Phone-tapping & the Right to Privacy: A Comparison of the Right to Privacy in Communication in Uganda & Canada

R. Kakungulu-Mayambala*

Email: kakungul@interchange.ubc.ca

Table of Contents

List of Acronyms.............................................................................................................2
Abstract .........................................................................................................................2
Key Definitions .............................................................................................................3
I. Introduction..................................................................................................................4
II. Historical and Legal Conceptions of the Right to Privacy in Uganda.................5
   2.1 History of Phone tapping and Surveillance in Uganda.................................5
III Elemental aspects of the right to privacy in communication in Uganda 1995 - 2008.........................................................................................................................7
   3.1 The Rationale for the right to privacy in communication.................................7
   3.2 Enjoyment of the right to privacy in Uganda for the period 1995 – 2008....9
IV. The Right to Privacy in Communication in Canada and lessons for Uganda....17
   4.1. The Experiences with and approaches to the Right to Privacy in Communication in Canada ...............................................................17
   4.2. The Right to Privacy in Communication in Canada and Lessons for Uganda ..........................................................................................19
V. Conclusion ..................................................................................................................22
References.....................................................................................................................22

* LL.M. (with Distinction) Lund; LL.B. (Hons.) Mak; Dip. LP. (LDC); Advocate High Court of Uganda & East Africa.
**List of Acronyms**

ACHPR – African Charter on Human and Peoples’ Rights  
E.C – European Commission  
E.U – European Union  
FDC – Forum for Democratic Change  
ICCPR – International Covenant on Civil and Political Rights  
IMF – International Monetary Fund  
UDHR – Universal Declaration of Human Rights  
UHRC – Uganda Human Rights Commission  
UN – United Nations  
UPDF – Uganda Peoples’ Defence Forces  
U.S.A. – United States of America  
WIPO – World Intellectual Property Organisation  
WTO – World Trade Organisation

**Abstract**

This paper seeks to examine the extent to which the right to privacy in communication is being realized within the context of the operations of the national security, surveillance and defence organs/agencies of the Republic of Uganda. It is especially concerned to provide the legal, historical and practical framework within which it is necessary to understand the right, and makes an effort to examine how the Canadian and Ugandan conceptions of privacy interests differ from one another and how these conceptions affect the practical articulation of rights.

Any State organ that purports to keep and maintain national security in Uganda must adhere to certain minimum international and constitutional standards of maintaining peace and security. In particular, such organs are obligated to protect and uphold the fundamental right to privacy. The right to privacy is multifaceted and very broad in nature. It includes the right not to be subjected to unlawful search of the person, home or other property of that person, unlawful entry by others of the premises of that person, and the prohibition on the interference with the privacy of a person’s home, correspondence, communication or other property. In their totality, these rights constitute the minimum standards for administering the right to privacy in a free and democratic society of which Uganda is aspiring to be.

The fight against terrorism and armed rebellion in Uganda has sparked off a wave of public concern over the involvement of security organs/agencies in the interception and conducting of surveillance on people’s correspondence and communication in the guise of maintaining peace and security in the country. It has also presented an opportunity for the re-examination of the role of security
organs/intelligence agencies in the observance and enjoyment of the right to privacy in Uganda. The paper shall examine the privacy interests in Uganda alongside the Canadian treatment of the same right.

Key Definitions

"Intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;¹

"Privacy" means the right of a person to keep his or her matters and relationships secret;²

"Proprietary information" means information relating to any manufacturing process, trade secret, trademark, copyright, patent or formula protected by law or by International Treaty to which Uganda is a party;³

"Public body" includes a government, ministry, department, statutory corporation, authority or commission;⁴

"Record" means any recorded information, in any format, including an electronic format in the possession or control of a public body, whether or not that body created it;⁵

"Relevant authority" means the Minister responsible for that public body or the person designated in writing by that Minister;⁶

"Request for access" means a request for access to a record of a public body under this section;⁷

"Security" means the protection of Uganda against threats such as crime, criminals and attacks by foreign countries;⁸

"Sovereignty" means the supremacy of the State;⁹

"Telephone tapping" is the monitoring of telephone and Internet conversations by a third party, often by covert means entailing the act of electronically intercepting conversations without the knowledge or consent of at least one of the participants.¹⁰

