds the space available for matters of real interest to the community, it nourishes triviality than robustness. With rapid mushrooming online blogs operated by a good mass of the youth, which requires just a computer and cheaply accessible internet, mainly CDMA wireless modems, privacy unfriendly incidents are in the horizon in Ethiopia.[118]

Another example is a newly launched television program called *'chewata'*, where in one of its episodes, the hosts tried to create fun by spraying water on innocent pedestrians from a hidden location. The right not to be subjected to unlawful molestation is among the various personality rights guaranteed under the Ethiopian Civil Code by which a person subject to molestation can

[115]Warren and Brandeis, supra note 111.
[116] Warren and Brandeis, supra note 111.
[117] Ibid.
[118]The wedding of music star Tewodros Kassahun (aka Teddy Afro) which attracted extensive media attention perhaps signals the future. On top of many photos of the musician and his bide gone viral over the net (apparently taken in what they call it the US Paparazi snapshots), some bloggers went a bit far to disclose sensitive previous individual relationships of the bride and bridegroom. See, for instance, Teddy Afro and Amleset Muchie Get Married, *Addis Journal,* september 27, 2012, available at < http://arefe.wordpress.com/>. [Accessed on September 27/2013]

demand cessation of the act[119] and perhaps be entitled to damages for harms done under extra-contractual liability.[120] A number of tort law provisions may also be invoked against the molestation by the media, physical assault and interference with ones liberty.[121]

3.6 Privacy and Collection and Cross-organizational Transfer of Personal Data

While Ethiopia doesn't have specific data protection law proper, there are a handful of provisions scattered across various legislations that provide for data protection. A good case in point is the duty of confidentiality provision of the Income Tax Proclamation (ITP). The tax authority is obliged under Article 39 of the ITP to keep tax information confidential except such disclosures, *inter alia*, to law enforcement agencies for prosecuting a person for tax violations. The same provision carves out an exception also for such disclosures to courts to establish tax liabilities or any other criminal cases.[122] Yet, bodies to which such information are disclosed are under obligation not to transfer the data to other parties except to the limit necessary to achieve the purpose for which the disclosure is permitted.[123]

In all other cases, disclosure of tax information is possible only when the taxpayer gives a written consent.[124] It is to be noted that the exception with regard to disclosure for law enforcement agencies is strictly qualified in that disclosure would be lawful only when it relates to a specific taxpayer, and

---

[119] The Civil Code of the Empire of Ethiopia, Proclamation No. 165/1960, Negarit Gazetta, Extraordinary Issue, Art 10.

[120] E. Stebik, *Ethiopian Law of Persons: Notes and Materials* (St. Mary University College Faculty of Law, 2007), p. 123.

[121] See the Civil Code, supra note 119, Arts 2038 and 2040 of.

[122] Income Tax Proclamation, supra note 84, Art 39(1(c)).

[123] Ibid, Art 39(2).

[124] Ibid, Art 39(3).

most importantly, it must be for the purpose of prosecuting tax violations such as tax evasion. This exception therefore doesn't allow disclosure to other authorities that may seek to proceed against a taxpayer for other purposes such as for prosecuting for crimes related to terrorism or treason. Given that tax violations are prosecuted by the tax authority itself as it has a special prosecution wing[125], there could not be tax violation cases that the intelligence authorities might be interested in.

That notwithstanding, a relatively recent law on prevention and suppression of money laundering and financing of terrorism categorically changes the duty of confidentiality noted above. According to this law, no obligation of confidentiality imposed by other laws (income tax law included) shall affect obligations of accountable persons[126] to report or furnish information on customers to competent authorities.[127] It hence completely lifts the duty of confidentiality of tax information so long as the latter happens to help to gather information on money laundering offences. This is not the only catastrophe that the law brought along; it also allows the competent authorities to share the information obtained to other authorities, be it local or foreign, without regard to the consent of the data subjects.[128]

---

[125] See the Proclamation to Provide for the Establishment of The Ethiopian Revenues and Customs Authority. No. 587/2008, Federal Negarit Gazeta., 14th year, No. 44, Art 7(2).

