Exploring Safeguards of Privacy Right in the Digital Age: How to Regulate Invisible Intrusion in Ethiopia?

Yisak Abraham*

Abstract

Everyone has some aspect of their personal life that should not be exposed involuntarily. Respect for privacy enhances personhood and dignity. Despite the immense significance of privacy, the extent of interference in private life has been increasing on account of emerging sophisticated surveillance technologies. It is not uncommon to notice surveillance cameras on streets, public and private places in Addis Ababa. Most often, the public does not know who is watching and the modalities of surveillance. On top of this, the images are stored and can be used for undesired purposes thereby encroaching on privacy rights. This article examines the possible threat posed by video surveillance cameras and assesses the adequacy of the existing legal framework in Ethiopia. To do so the article applies a mixed research methodology. Video surveillance rules developed elsewhere in the globe and literature in the field are analyzed through doctrinal research methodology. Foreign codes of conduct, theories, and experiences would be a good lesson in designing the Ethiopian video surveillance code of conduct. Finally, the article recommends for the adoption of a strong regulatory framework for video surveillance that aligns with international standards and best practices.

Keywords: video surveillance, the right to privacy, pervasive, interference, protection, regulatory framework

1. Introduction

The right to privacy is one of the very crucial human needs that enhances personhood and dignity. Everyone aspires for some form of privacy. Some aspects of life should be kept private and should not be disclosed to everybody. Privacy, therefore, is an aspect of human life. However, the meaning, and nature of privacy as well as "an exact line of delineating a private and public part of our life is not easy. Simply put, as it is not easy to define the term privacy as its contours are blurry. Consequently, it is claimed that the term privacy is a "slippery concept"[1] - "a concept in disarray."[2]

*LL.B., LL.M. Public Prosecutor, Hadya Zone, S/N/N/R/S. The Authtor is grateful to Dr. Tsega Andulem for the assistance rendered to Article to be accepted for publication. The author may reached at, yisakabrahamj2551@gmail.com

[1] James Q. Whitman: *The Two Western Culture of Privacy: Dignity Versus. Liberty,* Yale L. J. Vol. 113 (2004) p. 1153-54. https://www.yalelawjournal.org/pdf/246_ftn7jo8w.pdf (accessed 7/30/2022), See also Samuel D. Warren & Louis D. Brandies, *The Right to Privacy*, Harv. L. Rev. Vol. 4 No.5 (1890), p. 193 – 220). https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (accessed 7/30/22).

[2] Finn, R.L, Wright, D., Riedewald, M. "Seven Types of Privacy." In: Gutwirtch, S., Leenes, R., de Hert, P., Poullet, Y. (eds) *European Data Protection: Coming of Age*. Springer, Dordrech. (2013) p.3 https://doi.org/10.1007/978-94-007-5170-5_1 See also R.Finn and D.Wright, "Seven types of privacy" Trilateral Research & Consulting, London Michael Friedewald, Fraunhofer ISI, Karlsruhe January (2013) p.4.

No one can exactly articulate the notion of "privacy in a way acceptable to all. Scholars "[…] have frequently lamented the great difficulty in reaching a common satisfying conception of privacy,"[3] and generations often question its boundary line. Supposedly, culture, religion, and the way of life shape facts and factors that determine the contours of privacy. Be this as it may, all communities and individuals demand some form of privacy. What really privacy is, and how can we protect one's quest for privacy? The issue is more perplexing when one's privacy is unnoticeably invaded through invisible intruders.

As it can be fairly imagined, the term privacy sprung from the word "private" and defined in terms of one's interest in keeping undisclosed and undisclosable facts private. Thus, "privacy right" is *"*the right to be let alone [or] the right of a person to be free from unwarranted publicity."[4]

Despite the absence of an exact definition of the term "privacy" and the expression "privacy right," almost all states have recognized privacy right as a protectable right. Privacy is an umbrella concept that encompasses, *inter alia*, freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches, seizure, and interrogation.[5]

Though privacy right was articulated in the modern sense in academic discourse in the late 19th century, it was as old as mankind.[6] The concept of privacy emerged from the natural need to make a distinction between oneself and the other world. In ancient times, people "had a relatively limited possibility for self-determination as their private lives were strongly influenced by the state."[7] In the medieval period, individuals existed as members of a community, and so, private life was affected by constant "monitoring" conducted by other members of the society. The appearance of real privacy relates to the transformation of those small communities into cities.[8] The need for

https://www.researchgate.net/profile/MichaelFriedewald/publication/258892458_Seven_Types_of_Privacy/links/0c9605295d271f1575000000/Seven-Types-of-Privacy.pdf (accessed 7/30/2022)

[3] *Id*.
[4] *Id*.
[5] Daniel Solove, Understanding Privacy Harvard University, press (2008) p.7
[6] Adrienn Lukács *What is Privacy? The History and Definition of Privacy* https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (accessed 7/30/2022)
[7] *Id.*
[8] *Id.*

privacy was mentioned in primitive codes like Hammurabi, Holy books (the Holy Bible, the Qur'an,), Jewish law, and ancient communities (Greece and ancient China).[9]

During the 19thc, the new changes in the economy and society led to the transformation of the way of life that had generated change in social integration and impacted privacy. The growth of cities and population caused physical loss of privacy as people in cities had to live in crowded vicinities.[10] Further, the proliferation of invasive newspapers and other public media generated fertile ground for gossip and photojournalism.[11] Newspapers invaded private life, by exceeding hitherto untouched spaces to satisfy a prurient taste.[12] This has ignited the quest for privacy. As a result, privacy has become more important to individuals. Then, because of interference in private and domestic circles of individuals through invasive publications, a greater call for the legal protection of private matters and privacy was sprung.[13]

The right to privacy is one of the dynamic rights that have evolved through time. Today, the right to privacy is considered one of the most important human rights deserving legal protection.[14] Its meaning and elements expand with the technological advancement. Respect for privacy frees us from the worry of being watched (panoptical phenomena) and judged by those around us and enables us to control how and when we share information and so forth.[15] Undoubtedly, privacy is essential to one's autonomy and protection of human dignity thereby serving as a foundation upon which numerous other human rights are built. It is for reason that privacy right has been recognized in social as well as legal senses.[16]

Despite the crucial quest for privacy, the emerging surveillance technology, like video surveillance technology makes us wonder about the level of protection of our right to privacy. Today, personal

---

[9] Hixson, R., *Privacy in a Public Society: Human Rights in Conflict*, Oxford University Press, New York (1987) p. 3.

[10] *Id*.

[11] Bratman, B. E. Brandeis and Warren's, "The Right to Privacy and the Birth of the Right to Privacy", Tennessee Law Review Vol. 69. (2002). p. 344.

[12] Samuel D. Warren & Louis D. Brandeis *supra* note 1.

[13] *Id.*

[14] Alexandra Rengel, *Privacy in International Law Privacy as an International Human Right and the Right to Obscurity in Cyberspace,* Groningen J. of Int'l Law, Vol 2(2) (2014) p. 34.