¹ Canada Criminal Code.
² Section 4 of the Access to Information Act of Uganda.
³ Ibid.
⁴ Ibid.
⁵ Ibid.
⁶ Ibid.
⁷ Ibid.
⁸ Ibid.
⁹ Ibid.
¹⁰ Wikipedia, the Free Encyclopedia.
I. Introduction

Uganda's 1995 Constitution provides for the right to privacy in its Article 27, as a reasonable guide to what constitutes the right to privacy in correspondence and communication, and only stipulates it as a right without more. However, the United Nations (UN) and International Human Rights Instruments have interpreted the right to privacy in correspondence and communication based on the circumstances and complexities of the case (especially in the fight against terrorism and maintenance of national security) and the conduct of all parties, thereby providing a more elaborated framework within which consideration of the right should be undertaken.\(^{11}\)

The Constitution and Other laws in Uganda place limits to the enjoyment of rights including the right to privacy as clearly seen in the Access to Information Act, Act No.6 of 2005 and the Anti-Terrorism Act, Act No.14 of 2002 which actually provides for the interception of communication and surveillance of any person suspected of engaging in terrorism activities. The Constitution also obliges security organizations including all intelligence services to observe human rights under Article 221.\(^{12}\)

The predicament of infringement of the right to privacy by security organizations/intelligence services in Uganda has grown and is caused by several factors, including complaints received by the Uganda Human Rights Commission (UHRC) on alleged interference with the correspondence and communication of especially members of the Opposition in Uganda, the lack of a culture of human rights observance on the side of security organizations in Uganda, including the existence of loopholes in the enabling law.

Though the right to privacy in correspondence and communication did not pose a major challenge in Uganda two decades ago, new developments in *science and technology* continue to pose new challenges to human rights, in particular the right to human dignity and privacy. In the fight against organized crime and terrorism, modern police and intelligence agencies are using information and *surveillance technology*, including phone tapping, that potentially affects numerous innocent citizens and constitutes far-reaching interference with the right to privacy and data protection.\(^{13}\)

---


\(^{12}\) Unlike in Canada where there is a strict adherence to proper identification and registration before one can be connected to a service phone provider be it mobile or fixed line, Uganda telephony service providers do not enforce the identification requirement, which has in turn led to increased telephone crime due to the cheap telephony in which a Sim Card costs as low as CAD $1. *See, The New Vision, Friday, 14th March, 2008.*

The legal challenges posed by technological change and by increased State involvement in the private lives of citizens necessitate the constant, dynamic development of new measures of protection within established State obligations and a wide application of the principle of privacy.\textsuperscript{14} Ample evidence of this is provided in the media reports and complaints at the UHRC relating to interception of communication and surveillance. One may, however, question whether the limits of Article 27, even within the Constitution and other laws relating to national security, can, in the long run, satisfy the actual needs. Further, elaboration of the principles of the right to privacy enshrined in Article 27 of the Constitution and Uganda's obligations in international human rights law must be given priority.\textsuperscript{15}

**II. Historical and Legal Conceptions of the Right to Privacy in Uganda.**

This part of the paper concerns itself with the historical evolution and legal conceptions of the right to privacy in Uganda. In discussing the history relating to the right to privacy in Uganda, this part of the paper shall be core to forming the basis upon which the right to privacy in communication can best be understood in the Ugandan context.

---

**2.1 History of Phone tapping and Surveillance in Uganda**

Though slightly new in Uganda, communication interception and surveillance of which phone tapping is just an example has been around for more than a century. It was born during the Presidency of President Abraham Lincoln of the United States of America.\textsuperscript{16} Communication interception can be traced back to the period of the American Civil War where eavesdropping of telegraph (telegraphy system invented in 1844) conversations was the first recorded.\textsuperscript{17} Though not clear as to when the telephone was first used, the telephone was first invented in 1876 and it is believed that telephone tapping is as old as the telephone itself at least in the developed world. According to Kaduuli, telephone wiretapping began in the 1890s, following the invention of the telephone recorder. Kaduuli further bases his timing on phone tapping to *The Einstein File* by Fred Jerome, arguing that from the time Einstein arrived in the United States in 1933 to the time of his death in 1955, the FBI files reveal that his phone was tapped, his mail was opened and even his garbage searched.\textsuperscript{18}