[126] The Ethiopian Revenues and Customs Authority is among the long list of accountable persons with the obligation to disclose confidential information to 'competent authorities'. See, Art 2(1(g)), A Proclamation on Prevention and Suppression of Money Laundering and Financing of Terrorism, Proclamation No. 657/2009, Federal Negarit Gazeta, 16th Year, No. 1.

[127] Art 2(4) of the Proclamation defines 'competent authorities' to include, among others, the Financial Intelligence Center.

[128] See Art 4(2) of the Proclamation No. 657/2009, supra note 126.

The Financial Intelligence Center, a body principally entrusted with enforcing the proclamation on the Prevention and Suppression of Money Laundering and Financing of Terrorism, is reportedly revising the law with view to make amendments.[129] According to reports, the revision mainly concerns providing detailed definitions of some of the terms in addition to making adjustments to the overall structure of the proclamation.[130] It is thus unlikely that the revision would concern the rules on disclosure of confidential information.

Other recent legislative developments are not also flattering. A recently adopted law on a uniform National Identification Card (NIC) permits cross-organizational transfer of data collected in the course of issuing the NIC to wide range of institutions including intelligence authorities without requiring the consent of the data subject.[131] The law stresses that information collected in relation to NIC has to be properly stored in a 'central database' in manner that the stored information could further be used for other purposes other than for which it was initially collected.[132] This proviso is at odds with one of the cardinal principles of data protection law called 'use limitation principles' which holds that 'use of personal data for purposes other than those specified should occur only with the consent of the data subject or clear legal

---

[129] E. Araya, Financial Intelligence Centre Drafting Anti-money Laundering Bill Update, Addis Fortune, Volume 13, Number 643 July 22, 2012; available at <http://www.addisfortune.net/Financial%20Intelligence%20Centre%20Drafting%20Anti-money%20Laundering%20Bill%20Update.htm.> [Accessed on September 27/2013].

[130] Ibid.

[131] See the Proclamation on the Registration of Vital Events and National Identity Card, Proclamation No. 760/2012, Federal Negarit Gazeta, 18th Year, No. 58, Arts 63 and 64. See also አዲስ አድማስ, ምስጢራዊ ቁጥር ያለው መታወቂያ የሚያሰጥ ረቂቅ አዋጅ ወጣ, June 23/2012.

[132] Ibid, Art 63(1). Intelligence and security agencies, tax authorities, crime investigation authorities are among a list of entities to which information collected in connection with NIC could possibly be disclosed.

authority'.[133] What is worrisome about these proposals is that the envisioned NIC database is set to include very private information about individuals such as 'ethnicity'.

In systems with developed data protection regimes such as the European Union, processing of sensitive personal data (which includes collection, disclosure by transmission and dissemination) is strictly prohibited save few exceptions such as when the data subject gives his explicit consent.[134] We suggest introduction of a clearly defined consent regime in those areas where disclosure of (sensitive) personal data is required.

3.7 Making Sense of Snowden's Leakes — The Impact on Privacy of Ethiopians

On June 6, 2013, The Guardian and the Washington Post revealed massive secret surveillance documents. Edward Snowden, a former US National Intelligence Agency (NSA) analyst, was later announced to be the source of the intelligence documents. According to the leaked documents, a top secret program called "PRISM" enables the NSA to directly access the servers and databases of internet giants such as Microsoft, Google, Facebook and Apple.[135] NSA analysts, through this program, are able to access users' search history, content of e-mails, file transfers and live online chats.

---

[133] See, L. Bygrave, "Data Protection Pursuant with the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, Vol. 6, 1998, p. 249.