[15] For an overview of the different theories of privacy, see Solove, D.J. "*Conceptualizing Privacy"*, California Law Review 90 (2002) P.1087-1155; Solove, D.J: *Understanding Privacy* (Harvard University Press: Cambridge, Mass.) (2009); and Nissenbaum, H. (2010), Privacy in Context (Stanford University Press: Stanford, California).

[16] Rachel Finn and David Wright *supra* note 2.

information can be accessed, not by infringing our physical space, but through invisible hands that can unnoticeably intrude our personal vicinities and get access to our most vital secrets just by a simple click for commercial or other purposes.

The issue of invisible intrusion through video surveillance systems also concerns Ethiopians, as the country has started to use highly sophisticated video surveillance devices that are planted in public and private infrastructures. Yet, the regulatory landscape is absent or weak. More specifically, questions like how far the existing Ethiopian laws address the issue of video surveillance technology and the right to privacy need scrutiny. With a view to proactively tackle the potential threats of surveillance systems lessons can be learnt from advanced systems. This article attempts to address the compatibility of public interest through video surveillance and privacy right.

After a brief discussion on provocative issue of nature and scope of privacy right in Part I, the Second Part briefly discusses the right to privacy as stipulated in the international and regional human rights instruments. Part Three examines the implications of video surveillance on the right to privacy. The regulation of video surveillance in Ethiopia from the perspective of the right to privacy and possible lessons that can be learned from advanced systems is briefly discussed in Part Four.

2. The Protection of the Right to Privacy under International and National Laws

2.1. The Right to Privacy under International Human Rights Law

Most important international human rights instruments recognize the right to privacy as a central aspect of human dignity.[17] The right to privacy is enshrined under the UDHR[18] and other bills of rights.[19] Pursuant to Art. 17(2) of the ICCPR, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks upon his honor and reputation."[20] In General Comment No.16 the committee noted that, privacy right to be guaranteed against all unlawful and arbitrary "interferences and attacks whether they emanate from

[17] Alexandra Rangel *supra* note 14.
[18] See Article 12 UDHR. It imposes a general restriction on Article 29.
[19] ICCPR, Art. 17.
[20] *Id*; The Universal Declaration of Human Rights, Art. 12.

State authorities or from natural or legal persons."[21] The Committee also attempted to elaborate on the meaning of unlawful interference – it is invasion of privacy that is not envisaged by law.

Moreover, as stipulated in General Comment No. 16, the respect to right to privacy "requires the State to adopt legislative and other measures to give effect to the protection of this right."[22] Article 12 of the UDHR provides the same rule. This has inspired numerous constitutions to follow the same suit in recognizing the requirement to take position action that has power to enforce the right to privacy, and "limit the ability of individuals, private organizations and the state to collect information about people's personal lives, or to monitor them without their knowledge or consent ever than before."[23] Regarding the substances of domestic privacy protecting laws, the spirit of the General Comment No.16 indicates that such laws must be in conformity with the provisions, aims, and objectives of the ICCPR. This builds international compatibility, while permitting some form of flexibility in domestic implementation.[24] Moreover, General Comment No.16 provides room for the possibility of limitation on privacy right.[25] As all rights are not absolute, the right to privacy also suffers from exceptional limitations. Exceptional situations cannot be presumed. There shall be an express declaration that restricts the right to privacy. The law requires the limitation should be necessary and proportional to the situation that necessities encroachment on privacy right.

2.2.The Right to Privacy under Regional Human Rights Treaties

2.2.1. Protection of the Right to Privacy in Europe

Comparatively speaking, Europe has more developed jurisprudence on the privacy right. In Europe there are various treaties that = protect privacy. Some of them are solely concerned with the issues of privacy. Other regions have no such comprehensive normative framework that is typically meant to regulate privacy. Among the other instruments, the very important treaty in the region is the European Convention on Human Rights. Article 8 of the Convention provides:

[21] General comment No. 16: Article 17 (Right to privacy) Thirty-second session (1988), pp.1.
[22] ICCPR General Comment No. 16: Article 17 (Right to Privacy) Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988.
[23] Alexandra Rangel *supra* note 14.
[24] The UN Conference on Trade and Development, Data Protection Regulations and International Data Flows, in New York and Geneva (2016).
[25] GA Report of the Human Rights Committee (43rd session) A/43/40, (1988), par.7-9.

1. Everyone has the right to respect for his private and family life, his homes, and his correspondence.
2. There shall be no interference by a public authority with the exercise of his right except such is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [26]

This article provides for protection against unlawful and arbitrary interferences with the right to privacy; contents of the right; obligation of member states to promulgate privacy protecting laws; and principles that governs measures limiting the right to privacy.

Next to the Convention, the most significant comprehensive privacy protection legislation having significance, not only in the region, but also in the wider world is the European community's Directive of 1995.[27] It sets standards of privacy protection to be incorporated by all members of the community in their national legal documents.[28] The directive requires that personal data be "processed fairly and lawfully; limits purpose for which personal data may be used to situations where the individual has given consent or where use is required by law; seeks to ensure the openness of data systems for scrutiny and change by data subjects; requires confidentiality and security in processing of data; and calls all member states to create an independent "supervisory authority" to monitor the application of the directive."[29] The need for supervisory organ is particularly special one in this directive than other international and regional laws.

Another very important treaty in the region is the convention for the protection of automatic processing of personal data called the "Council of European Convention on Data Protection (ETS No.108/1985)." Article 1 of the Convention stipulates:

> The purpose of this Convention is to secure in the territory of each party for every individual whatever his nationality or residence, respect for his rights and

[26] Council of Europe, European Convention on Human Rights, (4 Nov.1950) Article 8 (1 & 2).
[27] James B. Rule, *Privacy in Peril* (Oxford University press, 2007), p.31.
[28] *Id*.
[29] *Id*.

fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data (data protection).[30]

As the protection of personal data falls within the realm of private life, the convention purports to protect individuals against abuses while collecting and processing "personal data and seeks to regulate at the same time the trans-frontier flow of personal data."[31] ETS also enshrined the subjects of surveillance's rights to know what information is stored on him or her and, to have it corrected if required.[32]

The additional protocol of ETS, 1985 also enhances the protection of personal data and privacy by improving the original convention of 1981 by providing for the setting up of a national supervisory body responsible for ensuring compliance with laws adopted in conformity of the convention concerning personal data protection.[33] One more improvement is on transboundary data flow to the non-member states. Accordingly, data may only be transferred if the recipient State or IO is able to afford an adequate level of protection.[34]

2.2.2. Protection of the Right to Privacy in Africa

The African Charter on Human and People's Rights of 1981 does not expressly provide for the right to privacy.[35] But, it does not mean that there is no legal protection for privacy in the region. For instance, one can see the Declaration of African Commission on Human and Peoples Rights' (hear after, DACHPR) that shows the jurisprudence of the commission on privacy. The ACHPR expands States obligation concerning access to information and developed the standards related to new areas of concerns including a legal framework on privacy and the protection of personal information under its new Declaration on Principles of Freedom of Expression and Access to

---

30 ETS No.108/1985, Art. 1.

31 European Commission for Democracy through Law: "Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights," adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006\p.9 &10.

32 *Id*.

33 Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans Border Data Flows, into force on 1 July 2004.