---

\begin{itemize}
\item[18] *Ibid.*
\end{itemize}
Though there may be disagreements between Kaduuli and Jerome as to the exact dates when phone tapping may have started, it is clear that phone tapping has been around for at least more than half a century. The right to privacy in communication is not new in Uganda. It was equally provided for in the Bill of Rights of the 1962 and 1967 Constitutions. Uganda’s 1995 Constitution provides for the right to privacy in its Articles 27, as a reasonable guide to what constitutes the right to privacy in correspondence and communications, and only stipulates it as a right without more. What is new however is phone tapping which is an infringement of the right to privacy in communication. Though the right to privacy in communication did not pose a major challenge in Uganda two decades ago, new developments in science and technology continue to pose new challenges to human rights, in particular the right to human dignity and privacy.\textsuperscript{19} In the fight against organized crime and terrorism, modern police and intelligence agencies are using information and surveillance technology, including phone tapping, that potentially affects numerous innocent citizens and constitutes far-reaching interference with the right to privacy.\textsuperscript{20} Lt. Gen. David Tinefuza was possibly the first high profile government official to complain about phone tapping after his failed bid to resign from the army in 1997.\textsuperscript{21} In 2003, the Member of Parliament for Lira Municipality, Ms. Cecilia Ogwal, was up in arms with the government and President Yoweri Museveni in particular for allegedly tapping her mobile phone conversations. This was after the latter told Parliament on September 8, 2003, that he had listened in on a conversation between Ogwal and a rebel commander of the Lord’s Resistance Army.\textsuperscript{22} The media was however awe with the opposition politicians accusing the state intelligence operatives and agencies of phone tapping at the height of the 2001 Presidential and Parliamentary Campaigns.\textsuperscript{23}

The Constitution and other laws in Uganda place limits on the enjoyment of rights including the right to privacy as clearly seen in the Access to Information Act,\textsuperscript{24} and the Anti-Terrorism Act,\textsuperscript{25} which actually provides for the interception of communication and surveillance of any person suspected of engaging in terrorism activities. The Constitution also obliges security organizations including the intelligence services to observe human rights under Article 221. Though the law in Uganda provides for phone tapping, the same does not provide for the procedure to be followed in this exercise. Thus, the government recently proposed the

\begin{flushright}
\textsuperscript{19} Nowak, M., \textit{Introduction to the International Human Rights Regime}, 2003, Nijhoof, Leiden.
\textsuperscript{20} \textit{Ibid.}\textsuperscript{21} The Monitor Newspaper, October 1, 2003.
\textsuperscript{22} The Monitor Newspaper, October 4, 2003.
\textsuperscript{23} See Complaint lodged by Col (rtd) Dr. Kizza-Besigye at the Uganda Human Rights Commission (UHRC) on alleged phone tapping by the State during the 2001 Presidential and Parliamentary campaigns in which he contested as the Reform Agenda (RA) Presidential Candidate.
\textsuperscript{24} Act No. 6 of 2005.
\textsuperscript{25} Act No. 14 of 2002.
\end{flushright}
Regulation of Interception of Communication Bill 2007 which was presented by the Security Minister Hon. Amama Mbabazi to the ruling/NRM party meeting where government was canvassing MPs to ensue the bill sails through Parliament.\(^\text{26}\) President Yoweri Museveni, who was in attendance, said that the bill was intended to monitor communication between suspected terrorists.\(^\text{27}\) The opposition and members of the public have already vehemently condemned the proposed bill.\(^\text{28}\)

The debate is basically about the right to privacy vis-à-vis security of person and the state. All commentators are aware that Government has for some time been tapping phones albeit illegally in Uganda. The main battle field between those opposed to the bill and those pushing for it is whether there should be no law at all to regulate phone tapping or there should be watertight safeguards in the law to ensure that the citizens’ rights are not trampled upon. Whatever reasons the two opposing sides may have for either supporting or opposing the bill, what remains clear is that the state has been tapping phones without any regulation/illegally and will continue to do so whether the bill is passed or not!