[134] See, theEuropean Union Data Protection Directive 95/46, Art 8 available at < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF> [Accessed on September 27/2013]

[135] G. Greenwald and E. MacAskill, 'NSA Prism Program Taps into User Data of Apple, Google and Others', The Guardian, 7 June 2013, available at <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. [Accessed on September 27/2013]

Another related surveillance program called XKeyScore enables analysts to search, with no prior authorization, through vast databases containing e-mails, online chats and browsing history of millions of individuals.[136] Apparently, the surveillance concerned any internet user irrespective of his/her geographic locations. Indeed, it also covered foreign presidents and embassies of various countries.[137] This has resulted in stiff row between the US and other countries including its strategic allies. The EU, known for its robust data protection regime, threatened to suspend data sharing pacts that it has with the US.[138] This is notwithstanding the lots of criticisms forwarded and concerned aired from privacy advocates and commentators.[139]

Defending the surveillance, President Obama said that "it was a modest encroachment on privacy necessary to protect the US from terrorist

---

[136] G. Greenwald, XKeyScore: NSA Tool Collects 'Nearly Everything a User Does on the Internet', The Guardian, 31 July 2013, available at < http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. [Accessed on September 27/2013]

[137] The news that the surveillance targeted presidents of Brazil and Mexico caused controversies between the countries and the United States. See details at <http://www.bbc.co.uk/news/world-latin-america-23938909>. [Accessed on September 27/2013]

[138] A Croft, EU Threatens to Suspend Data-sharing with U.S. Over Spy Reports, Yahoo! News, July 5 2013, available at < http://news.yahoo.com/eu-threatens-suspend-data-sharing-033550042.html >[Accessed on September 27/2013]

[139] Dismayed by the news of surveillance, some scholars even preferred to suggest a better technical solution to curb massive surveillance of internet activities by the state, rewriting the internet! See, L. Lessig, 'It's Time to Rewrite the Internet to Give Us Better Privacy, and Security', The Daily Beast, June 12 2013, available at <http://www.thedailybeast.com/articles/2013/06/12/it-s-time-to-rewrite-the-internet-to-give-us-better-privacy-and-security.html>. [Accessed on September 27/ 2013] A more enlightnening work on the impact of the NSA spying on non-American wasby the British privacy expert Caspar Bowden. See, C. Bowden, The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and their Impact on EU Citizens' Fundamental Rights, Briefing Note to the European Parliament, September 2013. Available at <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf> [Accessed on September 27/2013]

attacks".[140] The US spy chief James Clapper defended the act stating that all the information gathered under PRISM was obtained with the approval of FISA court, a secret surveillance court established under Foreign Intelligence Surveillance Act of 2008 (as amended) to entertain requests for surveillance.[141] Obama's remarks that the 'the monitoring of internet communications doesn't apply to American citizens and those who live within the United States' fanned the fire as he made it crystal clear that non-Americans are targets of the surveillance programs. It is certainly true that US surveillance law is entirely clear in that non-US citizens and those who are not residing the US (Ethiopians included) are with no constitutional protections.[142]

Little is heard from Africa in general and Ethiopia in particular about the privacy invasions by the NSA. Given that only a few million Ethiopians are connected to the internet (about 2.5 million by the end of 2012), the lack of concern from Ethiopian internet users is not unexpected.[143] It is in fact doubtful if an average Ethiopian internet user had ever felt what the revelations meant to his/her privacy.

---

[140] M. Dorning and C. Strohm, 'Obama Defends Data Spying as Modest Privacy Encroachment', Bloomberg, June 8 2013, available at < http://www.bloomberg.com/news/2013-06-07/obama-defends-data-spying-as-modest-privacy-encroachment.html > [Accessed on September 27/ 2013]

[141] See US Spy Chief Clapper Defends PRISM and Phone Surveillance, BBC News, 7 June 2013, available at < http://www.bbc.co.uk/news/world-us-canada-22809541> [Accessed on September 27/2013]

[142] I. Brown,'Yes, NSA Surveillance Should Worry the Law-abiding', The Guardian, 10 June 2013, available at <http://www.theguardian.com/commentisfree/2013/jun/10/nsa-snooping-law-abiding>. [Accessed on September 27/2013]