34 *Id*.

35 Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties,* Int'l J. of L. & Tech, Vol. 6 (1998) p. 247 – 287). https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf (accessed 7/30/2022).

Information in Africa (2019) or the Declaration of article 9 (the right to receive information and free expression) of the African Charter on Human and Peoples' Rights (the Declaration).[36] As per the principles 40 & 41 of the declaration, the commission directly addressed the protection of personal information and communications surveillance in the context of the right to privacy. If we see principle 42 of the Declaration, it establishes a regulatory framework for the protection of personal information that requires States to adopt laws regulating the processing of personal information.[37]

In addition, States must ensure that individuals consent to the processing of their personal information; the processing also should be "in accordance the purpose for which it was collected"[38] and not excessive; the data is deleted when the processing is complete; the processing should be transparent; and also the information should be held confidential and be "secure at all times".[39] Moreover, the principle also provided for the mandatory accessibility of personal information to the data subjects and an opportunity to object the processing. An individual also must be notified when an unauthorized person has accessed their information and must have access to "legal recourses to effective remedies in relation to the violation of their privacy".[40]

Another very important regional legal framework relevant to the right to privacy is the Malabo Convention on Cyber Security and Personal Data Protection adopted in 2014.[41] The Convention stipulates the basic principles governing the processing of personal data aiming at protecting the right to privacy. Article 13 of the Convention provides for the principles of consent and legitimacy of personal data processing; purpose, relevance and storage of processed data; accuracy of personal data; transparency of personal data processing and confidentiality and security of personal data.[42]

---

[36] Privacy International at the Sixty Second Session of the African Commission on Human and People's Rights (April 2018). https://privacyinternational.org/news-analysis/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights (accessed 7/30/2022).

[37] ACHPR, Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019, principle 40-41.

[38] Principle 42.

[39] *Id*.

[40] *Id*.

[41] African Union Convention on Cyber Security and Personal Data Protection, adopted June 27, 2014, last signature May 11, 2020, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 7/30/2022).

[42] *Id*. Art. 13.

Furthermore, the convention stipulates special rules for the processing of sensitive data under article 14.[43] Accordingly, the State shall:

> " […] undertake to prohibit any data collection and processing revealing racial, ethnic, and regional origin, parental filiations, political opinions, religious or philosophical beliefs, trade unions membership, sex life and genetic information or more generally on the state of health of the data subject."[44]

Another very crucial protection is the provision for the "Data Subjects right"-the right to information,[45] to access,[46] to object,[47] and right of rectification or erasure.[48] To ensure better protection of the right, the convention also imposes obligation on the state parties to establish an independent authority in charge of protecting personal data.[49] "Preliminary personal data processing formalities" are there to be checked out by the authority concerned.[50] The treaty also imposes obligations of confidentiality,[51] security,[52] storage,[53] and sustainability[54] on the personal data controllers. At sub-regional level, the existing privacy laws framework in Africa includes the SADC Model Law on Data Protection (2010), ECOWAS Supplementary Act on Personal Data Protection (2010), and EAC Framework for Cyber Laws (2008).[55]

At a national or domestic level, many African countries have been attempting to take steps toward protecting the right to privacy, both online and offline as well. Primarily, almost all States in Africa are parties to the major international human rights instruments incorporating provisions for the protection of the right to privacy.

---

[43] *Id*. Art. 14.
[44] *Id.*
[45] *Id*. Art. 16.
[46] *Id*. Art.17.
[47] *Id*. Art. 18.
[48] *Id*. Art. 19.
[49] *Id*. Sub-art. (1),(a) of Art. 11.
[50] *Id*. Art. 10.
[51] *Id*. Art. 20.
[52] *Id*. Art. 21.
[53] *Id*. Art. 22.
[54] *Id.* Art. 23.
[55] Verengai Mabika (Senior Policy Advisor – Africa) Privacy & Personal Data Protection Guidelines for Africa p. 6 https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf (accessed 7/30/22).

Another indication is that, nearly all countries in Africa have recognized a specific right to privacy in their constitution, and some states even have introduced somehow comprehensive privacy laws, particularly of data protection legislation.[56] Until 2016, 17 countries in Africa have enacted a comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia, and Western Sahara.[57]

As some scholars argue, the driving factor for such progress in the protection of privacy in Africa is the need for adequate protection of personal data for the trans-border flow of personal data from Europe to other States as stipulated under article 25(1) of the European Union's Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data 95/46/EC. Accordingly, the Africa's trade with Europe has posed pressure on states to ensure that their data protection laws and directives are in line with this requirement to conduct business with European countries, i.e., the economic importance of meeting the requirement.[58] Other factors are "the development of internet, the operations of multinational corporations, and the trans-national flow of data."[59]

2.3. The Right to Privacy under Ethiopian Laws

In Ethiopia, there is no comprehensive privacy law till now. Despite the lack of comprehensive privacy law, Ethiopia is one of the countries that expressly recognized the right to privacy in various legislation including the Constitution. Primarily, the FDRE Constitution protects the right to privacy in two significant dimensions. First, it expressly recognizes the right to privacy and stipulates the restrictive conditions/principles (necessity, legality, and proportionality) of privacy as follows:

> 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.

---

[56] Arthur Gwagwa *et al*, *Protection of the right to privacy in Africa in the digital age IDRC& CRDI* (May 2014) p.7, https://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf (accessed 7/30/22).

[57] Cynthia Rich "Privacy Laws in Africa and Near East "Bloomberg BNA World Data Protection Report, 1, (2016), https://paperzz.com/doc/7620737/privacy-laws-in-africa-and-the-near-east (accessed 7/30/22).

[58] Arthur Gwagwa *et al* *supra* note 56 p.5.

[59] *Id*.

> 2. Everyone has the right to the 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."[60]

Sub-art. 1 encompasses possible contents of the right to privacy. But, when compare it with the contents of article 17 (1) of the ICCPR does not hold all aspects of the right to privacy.

Secondly, the constitution integrated the International Human Rights Instruments into laws of the land (Art. 9(4). Thus, the rules and principles regulating the right to privacy under the UDHR, ICCPR, CRC, Convention on the Protection of Migrants, the African Charter on Rights and Welfare of the Child (1990) and the UNGA (2013) Resolution on the Right to Privacy in a Digital Age are applicable as part and parcel of the Ethiopian privacy laws. Furthermore, the fundamental rights and freedoms including the right to privacy specified in Chapter three of the Constitution "shall be interpreted in a manner conforming to the principles of the Universal Declaration of Human Rights, International Covenants on Human Rights and International instruments adopted by Ethiopia."[61]

Though not comprehensive enough, the subsidiary laws which have extended guarantees to privacy include: article 32 &33 of the Criminal Procedure Code of Ethiopia,[62] article 6-9 & 12 of the Freedom of Mass Media and Access to Information Proclamation, [63]article 4&29(2) of the Electronic Signature Proclamation,[64] article 39 of the Income Tax Proclamation,[65] article 64(1) of the Registration of Vital Events and National Identification Cards Proclamations,[66] article 21 of the Documents Authentication and Registration Proclamation,[67] article 11, 13, 20,24, & 31 of the

---

[60] The FDRE Constitution, Proc. No. 1, 1995, Fed. *Neg. Gaz.* Year 1, No. 1, (Aug 1995) A.A., Art. 26.
[61] *Id*. 13(2).
[62] Ethiopian Criminal Procedure Code, Proc. No. 185/1961, Arts. 32&33
[63] Freedom of Mass Media and Access to Information Proclamation, Proc. No.590/2008, Arts. 12 & 6-19.
[64] Electronic Signature Proclamation, Proc. No.1072/2018, Arts. 4 & 29 (2).
[65] Income Tax Proclamation, Proc. No.286/2002, Art. 39.
[66] Registration of Vital Events and National Identification Cards Proclamation, Proc. No.760/2012, Art. 64 (1).
[67] Authentication and Registration of Documents, Proc. No. 922, 2015, Art. 21.