### III Elemental aspects of the right to privacy in communication in Uganda 1995 -2008

This chapter deals with the elemental aspects of the right to privacy in communication in Uganda for the period 1995-2008. The Chapter will essentially discuss the rationale for the right to privacy in communication, the enjoyment of the right to privacy in communication in Uganda for the periods 1995-2008. The chapter also addresses the major impediments to the enjoyment of the right to privacy in communication in Uganda and how national security and intelligence agencies engaged in the fight against terrorism and organised crime can be helped to develop a culture of human rights observance in the execution of their duties.

#### 3.1 The Rationale for the right to privacy in communication

The rationale for the right to privacy in communication is to secure the individual against arbitrary interference by the public authorities in his private and family life. This notwithstanding, one of the most contentious issues of our times relates to the protection of the right to privacy in communication in the era of terrorism and

---

\(^{26}\) The Regulation of Interception of Communication Bill is currently being considered by the Uganda Parliamentary Committee on Information and Communication Technology (ICT), and has been approved by the majority Members of Parliament of the ruling National Resistance Movement Government of President Yoweri Kaguta Museveni which means that phone tapping has in effect been legalized in Uganda. See The New Vision, April 7, 2008, and The Daily Monitor, April 10, 2008. See the websites at [http://www.newvision.co.ug](http://www.newvision.co.ug) and [http://www.monitor.co.ug](http://www.monitor.co.ug)


\(^{28}\) See Mollynn G Mugisha, 'Do not support phone tapping’ letter in the Daily Monitor, June 4, 2007, at p.11.
organised crime. The raise in organised crime and terrorism is a big challenge to the right to privacy in communication. Owing to the core relevance of the right to privacy in communication, this right has been made subject of the ‘principle of legality’ in other jurisdictions requiring that actions by public authorities which infringe significantly on the rights and freedoms of private citizens (eg police surveillance), be authorised by Statute/law. The ambitious expansion of electronic surveillance and its implications on are enormous. What used to be the rationale for the protection of the right to privacy in communication is now being looked at in relation to national security and the fight against terrorism. New developments in the area of national security and terrorism have set the stage for discussion on what should be the appropriate limits of national security and anti-terrorism.

Though the concept of privacy in communication figures prominently in the discourse about the social and political threats posed by modern information and communication technology, the rational for privacy in communication can basically be found in terms of information control. Privacy is mainly regarded as being of value to individual persons and of societal benefits. Most discourse on privacy and privacy rights tends to focus only on the benefits these rights have for individuals. These benefits are typically cast in terms of securing (or helping to secure) individuality, autonomy, dignity, emotional release, self-evaluation, and interpersonal relationships of love, friendship and trust. They are, in the words of Westin, largely about “achieving individual goals of self-realisation”. The converse side of this focus is that privacy in communication rights are often seen as essentially in tension with the needs of the wider “society”. This is more so the case when it comes to the balancing of the rights to privacy in communication and national security or the fight against terrorism. This view observers comment carries sometimes over into the claims that privacy rights can be detrimental to societal needs.

---

30 See for example Norway’s Personal Data Act of 2000 and the Personal Data Registers Act of 1978.
31 See for example Norway’s Personal Data Act of 2000 and the Personal Data Registers Act of 1978.
As Professor Lee Bygrave observes:

‘Casting the value of privacy in strictly individualistic terms appears to be a common trait in the equivalent discourse in many other countries. Indeed, it is an integral feature of what Bennett and Raab term the “privacy paradigm” – a set of liberal assumptions informing the development of data privacy policy in the bulk of advanced industrial states.”

This notwithstanding, the grip of that paradigm varies from country to country and culture to culture. For example, whereas the Canadian courts emphasise the value on the individual right to privacy in communication, the Ugandan courts are yet to be faced with such challenges of having to deal with evidence illegally obtained through wire tapping. The law on privacy in communication seeks to protect human identity, the rights of man, privacy, individual and public liberties. These virtues are core to any free and democratic society. Concern for privacy tends to be high in societies espousing liberal ideals, particularly those within the Western liberal democratic “camp” Canada inclusive compared to the less liberal and undemocratic societies like Uganda and other African states. As Lukes notes, privacy is in the sense of a “sphere of thought and action that should be free from ‘public’ interference” constitutes “perhaps the central idea of liberalism”. The liberal affection for privacy is amply demonstrated in the development of comprehensive legal regimes for privacy protection in Western liberal democracies. By contrast, such regimes are under-developed in most African nations Uganda inclusive. It is tempting to view this situation as symptomatic of a propensity in Ugandan and African cultures to place primary value on securing the interests and loyalties of the group at the expense of the individual.