[143] For more on the rampant oblivion on the right to privacy in Ethiopia, see K. Yilma, 'Where Does the Right to Privacy End?',Addis Fortune, Vol. 14, No. 688, 7 July 2013, available at <http://addisfortune.net/columns/where-does-the-right-to-privacy-end/>. [Accessed on September 27/ 2013]

What is more serious is the fact that Ethiopia does not have a legal framework through which internet content providers such as Google and Facebook, accessories in the above data snooping, could be held liable for breach of user data. Like many internet users in other countries, Ethiopian users barely have both the interest and the patience to thoroughly read through the terms of use of internet services of those companies which often are set out in rather complex and lofty manner. Most reluctantly and grudgingly accept those terms. In fact, there barely exists any other option than accepting the terms.

What is peculiar about these terms of use is that they are mere self-regulatory policies, not laws in the stricter sense of the expression. And, it is in response to this that may countries have enacted data protection laws that regulate acquisition, storage and processing of users personal data by service providers like Facebook, Google, and Yahoo!.[144] As already noted, Ethiopia doesn't have data protection law proper. The Information and Communication Technology Policy of 2009 however clearly recognizes the need to issue data protection law.[145] As the number of internet users increases overtime (the government plans to increase it to 3.69 million by the end of the Growth and Transformation Plan year), data privacy of Ethiopian

---

[144] Close to 90 countries have so for issued data protection laws. See, G. Greenleaf, 'Global Data Privacy Law: 89 Countries and Accelerating', Queen's Mary University of London School of Law, Legal Studies Research Paper No. 98, 2012, available at < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034&download=yes>. [Accessed on September 27/2013]

[145] See *The Federal Democratic Republic of Ethiopia, The National Information and Communication Technology Policy and Strategy*, Addis Ababa, August 2009, p. 8 *et seq*. Laws that regulate behavior online are on the pipeline in Ethiopia. A cybercrime law (drafted by the Information Network Security Agency) and E-commerce law (reportedly drafted by the Ministry of Communication and Information Technology in collaboration with UN Economic Commission for Africa) are examples. Nothing is, however, heard so far concerning data protection law.

internet users would undoubtedly be more vulnerable to abuses and breaches. It is therefore high time to promulgate a law that protects citizens from data privacy breaches by internet companies and foreign intelligence agencies.

4. Conclusion

Though to a varying degree, Ethiopia recognized the right to privacy of citizens throughout its constitutional history .Well informed by major international human rights instruments especially the UDHR and ICCPR, the FRDRE Constitution succinctly sets out the right to privacy of persons in their persons, home and communications. Nevertheless, the nature, scope and limits of the right to privacy have not received due academic interest. More importantly, the privacy provision of the FDRE Constitution and its interplay with other laws of the country with potential privacy implications have not been subjected earnest critique.[146] With the view to partly mitigate this void, this article has closely examined a selection of post-1995 laws and practices

[146] It is also doubtful if there have been cases litigated before courts that implicate right to privacy. Quite interestingly, in a widely acclaimed didactic TV program called '*chilot*', which presents role-playing of court proceedings concerning various laws of Ethiopia, an issue relating to privacy was recently raised. The matter related to customs/tax law violation where employees of the tax authority along with a tax/customs evader were accused of conspiring to let in goods without the proper customs procedure and without paying taxes due. The prosecutor presented an electronic evidence (obtained from a secret surveillance Closed Circuit Television or CCTV camera) to corroborate the charges of abetting and aiding the commission of the crime. And, the accused (employees of the tax authority) argued that such evidence should not be admissible as they were not aware of the existence of such secret surveillance and that they would do other 'private' activities assuming that the spot is not under surveillance. [Note that what the accused persons raised is what in the US privacy jurisprudence called "reasonable expectation of privacy", which literarily denotes that persons reasonably expect privacy when they are not in public places]. The court ruled, without any further inquiry, that there is no legal bases to exclude evidences obtained through secrete surveillance and that the issue shall rather be on how much weight shall be attached to the evidence. Note however that neither the court nor the accused persons mentioned Art 26 of the FDRE Constitution. See podcast of the program at < http://www.youtube.com/watch?v=luasDXonHcM>. [Accessed on September 27/2013]

and uncovered their potential implication on the constitutional right to privacy.