Civil Code of Ethiopia[68]. In the context of the specific sectors governed by these laws, the provisions impose some obligations on data collectors like, an obligation to hold personal information confidentially, and grant some rights to data subjects, for example, the right to be consulted for their consent in case their personal information required to be disclosed.

Unlawful and arbitrary interferences into the right to privacy are punishable under the Ethiopian criminal law regime. In accordance with article 604 of the Criminal Code of the Federal Democratic Republic of (hereafter the Criminal Code) "Violation of Privacy of Domicile or Restricted Areas" i.e. Entering into domiciles, or restricted areas unlawfully, and without the permission or wishes of the lawful occupant, and even refusing to leave such premises after having entered with permission or without opposition of the lawful occupant is punishable with simple imprisonment not exceeding 3 years, or fine.[69] In case of the violation "committed by a public servant who is not authorized to take such action, or who does so in violation of legal safeguards and formalities, the special provision (Art. 422) shall apply."[70] Aggravating circumstances to this offence are also listed under article 605 of the Code. Accordingly, if the offence is committed by "carrying weapons, making use of threats or resorting to violence; by a group of persons acting in common; or between the hours of 6 PM and 6 AM; or by a person holding himself on to be a public servant or official, unless otherwise authorized by law, is punishment shall by rigorous imprisonment not exceeding five years."[71]

Article 339 of the Code also stipulates breaches of professional secrecy as a crime. The Code also protects privacy of communications under article 606. Violation of the Privacy of Correspondence or Consignments is "punishable up on compliant, with a fine not exceeding one thousand Birr, or according to the circumstances of the case, with simple imprisonment not exceeding three months."[72] More severely, intentional and unlawful interceptions, destructions, retentions, or diversions from their true destination of the "correspondences or packages, is punishable upon accusation with simple imprisonment not exceeding six months, where his act does not constitute a specific crime punishable more severely."[73] However, the Criminal Code does not incorporate

[68] Civil Code of Ethiopia, Proc. No.165/1960, Arts. 11, 13, 20, 24, & 31.
[69] Criminal Code of the Federal Democratic Republic of Ethiopia, Proc. No. 414/2004, Art. 604(1).
[70] *Id* sub-art. 2.
[71] *Id.* Art. 605.
[72] *Id*. Art. 606.
[73] *Id* sub-art. 2.

all possible violations of types of privacy noted at the beginning of the article and the punishments provides for are somehow simple and it would be great if the crimes were made punishable up on accusation than upon a complaint.

Another criminal law safeguards for the right to privacy in Ethiopia are stipulated through sector-specific privacy protecting laws such as the finance sector privacy rules (the National Payment System Proclamation No. 718/2011,[74] the Payment Instrument Issuers Directive[75] and the Banking Business Proclamation,[76] ICT sector (Part II of the Computer Crime Proclamation),[77] and so on. Yet, it is possible to argue they if we examine the criminal law, we cannot get any provision that deals with the infringement of privacy through secret video cameras which are very pervasive by their nature and becoming common in Ethiopia.

Concerning judicial precedent, we have very few cases that are reported in the area of privacy. One notable case is *Riyan Miftah* v. *Elsewdi Kebels Plc*[78] in which Court ruled that images of a person cannot be publicized without consent of the person concerned. The Draft Data Protection Proclamation which is initiated by the Ministry of Innovation And Technology is expected to fill the existing gaps in the field and be used as a starting point to have a comprehensive and sufficient privacy law in Ethiopia. As to the Director General of the Legal Service Directorate in the Ethiopian Innovation and Technology Minister, the Draft Proclamation is assumed to regulate issues related to privacy comprehensively and adequately, particularly aimed to protect and minimize the technological threats posed on the right to privacy and the draft introduces an authority namely, Privacy or Data Protection Commission.[79] Currently, the draft is completed at the Ministry level and is to be sent to the Federal Attorney General soon. Also, some minimal provisions of the 2016 Computer Crimes Proclamation are expected to fill the existing gaps on the field and be used as a basement.

Despite the efforts which have been made to protect the right to privacy throughout its legal history, an adequate protection of privacy is yet to be realized in Ethiopia. As some studies

[74] National Payment System Proclamation Proc. No. 718/2011, Art. 35 (2) (e).
[75] Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020, Art 17
[76] Banking Business Proclamation, Proc. No. 592/2008, Art. 58 (7).
[77] Computer Crime Proclamation, Proc. No. 958/2016, Art. 3 – 8.
[78] Cassation Court of the Supreme Court of Federal Democratic Republic of Ethiopia, File No. 91710.
[79] Interview with Ato Hayalneh Lemma, the Legal Service Directorate Director at Ethiopian Innovation and Technology Minster, 20 April 2021.

indicated, like most African countries, Ethiopia faces contemporary challenges that threaten data protection and privacy.[80] Over the past decade, the Ethiopian government has procured and deployed numerous surveillance and intrusive technologies in Ethiopia.[81] As Berhan Taye and Roman Teshome explained in their study "Privacy and Personal Data Protection in Ethiopia", the causes for the mass violation of the right to privacy by public and private bodies in Ethiopia include, but are not limited to lack of comprehensive institutional framework, lack of implementing policy guidelines for privacy-protecting laws, absence of sufficient transparency and consultation while drafting laws, an inadequate legal framework for privacy, and the emerging pervasive technologies.[82]

3. The Right to Privacy in the Era of Technology: How Can We Control Invisible Intruders?

3.1. The Effort to Regulate Video Surveillance

Historically, the debate on the relationship between new technologies, and issues of human rights appeared in 1968 during the International Conference on Human Rights in Tehran, which brought some recommendations for deliberation by the United Nations General Assembly, hereafter (UNGA), and then the Resolution number 2450(XXIII) which mainly reflects on the protection of human right in the age of digitalization was adopted.[83]

In the world we are living today, there is a high tendency to use the emerging highly sophisticated surveillance technologies to ensure security and safety at government, business organizations and individual levels. Even some scholars argue that the protection and conceptualization of privacy cannot be detached from technological development.[84] There are a range of newly emerging sophisticated surveillance technologies such as growing automated surveillance in public places, internet surveillance, deep packet inspection, automatic license plate recognition systems, satellite monitoring, cell-phone tracking, facial recognition, CCTV, drone-based surveillance, and so forth,

---

[80] Berhan Taye & Roman Teshome *Privacy and Personal Data Protection in Ethiopia* (2018), https://cipesa.org/?wpfb_dl=379 (accessed 7/30/2022).