3.2 Enjoyment of the right to privacy in Uganda for the period 1995 – 2008

37 The Uganda Evidence Act, Cap.6, Laws of Uganda, does not expressly deal with evidence acquired illegally say through a wire tap but courts in Uganda follow the long established common law doctrine of illegality in which case any evidence acquired illegally (including unauthorized wire taps) would as a general rule be inadmissible in evidence before any court of Law in Uganda. This would not be the case in Canada owing to s.24 (2) of the Charter which outlawed the automatic exclusion rule of such evidence in Canada.
The notion of fundamental rights and freedoms has existed from the very outset of the birth of the modern constitutional state of Uganda in 1962. Thus, prior to the 1995 Constitution, the conceptualisation of fundamental freedoms and rights was manifested in the provisions of Chapters II and III of the 1962 and 1967 Constitutions respectively. Further, the predecessor constitutions provided for mechanisms for the enforcement of rights and freedoms, in particular through the courts. Evidently, a cursory glance at both constitutions does reveal emphasis on traditional civil and political rights, while the 1995 Constitution has since incorporated a range of new categories of rights and freedoms, particularly socio-economic and cultural rights and specific group-based rights (in respect of, for instance, women, children, persons with disabilities, and minorities).

Notwithstanding the provisions on human rights under both the 1962 and 1967 Constitutions, the human rights situation in Uganda was largely dismal, as the period from 1962 to 1995 was characterised by abuses in the form of arbitrary arrests, preventive detention, torture, disappearances. The political situation militated against the meaningful enjoyment of rights.41

The protection and enforcement/enjoyment of the right to privacy in communication in Uganda (1995-2008) as provided for in article 27 of the Constitution has now been tested for thirteen years since the Constitution came into operation.

Lt. Gen. David Tinyefuza was possibly the first high profile government official to complain about phone tapping after his failed bid to resign from the army in 1997.42 In 2003, the Member of Parliament for Lira Municipality, Ms. Cecilia Ogwal, was up in arms with the government and President Yoweri Museveni in particular for allegedly tapping her mobile phone conversations. This was after the latter told Parliament on September 8, 2003, that he had listened in on a conversation between Ogwal and a rebel commander of the Lord’s Resistance Army.43 The media was however awe with the opposition politicians accusing the state intelligence operatives and agencies of phone tapping at the height of the 2001 Presidential and Parliamentary Campaigns.44

The Constitution and other laws in Uganda place limits on the enjoyment of rights including the right to privacy as clearly seen in the Access to Information Act,45

42 The Monitor Newspaper, October 1, 2003.
44 See Complaint lodged by Col (rtd) Dr. Kizza-Besigye at the Uganda Human Rights Commission (UHRC) on alleged phone tapping by the State during the 2001 Presidential and Parliamentary campaigns in which he contested as the Reform Agenda (RA) Presidential Candidate.
45 Act No. 6 of 2005.
and the Anti-Terrorism Act,\textsuperscript{46} which actually provides for the interception of communication and surveillance of any person suspected of engaging in terrorism activities. The Constitution also obliges security organizations including the intelligence services to observe human rights under Article 221. Though the law in Uganda provides for phone tapping, the same does not provide for the procedure to be followed in this exercise. Thus, the government recently proposed the Regulation of Interception of Communication Bill 2007 which was presented by the Security Minister Hon. Amama Mbabazi to the ruling/NRM party meeting where government was canvassing MPs to ensure the bill sails through Parliament. President Yoweri Museveni, who was in attendance, said that the bill was intended to monitor communication between suspected terrorists.\textsuperscript{47} The opposition and members of the public have already vehemently condemned the proposed bill.\textsuperscript{48}

However, a close look at the enjoyment of this right as espoused in the article in the last twelve years has had some problems. The problems that have hindered the enjoyment of this right have been multifarious as discussed hereunder.