It began by tracing the origin of claims of privacy in primitive and modern societies. We noted that the desire for temporal seclusion and delineation of private sphere is to be found virtually in every society. The various conceptualizations of privacy such as privacy as non-interference, privacy as informational control, privacy as freedom and privacy as dignity have also been briefly highlighted. The second part of the article presented privacy as a human right and described privacy as provided in maior international human rights instruments and the FDRE Constitution.

The third part of the article closely scrutinized a selection of laws such as the recently adopted law of telecom fraud offenses, tax foreclosure rules, and criminal procedure rules in light of Article 26 of the FRDE Constitution. Collection and cross-organizational transfer of taxpayers' personal data, installation of deep packet inspection are among practices reviewed in the light of the privacy provision of the FDRE Constitution. We stressed that aspects of those laws and practices have presented insidious threat to the constitutionally envisaged right to privacy of citizens and must be revisited to live up to the requirements of the FDRE Constitution. Ongoing legislative initiatives such as the issuance of national identification number have also been raised in passing pointing out their potential privacy implication.

Accordingly, we proffer the following recommendations:
In order to prevent and control a terrorist act, the National Intelligence and Security Service and the police are empowered to use different methods ranging from electronic surveillance to warrantless search. The preventive

police work includes the use of covert and sudden searches. In a sudden search, the police officer is granted to carry out warrantless search and seizure solely on the basis of reasonable belief that a terrorist act may be committed. Such discretionary powers may pose a threat to the constitutional right to privacy. We recommend that such a search should be conducted upon judicial authorization.

ii. The Revised Anti-Corruption Special Procedures and Rules of Evidence Proclamation grants the head of appropriate organ to order a warrantless exclusive discretion to intercept the communications of individuals. Such a discretionary power would undermine the constitutional right to privacy. We suggest that interception should be made through judicial oversight.

iii. Given the low level of the development of the tax administration system and with the view to enhance confidence of taxpayers towards the tax system, and indeed to maintain constitutionality, we suggest embracing judicial authorization before taking abrupt collection. This applies mainly in relation to seizing the property of allegedly delinquent taxpayers.

iv. We strongly recommend clarity on the scope of the power police covert search powers and the discretion of courts in entertaining a request for a covert search warrant. The rule on the admissibility of evidences obtained through secret surveillance needs also to be revisited. This may better be dealt with by clearly setting out the powers and roles of both the police and courts in relation to covert searches. Once that is sorted out, all evidences collected through police surveillance in contravention of the search warrant would be inadmissible.

v. We found the anti-money laundering proclamation's rule that obliges a range of entities to disclose personal data of individual without the explicit consent of the individuals concerned as dangerous erosion of the right to privacy.

While we acknowledge the need to combat terrorism, obliging data controlling entities to disclose personal data of their clients represents the biggest threat to the protection of personal data. As a result, we recommend revising this part of the law and setting a clearer consent regime under the proclamation.

vi. At the most basic level, it is worth stressing the importance of exposing draft laws to public and expert debates before they enter the statute book. Views of experts and concerned stakeholders on draft legislations would significantly help in honing the laws thereby preemptively avoiding glitches during implementation.

vii. We also call the attention of concerned stakeholders including the relevant state organs and the media to pay attention to the privacy implications of evolving media practices. This should include extensive public awareness education on the right to privacy and its relation with the freedom of expression.

Finally, the authors want to stress that this article has focused on major laws and practices and there is a need for further study on these and other laws and practices in relation to their impact on the right to privacy.