[81] *Id* p.5.

[82] *Id* p.25.

[83] Coccoli, J., "The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era," *Peace, Human Rights Governance,* Vol.1 (2), (2017) p. 3&4.

[84] Ann Cavoukian, *Surveillance, then and now: Securing Privacy in Public Spaces,* (June 2013), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf (accessed 7/30/2022).

to which the international and domestic laws have yet to respond effectively.[85] In the words of Alexandra Rangel:

> To determine the effect of new technologies on the right to privacy, and provide adequate solutions, a contextual analysis of the potential infringements that technology facilitates and the resources available for protection is essential.[86]

Unlike some other rights, the negative impact of technological advancements on the right to privacy seems to outweigh its benefits. In her study entitled "the impact of technology on the privacy of the individual," Rosenberg, concluded that; "technology continues to be viewed as a threat to privacy than a possible solution."[87] In reviewing the concept of privacy, new technologies often make us wonder what level of protection of privacy is possible in a world where personal information about us can be accessed not by interfering physical space, but by pressing a button and looking at a screen.[88] In addition, due to the development of science and technologies, the intrusion into someone's privacy is getting increased.[89] It is now very easy for companies and governments to monitor every conversation we conduct, every location we visit, and each commercial transaction we undertake. Such capabilities may lead to negative effects on individuals. They also affect how we think about the relationships between individuals, markets, society, and the state. Electronic surveillance can lead to a feeling of fear and of always being watched. Such negative impacts in turn result in loss of dignity.[90] Further, the most visible challenge to privacy is that the right can be compromised without the individual being aware of it.[91] In physical invasion of the right of privacy individuals are aware of the intrusion-being detained, censored, or restrained.[92] Besides, individuals are aware of the transgressor in case of other rights.[93] This has a great contribution in holding the transgressors responsible for what they have done, in case of unlawful and arbitrary interference. But this is very difficult in the case of

---

85 *Id*.
86 Alexandra Rangel *supra* note 14 p. 10.
87 Rosenberg, The Impact of Technology on the Privacy of Individual, (1994), http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html (accessed 7/30/22).
88 Alexandra Rangel *supra* note 14 p. 1.
89 Adrienn Lukács *supra* note 6.
90 J.J.Britz, *Technology as a threat to privacy: ethical challenges to the information profession* university of Pretoria South Africa, http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html, (Accessed 7/30/22).
91 Privacy International, https://privacyinternational.org/explainer/56/what-privacy (Accessed 7/30/22).
92 *Id*.
93 *Id*.

the right to privacy as the interferer's hands are most of the time invisible. We are also not being informed about the monitoring we are placed under and are not equipped with the capabilities or given the opportunity to question those activities. That means the surveillance technologies are excluding us from being involved in decisions about how our lives are interfered with, our information processing, our bodies securitized, and our possessions searched. So, secret surveillance is posing a great danger, because of its intrusiveness, lack of accountability and so on.[94]

While Government organs use technologies for the sake of law enforcement,[95] Even "surveillance of specific individuals- often journalists, opposition figures, critics and others exercising their right to freedom of expression has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings."[96]

One of the threats to privacy rights is the collection of a large amount of personal data by government organs, without adequate legal, regulatory, and policy frameworks.[97] Usually, most of African countries, including Ethiopia face such challenges too.[98] For example, over the past decade, the Ethiopian government has procured and deployed numerous surveillance and intrusive technologies.[99]

3.2.The Threats of Video Surveillance on the Right to Privacy

Despite the significant benefits brought by technological advancements all over the world, surveillance technologies, including video surveillance, pose direct and indirect human rights infringements. This Section focuses on video surveillance technology and its possible threat to privacy. As a mechanism of tackling terrorism, the widespread use of surveillance technology has become a common phenomenon even in Ethiopia. Basically, "surveillance camera system" is a system that includes the Closed Circuit Television (herein after CCTV), Body Worn Video, Drones, Dashboard Cameras, Automatic Number Plate Recognition (ANPR), Automatic Facial

---

[94] *Id.*
[95] Ann Cavoukian, *supra* note 84.
[96] UNHRC, Special rapporteur, surveillance and human rights, human rights council –forty –first sessions, https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session41/list-reports (Accessed 7/30/22).
[97] Berhan Taye & Roman Teshome *supra* note 80.
[97] *Id.* p.2.
[98] *Id.*
[99] *Id.* p.5

Recognition (AFR) technology etc.[100] CCTV is a system that allows one to keep an eye on what is going on in and around certain premises.[101] Cameras and monitors enable us to view events live and recorded footage for later reference**.** CCTV, therefore, is an electronic surveillance tool that employs a "network of cameras to monitor a particular area for protection against violence, terrorism, theft,"[102] vandalism and other criminal acts as well.

The sophisticated video surveillance system may include *thousands of cameras linked together* making use of technology to automatically identify and track a particular person from one location to another.[103] The cameras are enabled to pan, tilt, diagnose and provide a lot more detailed images of even very distant objects than previously possible. There is a camera that has 60 times optical zoom lens that can read even tiny letters like terms written on a cigarette pack at 100 yards.[104] More surprisingly, even 400 times magnification cameras have been deployed in some cities.[105]

Also, improved quality of recordings, reduced storage costs, and the use of digital technology enabled traversing and exploitation of recorded data in ways previously impossible with analogue recording systems. Furthermore, although facial recognition and other biometric systems are yet in their infancy, advancements in these areas can be integrated with CCTV systems to track movement in their field of view or across networked cameras allowing an operator to automatically follow a target object in an entire city in real-time or the stored data.[106] As a result of improvements in video surveillance technology, the system is cost-effective and efficient to fight severe threats to public safety with minimum human power. Due to this advantage of CCTV, nowadays, there is high interest to use the technology. For instance, there are more than 4 million cameras in the

---

[100] See the United Kingdom Protection of Freedom Act of 2012 (PoFA), Section 29(6).

[101] See State systems, https://www.statesystemsinc.com/blog/what-is-cctv (Accessed 7/30/22).

[102] Mahmoud Rajpoot, Q., & Jensen, C. D, "Video Surveillance: Privacy Issues and Legal Compliance," In V.Kumar, & J. Svensson (Eds.), Promoting Social Change and Democracy through Information Technology IGI global, (2015). https://backend.orbit.dtu.dk/ws/files/110934780/Video_Surveillance_Privacy_issues_and_legal_compliance.pdf (Accessed 7/30/22).

[103] Moncrieff, S., Venkatesh, S., & West, G. A. *Dynamic Privacy in Public Surveillance* (2009) p., 22–28.

[104] Slobogin, C. Camera *Surveillance of Public Places and the Right to Anonymity*, Mississippi Law Journal, 72(1), (2002) p. 213−233.

[105] Stephen Kinzer, *Chicago Moving to Smart' Surveillance Cameras*, The New York Times, https://www.nytimes.com/2004/09/21/us/chicago-moving-to-smart-surveillance-cameras.html, (Accessed 7/30/2022).