\textbf{3.3 Major impediments to the enjoyment of the right to privacy in Uganda 1995-2008}

Though the right to privacy in communication did not pose a major challenge in Uganda two decades ago, new developments in \textit{science and technology} continue to pose new challenges to human rights, in particular the right to human dignity and privacy. In the fight against organized crime and terrorism, modern police and intelligence agencies are using information and surveillance technology, including phone tapping, that potentially affects numerous innocent citizens and constitutes far-reaching interference with the right to privacy and data protection.

In a bid to maintain national security and counter terrorism, the Uganda government has passed legislation which has had drastic effects on the enjoyment of the right to privacy in communication. A case in issue is the Anti-Terrorism Act. S.18 of this Act is the most relevant. It provides thus:

18. (1) The Minister may, by writing, designate a security officer and an authorized officer under this part.
(2) An order issued by the Minister in respect of an authorized officer shall have the right to intercept the communications of a person and otherwise conduct surveillance of a person under this Act.

\textsuperscript{46} Act No. 14 of 2002.
\textsuperscript{48} See Mollynn G Mugisha, 'Do not support phone tapping' letter in the Daily Monitor, June 4, 2007, at p.11.
19. (1) Subject to this Act, an authorized officer shall have the right to intercept the communications of a person and otherwise conduct surveillance of a person under this Act.
(2) The powers of an authorized officer shall be exercised in respect of a person or a group or category of persons suspected of committing any offence under this Act.
(3) The functions of an authorized officer shall be exercised only in respect of the person or group or category of persons described in the order.
(4) The purposes for which interception or surveillance may be conducted under this part are----
(a) safeguarding the public interest;
(b) prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism;
(c) preventing or detecting the commission of any offence under this Act; or
(d) safeguarding the national economy from terrorism.
(5) The scope of the interception and surveillance allowed under this Part is limited to----
(b) interception of the telephone calls, faxes, emails and other communications made or issued by or received by or addressed to a person;
(g) searching of the premises of any person.
(6) For the avoidance of doubt, power given to an authorized officer under subsection (5) includes----
(a) the right to detain and make copies of any matter intercepted by the authorized officer;
(b) the right to take photographs of the person being surveilled and any other person in the company of that person, whether at a meeting or otherwise; and
(c) the power to do any other thing reasonably necessary for the purposes of this subsection.

(20) Any person who knowingly obstructs an authorized officer in the carrying out of his or her functions under this part commits an offence and is liable, on conviction, to imprisonment not exceeding two years or a fine not exceeding one hundred currency points, or both.

(21) Any authorized officer who—
(a) demands or accepts any money or other benefits in consideration of his or her refraining from carrying out his or her functions under this Part; or
(b) demands any money or other benefit from any person under threat to carry out any of his or her functions under this Part;
(c) fails without reasonable excuse or neglects to carry out the requirements of the order;
(d) recklessly releases information which may prejudice the investigation;
(e) engages in torture, inhuman and degrading treatment, illegal detention or intentionally causes harm or loss to property, commits an offence and is liable, on conviction, to imprisonment not exceeding five years or a fine not exceeding two hundred and fifty currency points, or both.

(22) Any recording, document, photograph or other matter obtained in the exercise of the functions of an authorized officer under this Part is admissible in evidence in any proceedings for an offence under this Act.

For a long time since the Anti-Terrorism Act came into force in 2002, the government has not passed any Regulations to regularize/operationalise phone-tapping or interception of communication of suspected terrorists. This comes at the backdrop of allegations that the absence of a law operationalising phone-tapping not withstanding, the government has nevertheless intercepted communication and done surveillance on suspected terrorists. It is upon this background that the government has proposed the Regulation of Interception of Communication Bill 2007 which seeks to make provision for lawful interception and monitoring of certain communications in the course of their transmission through telecommunication, postal or any other related services or system in Uganda.

As MP Reagan Okumu said:

“The Government is now moving towards legalizing what they have been doing. Security organs have been tapping people’s phones especially for those of us who are in the opposition. Is there anything new? My only worry is that the system may turn out to be expensive,”

---

49 This assertion was affirmed by Col. (rtd) Dr. Kiiza-Besigye [Party President, FDC] in the interview done on 28th January, 2008.
50 Interview with Hon. Rose Namayanja [Chairperson, National Defence Parliamentary Committee] done on 1st February, 2008, affirmed the fact that the Bill would make it possible for the government to now use in court evidence against wrong elements suspected of terrorism obtained through surveillance including phone-tapping.
The Bill is intended to suppress terrorism in Uganda. The Bill would also reinforce the provisions of the Interception of Communications and Surveillance of the Anti-Terrorism Act 2002, whose main focus is suppression of terrorism.

The Bill states that people authorized to apply for warrant of Interception of Communication will be chief of defence forces, director of ESO and ISO, Inspector General of Police and the Commissioner General of Prisons. According to Government the purpose of the Bill is to put a law in place authorizing who can tap phones, now that it is done haphazardly. Another reason for the Bill according to its major sponsors is to intercept terrorists’ communication with bad motives and those bad elements who deal in trafficking arms. At this stage, the sword is now drawn between the sponsors of the Bill and those opposed to it with the predominant view being whether to tap illegally or to tap with judicial review? The general consensus is that the government should not interfere in the civil liberties of its citizens. However, since the government is bent on infringing the citizens’ right to privacy and has also been tapping phones illegally, there is now a shifting paradigm: that tapping phones should be used for the common good of any society and not for selfish motives and that there should be watertight safeguards in the law to ensure that the citizens’ right are not trampled upon.

As MP Guma Gumisirisa rightly observed:

“It is not bad but such a law should put into consideration people’s right to privacy and secrecy. The idea of tapping people’s phones cannot be accepted,”

Article 27 of that the Constitution provides for the right to privacy. It states

“(1) No person shall be subjected to----
   unlawful search of the person, home or other property of that person; or
   unlawful entry by others of the premises of that person.

(2) No person shall be subjected to interference with the privacy of that person’s home, correspondence, communication or other property.

Sections 18 and 19 of the Anti-Terrorism Act run counter to Article 27 (2) of the Constitution. The said sections completely negate Article 27 and almost render it inoperative.

---

52 See Section 12 of the Proposed Bill.
Article 43 of the Constitution places general limitations on fundamental and other human rights and freedoms. This article permits any limitation of the enjoyment of the rights and freedoms prescribed by the bill of rights in the Constitution as long as it is not beyond what is acceptable and demonstrably justifiable in a free and democratic society, or what is provided in the Constitution. Another article in the Constitution which touches on this concept is 41 on the right of access to information in the possession of the State (or its organs and agencies). The article provides thus:

“(1) Every citizen has a right of access to information in the possession of the State or any other organ or agency of the State except where the release of the information is likely to prejudice the security or sovereignty of the State or interfere with the right to privacy of any other person. 54

(2) Parliament shall make laws prescribing the clauses of information referred to in clause (1) of this article and the procedure for claiming access to that information.” 55

Unlike Sections 18 and 19 of the Anti-Terrorism Act and Article 27 (2) of the Constitution which have not been tested in court yet, Article 41 of the Constitution has been tested in court in several cases bringing out interesting revelations about the scope and breadth of the article by the courts of law. In the Cases of Major General David Tinyefuza v. Attorney General56 and Attorney General v. Major General David Tinyefuza57 both the Constitutional Court58 and the Supreme Court59 remarked that it is not enough for the State to merely assert that the release of information would cause prejudice to those interest – to that end, the State had to avail evidence to that effect and, therefore, the burden of proof lay with the State to show that the information that is being sought was restricted. More significantly, the import of the exceptions in article 41 of the Constitution was considered, with Mulenga, JSC of the view that those exceptions pertain to the effect of the release of information rather than to categories of information:

“The exception under article 41 is not directed to types or categories of information... It is rather concerned with the effect of release of the information. The citizen is entitled to access any type of information, whether related to national security or national