[106] *Id*.

UK alone, [107] and it is estimated that an average person in London is caught on camera around 300 times a day.[108]

The use of the surveillances system is backed by a legitimate purpose. Its primary aim was to tackle people and transactions that are potentially dangerous for the maintenance of peace and security. Continuous surveillance is assumed to reduce destructive crimes ranging from terrorism to traffic regulation. However, the practice does not guarantee the system would work. In the UK, where surveillance cameras (more than 4 million) have been extensively deployed in public places, crime rates never changed.[109]

Ruther, the combination of the pervasive form of the system with the technological advancements such as high resolution, magnification, identification, and tracking have the potential to disrupt the balance between the need for managing peace and security, and the right to privacy. It is reported thatthe right to privacy is at stake because of extensive video surveillance. For example, in a report by the BBC in 2005 two Council CCTV workers used the technology CCTV cameras to spy a naked woman in her home.[110] In another incident reported by the Guardian in 2010, an airport worker at Heathrow Airport was given a police warning for harassing a female after he allegedly took a photo of a female colleague as she went through a full body scanner at the airport.[111] Studies undertaken on how the CCTV systems in Britain are operated have also found that most of the time, male operators usually use the system to voyeuristically spy on women.[112] The researchers found that one in 10 (ten) women was targeted for entirely voyeuristic reasons in the UK.[113]

---

[107] Norris, C., McCahill, M., & Wood, D. *The Growth of CCTV: A Global Perspective on the International diffusion of video surveillance in publicly accessible space. Surveillance and Society*, (2004) 2(2), 110–135. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3369/3332 (Accessed 7/30/2022).

[108] Reported by BBC news 2002. CCTV: Does it work? Retrieved 4, 8, 2022, from: http://news.bbc.co.uk/1/hi/uk/2071496.stm.

[109] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance.

[110] BBC News, *CCTV staff spied on naked woman* (2005), Retrieved from http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4503244.stm (accessed 7/30/2022).

[111] The Guardian, Airport *Worker Given Police Warning for Misusing Body Scanner* https://www.theguardian.com/uk/2010/mar/24/airport-worker-warned-body-scanner (Accessed 7/30/2022).

[112] American Civil Liberties *Union What is Wrong with Public Video Surveillance?* (2021), https://www.aclu.org/other/whats-wrong-public-video-surveillance (Accessed 7/30/2022)

[113] American Civil Liberties Union 2022, https://www.aclu.org › other › testimony-aclus-barry-steinhardt-surveillance-system-dc-city-council. (Accessed 7/30/2022).

Another important incident that was reported in the United States revealed that the New York City police in a helicopter while monitoring the crowds at the "2004 Republican Convention trained an infrared video camera on an amorous couple enjoying the night time "privacy" of their rooftop balcony."[114]

The other problem involving video surveillance systems is the unauthorized collection and processing of data. This may result in unlawful interception of data, "especially, if the data have been collected by covert surveillance methods."[115] Special problems happen when data collected by such means are used for purposes other than motives other than public objectives. The ECHR's jurisprudence in the *Peck vs. UK* [116]provides a vivid rule in video surveillance. The facts of the case were:

> The applicant was captured on CCTV as he carried a large knife and was in the process of attempting suicide. The police were able to prevent him from causing himself fatal harm. The CCTV footage was subsequently released to the press in order to demonstrate the effectiveness of CCTV.[117]

The ECHR decided that the disclosure of the CCTV footage exceeded security observation and surpassed a degree that the applicant could have possibly imagined. "The disclosure by the Council of the relevant footage, therefore, constituted a serious interference with the applicant's right to respect for his private life."[118]

Another impact of video surveillance on the right to privacy is its "chilling effect on public life"[119] or panoptical effect. The idea is that, when people are aware of being observed or might be observed at any moment by surveillance cameras, compelled to change their behavior in public

---

[114] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance (Accessed 7/30/2022).

[115] European Commission for Democracy through Law: "opinion on video surveillance in public places by public authorities and the protection of human rights" Adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006, pp.

[116] 36 EHRR 41 (2003). https://www.google.com/search?client=safari&rls=en&q=36+EHRR+41+(2003)&ie=UTF-8&oe=UTF-8 (Accessed 7/30/22).

[117] *'Peck v UK, Id*

[118] European Commission for Democracy through Law: "opinion on video surveillance in public places by public authorities and the protection of human rights" Adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007) Study No. 404 / 2006.

[119] American Civil Liberties Union, "what's wrong with public video surveillance?" available on: https://www.aclu.org/other/whats-wrong-public-video-surveillance (2021).

places. One columnist expressed, "if we know that we are being monitored by armed government agents we tend to put a damper on things. Also, we don't want to offend them or otherwise call attention to ourselves."[120]

The widespread use and massive deployment of CCTV, therefore, is a great concern for public and seen as a threat to privacy by critics and so forth. Thus, taking into consideration the immense impact of video surveillance on the right to privacy, this is the right time to regulate the use of surveillance cameras while the system is in its infancy.

4. Video Surveillance and Privacy Rights in Ethiopia

4.1. The Current Practice and Potential Growth of Video Surveillance in Ethiopia

The cheap availability of CCTV surveillance systems[121] and the threat posed by terrorism and other security issues caused Ethiopian security forces to rely on video surveillance systems in the streets of Addis Ababa, government offices, and other public places. Currently, it is not unusual to notice security cameras installed in Bole Street, Meskel Square, hotels, malls, industrial parks, airports, offices, and even individual residential areas.

Despite the wide availability of video cameras in Ethiopia, the use of sophisticated video surveillance technology is still in its infancy, but the high interest is apparent. An Ethiopian Video Surveillance System Market report, conducted by 6Weresearch in Sep 2019 suggests that the "growing construction projects in the industrial, manufacturing, and power utility sector owing to the surge in foreign investments in the country would drive the market for video surveillance system in Ethiopia."[122] Above all, the requirement " […] for the compulsory installation of surveillance camera in public would result in a further surge in deployment of surveillance cameras in the country."[123] It is further suggested that due to increased investments in security solutions in the newly constructed manufacturing and industrial sector in the country. the Ethiopia video surveillance system market size is expected to grow during 2019-2025. Addis Ababa is a key city

[120] *Id.*
[121] The CCTV cameras are available at price starting 4000-300,000 Birr in Ethiopia (Interview with Bereket Abraha (Engineer), the Network Administrator in ECO-Engineering Plc. April 22 2021).
[122] 6Wresearch, "Ethiopia Video Surveillance System Market (2019-2025)-size, share, and trends" Available: on http/www.com6Wresearch.com/industry, (Sept. 2019).
[123] *Id.*

in Ethiopia registering maximum installation of surveillance cameras. The construction of unforeseen types of high rise buildings in financial districts including state of the art building of the Commercial Bank of Ethiopia and Maritime Transit Shipping Enterprises Headquarters, Nib Bank, Hibret Bank and so forth, supposedly planted with cameras with multiple zooming capacities.[124]Apart from this, there exists more than 115 CCTV distributors found in Addis Ababa even at this stage.[125] This also proves the potential for the faster and wider spread of the system in Ethiopia.

Now considering the ongoing reality and interest in digital surveillance in Ethiopia, it is a practical necessity to examine the power of the Ethiopian regulatory and institutional framework that is meant to address the impending issues that may possibly arise from the use of video surveillance technology and the right to privacy. As noted elsewhere above, while there are several privacy laws governing specific sectors and aspects, there is virtually no legislation that directly deals with the use of video surveillance in the context of the right to privacy. Therefore, even though the existing sector-specific privacy rules provide a limited protection against unlawful and arbitrary interference to the right to privacy, there are currently no general legally enforceable rules to limit privacy invasions through the CCTV and protect against the abuse of the system in Ethiopia. There is also no evidence whether each sector (public or private) has its own laws or practices for video surveillance in Ethiopia. The upcoming Draft Data Protection Proclamation also does not specifically address the issues of video surveillance in the context of personal data protection. But, if the draft reaches to the level of law, a regulation or directives that may be issued may address privacy issues.[126]

Thus, in such a situation, issues like what kinds of surveillance cameras we need to install and where (purpose specification); what are the rights of the "data subjects" to the surveillance process and the data collected by the system; how long the footages shall be retained remain unsolved issues in Ethiopia. In turn, though the FDRE Constitution (article 26(3) provides for limitation on

[124] 6Wresearch, *supra* note 122.
[125] CCTV Distributors in Ethiopia,
[126] Interview with Hayalneh Lemma, the Legal Service Directorate Director at Ethiopian Innovation and Technology Minster, 20 April 2021.

right to privacy, where there is no sufficiently precise rules governing limiting the right to privacy through video surveillance, any restriction on video surveillance cannot be legitimate.

In absence of a regulatory framework, law enforcement authorities or other owners of digital surveillance infrastructure may set up a centralized surveillance center where operators can view thousands of video cameras and can abuse the system for illegitimate purposes. As a result, like troubling incidents reported in various countries will most likely happen in Ethiopia too. Besides, private sectors may also use surveillance cameras not only for the sake of maintaining safety, but also to assess employees' performance. Thus, regulation of video surveillance proactively is legislative prudence.

While developing a norm about how surveillance cameras should be used in Ethiopia, it needs to establish a clear public understanding of major issues associated with video surveillance. Among the other things, the need for notification of the surveillance to the public, prohibition or restriction of workplace surveillance, retention period of footages, public access to their data, need for authorization from the regulatory body before installing CCTV system and other privacy safeguarding issues should be explicitly regulated. These issues are usually called as a processing of personal data. In other words, Data processing in practice includes the collection, use, modification, storage/retention, disclosure, and destruction of personal information.[127]

4.2.Variables that may be Considered in Building Video Surveillance Code in Ethiopia

The widespread use of video surveillance cameras in major Ethiopian cities and possible encroachment on privacy, necessary calls for an adequate regulatory framework that can address the current and potential dangers of unrestricted use of surveillance tools. The emergence of complex crimes should be tackled through a digital systems, but the law should strike a balance between the need for surveillance and the interest of privacy. Norms create regulatory framework and control methods that establish responsibility and accountability. This section summarizes international norms and best practices that the law revision can consider. Tested international experiences and norms can easily be molded in a way applicable to the Ethiopian situation.

[127] Patricia K, & Adam K, *The International Comparative Legal Guide to: Data Protection 2018*, Global Legal Group Ltd, London, (2018), p.4.

i. Necessity

Since video surveillance is one of the means to limit the right to privacy, the principle of necessity should be strictly adhered. Almost all countries that have enacted video surveillance regulatory laws have incorporated the principle of necessity into their legislations. In Canada, the system cannot be used unless there is a 'real, substantial and verifiable' problem that calls for video surveillance.[128] It can only be conducted as a last option in absence of other lesser privacy-affecting mechanisms. In the Netherlands, one of the preconditions to deploy surveillance videos in business organizations is demonstrating the necessity of the system to the Dutch Data Protection Authority.[129] The Surveillance Camera Code of Practice (2013) of the United Kingdom also clearly provides for the mandatory requirements of necessary condition/ pressing need to use surveillance cameras.[130]

ii. Pre-existing Legal Base

To protect the right to privacy in the context, there should be sufficiently clear pre-existing rules governing video surveillance. The UK Surveillance Camera Code of Practice (2013) states that, "Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them."[131] In Canada, the law imposes an obligation on the private sectors to develop a policy on the use of video surveillance before starting to conduct the surveillance.[132]

iii. Operating CCTV for a specific purpose (proportionality)

To prevent and minimize abuse of the system, "the cameras should only be used for those purposes originally identified when the decision to install them was taken".[133] The progressive expansion of function should be avoided. Therefore, while the CCTV surveillance for the purpose of preventing

---

[128] See Ontario's Freedom of Information and Protection of Privacy Act (FIPPA), section38 (2). See also Municipal Freedom of Information and Privacy Act (MFIPPA), 28(2). See the Personal Information Protection and Electronic Documents Act, 2000(PIPEDA) of Canada.

[129] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[130] See The United Surveillance Camera Code of Practice (2013), principle 1. The Data Protection Act 1998 (DPA): data protection principle 2 and 3.

[131] See *Id*, principle 2 &5. And see The Data Protection Act 1998 (DPA): data protection principle 1 &2.

[132] The Canada Personal Information Protection Act and Electronic Documents Act, 2000 (PIPEDA). And see Guidelines for video surveillance in Canada (2015).

[133] Philosopher and criminologist Andrew Von Hirsch, "CCTV and human rights" pp. 3, the last paragraph.

theft or damage to property, and protecting employees and visitors in work place is allowed, it is forbidden to use surveillance cameras to assess employee's performance under the Netherlands CCTV law.[134]

The need for a specific purpose may include limiting the types of cameras required to be deployed and their equipment to the purpose aimed to achieve. For instance, high-resolution cameras can be allowed to read a pamphlet from a mile away. Similarly, cameras are equipped to detect wavelengths outside the visible spectrum. On the same token, cameras allowing night vision/see-through vision detection can be allowed to monitor incidents that may happen in nighttime. Depending on specific needs regulators may allow cameras equipped with facial recognition, or cameras augmented with forms of artificial intelligence.[135]Unless properly regulated otherwise, such capabilities in surveillance technologies would generate incalculable breach of the right to privacy. In this regard, Canada's surveillance law requires limiting the use and viewing range of cameras as much as possible.[136]

iv. Rights of the Public

While allowing processing of personal data through video surveillance, certain rights of data subjects such as the right to consent and withdraw the same, right to know, right to access, right to deletion of personal data, and right to complain in case of interference should be specifically covered by video surveillance regulation. In other words, data collectors and processors bear obligations to respect and promote these rights while collecting and processing personal data by using surveillance cameras.

According to the data protection laws of Canada that governs the video surveillance, there should be a clear signals that warn the public regarding surveillance cameras are in use, and "mentioning the perimeter of the surveillance areas, the person responsible for surveillance and his contact

[134] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[135] American Civil Liberties Union "what is wrong with public video surveillance" (2021), Available on:https://www.aclu.org/other/whats-wrong-public-video-surveillance.

[136] Public Surveillance System Privacy Guidelines, Office of the Information and Privacy Commissioner, British Columbia, OIPC Policy 00-001, June 21, 2000.

details in case of any queries."[137] This indicates the *public's right to know* what is going on, for what reason and the data collector's obligation to conduct the surveillance transparently. The Netherlands' law also requires signaling about the ongoing surveillance with prominently placed signs and other proper means.[138] In addition, the Surveillance Camera Code of Practice (2013) of the UK, "there must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints."[139]

This principle includes the rights of the public to know and to complain in case of wrong collection and processing of their data. There must be a clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used.

Data subjects also have *a right to access to their data* recorded via surveillance cameras. In this regard, the Canada's privacy law regime provides that "the people whose images are recorded should be able to request access to their recorded personal information."[140] Another crucial right of data subjects concerning video surveillance *is the right to consent and withdraw.* Mostly the need for consideration of this right may arise in case of disclosure of personal data recorded by the surveillance cameras. Though the laws in UK, Canada, and the Netherlands declare the need for rules and restricted disclosure of personal data for clearly identified purposes, they do not specifically incorporate the right of the data subject to the consent and withdrawal at time of disclosure.

Finally, the public has the right to complain in case of any wrong act regarding video surveillance process. In this regard, the Data Protection Act 1998 of UK provided for the right to claim compensation when there is damage.[141] The laws in Canada and Netherlands do not directly refer to this right in the specific context of the video surveillance.

---

[137] Ontario's Freedom of Information and Protection of Privacy Act *supra* note 128; Municipal Freedom of Information and Privacy Act supra note 128 Personal Information Protection and Electronic Documents Act *supra* note 128.

[138] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/

[139] See The United Kingdom Surveillance Camera Code of Practice (2013), principle 3 &4. The Data Protection Act 1998 (DPA): data protection principle 6.

[140] See Ontario's Freedom of Information and Protection of Privacy Act *supra* note 128.

[141] The United Kingdom, Data Protection Act (1998).

v. Retention period

Videos collected through surveillance systems cannot be retained forever. Depending on the nature of objectives for surveillance, the retention period may vary, but there shall be a time limit. According to section 5(1) of Regulation 460 of FIPPA, and section 5 of Regulation 823 of MFIPPA, the maximum period to retain personal information is one year.[142] Further, the guidelines require the recorded images to be destroyed when they are no longer in use.[143] In some jurisdictions, the period for storing data is very short. The Netherlands, for example, unless dictated by a particular incident that requires a longer time to resolve issues that triggered surveillance, the maximum retention period for footage is four weeks.[144]

vi. Installation Place

In the context of privacy, spaces can be understood as an "open air public places", semi-private spaces, and totally/completely private spaces. Since, the degree of privacy individuals need vary, applying surveillance cameras in certain very sensitive areas like washrooms, bedrooms in guest houses, and the like should be restricted or prohibited by law. Such a semi-private spaces are highly sensitive than "open air public spaces such as public roads, parks, and squares, where individuals generally have a lower expectation of privacy."[145] As per the Netherlands law of video surveillance by private sector, cameras should be placed in places where the possibility of threats to privacy is minimal.[146]

vii. Privacy Impact Assessment

Before embarking on surveillance, its impact on privacy and possible option that could mitigate adverse effects shall be thoroughly studied. Assessment can be conducted either before or after the commencement of the surveillance. In Canada assessment of the impact of CCTV on the right to privacy is a mandatory requirement.[147] In the UK, in addition to the review of the possible effects

[142] Section 5(1) of Regulation 460 of Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) and section 5 of Regulation 823 of Municipal Freedom of Information and Privacy Act (MFIPPA).
[143] Office of the Information and Privacy Commissioner, Public Surveillance System Privacy Guidelines, British Columbia, OIPC Policy 00-001, (June 21, 2000).
[144] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/
[145] Information and Privacy Commissioner of Ontario, Guidelines for the Use of Video Surveillance (2015).
[146] *Id*.
[147] *Id*, p.18.

of surveillance, the law requires publication of the review report.[148] The Netherlands code of conduct stipulates for assessment the existence of conflict between the employers right to use surveillance cameras and the privacy rights of the employees in advance.[149] If the right to privacy overweighs the employer's right, the system should not be used. Moreover, depending upon the purpose, if surveillance takes longer period of time, it is mandatory to conduct "data protection impact assessment".[150]

The experiences and norms developed in global communities suggestibly would assistive in setting a future Ethiopian video surveillance code. Rules of collection of images and other information, use, retention, disclosure, access, security of personal information collected can be a good resource in designing a legal and institutional framework in video surveillance regulation in Ethiopia.

5. CONCLUSION

Though the meaning, nature, and contours of the right to privacy are not uniform in all jurisdictions. the right to privacy is recognized, as a human right, in international and regional human rights instruments, and in almost all constitutions of the global community. The variables for determining privacy depend upon social, cultural, economic, and religious considerations. Despite variation in grounds for delineating privacy, there are common facts in all communities – the existence of matters that cannot be exposed to everyone – private matters that need to be protected. Privacy involves respect to the expectations of private persons that certain personal facts cannot be exposed without voluntary disclosure, including but not limited to personal data, correspondences, family life, premises, and so forth against unlawful and arbitrary interference.

Legal protection of the right to privacy essentially mean guarantees provided by international instruments that shape domestic legislation serving as a model or domesticated in national laws. In some exceptional situations, the right to privacy may be limited when an express and reasonable law that is meant to strike a balance between the public interest for safety and security, and the private interest for non-disclosure of private facts and information provides to do so. The limitation should be necessary and proportional to compelling circumstances.

[148] See The United Kingdom Surveillance Camera Code of Practice (2013), 2&10.
[149] The Netherlands video surveillance regulation for private sector, available at: https://business.gov.nl/regulation/cctv-monitoring/.
[150] *Id*.

However, the development of the digital surveillance methods enables invisible intruders to violate the requirements of law. The cheap availability and the possibility to watch remotely has attracted public institutions and private persons to rely on digital surveillance technology. Despite its significance in the fight against terrorism and destructive crimes, extensive use of video surveillance is subject to abuse. Thus, unless properly regulated, the negative effect of video surveillance on the right to privacy is incalculable.

As a member of the global community, Ethiopia not only recognizes the international bill of rights but also shaped its domestic law in light of international human rights pillars, including the right to privacy. Though not comprehensive and adequate enough to accommodate the ever-expanding digital surveillance system, Ethiopia has expressly recognized the right to privacy throughout various legislations. However, the existing Ethiopian laws do not align with the ever-changing lifestyles, economy, politics, and technological advancements. Secondly, the laws do not address sufficient contents of the right to privacy and lack policy frameworks. In Ethiopia, there is no legal framework that can address the emerging digital surveillance technology. Ethiopia needs to enact a comprehensive privacy law that can proactively address potentially dangerous intrusion in private life through remotely controlled video surveillance cameras. The new law should be designed in consideration of international norms, standards, and best practices.

The work points out the need for building video surveillance codes in line with the developed nations. Factors and possible variables that may be considered in setting guidelines for video surveillance regulation are briefly pointed out.