54 See e.g., Section 32 of the Access to Information Act No. 6 of 2005.
55 Parliament in 2005 passed the Access to Information Act No. 6 of 2005. Section 5 of this Act is a replica of Article 41 of the Constitution.
56 Constitutional Petition No. 1 of 1997 (CC) (unreported) (hereinafter Tinyefuza 1 case).
58 Tinyefuza 1 case, supra, at p.13.
59 Tinyefuza 11 case, supra, judgments of Wambuzi, CJ, at p.30; Oder, JSC, at p. 38; Mulenga, JSC, at p. 30 and Mukasa-Kikonyogo, JSC, at p. 18.
economy, as long as its release is not likely to prejudice the security or sovereignty (or interfere with the right to privacy of any other person).\footnote{Ibid, judgment of Mulenga, JSC, at p. 31.}

As a consequence, right of access should exist with regards to information of whatever kind unless the State (or its organs or agencies) can show that it falls within the scope of the limited regime of exceptions (in terms of the effect upon security or sovereignty of the State or individual privacy).\footnote{Onoria, H.M., Realization and Enforcement of the Right of Access to Information in Uganda, 1995-2005, Makerere Law Journal, 2004-5, pp. 39-58, at p.44.} Reflecting on the decision of the lower court on the issue of the release of the information in a 'limited context', the Supreme Court was agreed that the release of information in a 'limited context' has been proper in balancing the need to determine rights of the individual (the petitioner) as against any perceived prejudice to the security of the State that the release of the information to the public would occasion. Oder, JSC observed thus:

... [I]t appears the mischief feared is in the release of information to the citizen, probably with the consequence that such information might be made public, prejudicing the security of the State. If the release was of a \textit{limited context}, namely if it was denied to the public and the press but made available to the court and the parties for the determination of issues between the State and such party, then the prejudice to the security of the State would be averted by exclusion of the public and press and hearing in camera, as authorized by article 28(2) of the Constitution.\footnote{Tinyefuza 11 case, supra, judgment of Oder, JSC, at p. 38, see also judgments of Tsekooko, JSC, at p. 24; Karokora, JSC, at p. 14.}

To the contention by the government in the case of \textit{Dr. Paul Ssemwogerere & Another v. Attorney General}\footnote{Constitutional Petition No. 6 of 1999 (CC) (unreported).}, that article 41 of the Constitution only guaranteed access but not use of information, Okello, JA observed that 'access to information without use of it would be empty', and was of the view that 'access and use go together'.

Just as the individual can seek for information from government in the same way government can seek for information from an individual in public interest and for the security of the country.\footnote{Section 32 of the Access to Information Act, permits a mandatory disclosure in public interest of any information.} This leaves one wondering whether the State may derogate from its role of ensuring that ever citizen enjoys the right to privacy.
From the foregoing, it can be noted that the passing of the Anti-Terrorism Act, has greatly impacted on the enjoyment of the right to privacy in communication in Uganda. The Act provides for interception of communication of any one suspected of engaging in terrorist activities. Equally, the fight against terrorism and organized crime in Uganda coupled with the lack of government will to uphold the rights of its people, has negatively affected the enjoyment of the right to privacy in Uganda as discussed above.

IV. The Right to Privacy in Communication in Canada and lessons for Uganda

This part of the paper addresses the experiences with and approaches to the right to privacy in communication in Canada and its attendant lessons for Uganda. In this part, an analysis of how the Canadian and Ugandan conceptions of privacy interests differ from one another; and how these conceptions affect the practical articulation of the right to privacy in communication shall be discussed.

4.1. The Experiences with and approaches to the Right to Privacy in Communication in Canada

Not only is the problem of national security and the fight against terrorism and organised crime a threat to the right to privacy in communication in Least Developed Countries (LDCs) like Uganda but also other jurisdictions including Canada.

However, unlike in Uganda, Canada being a developed democratic country, wire tapping is strictly controlled to safeguard individuals’ privacy.

The Canadian Charter of Rights and Freedoms guarantees the right to privacy in s.8 which states that:

“Everyone has the right to be secure against unreasonable search or seizure.”

Similarly, s.24 (2) of the Charter conditions the admissibility of the evidence in any criminal matter on the very different consideration as to whether its admission “would bring the administration of justice into disrupt”.

Thus, the Charter guarantees the right “to be secure against unreasonable search or seizure”. American cases dealing with the similar right protected by the Fourth

---

Amendment have held that intangible conversation can be the subject of search and seizure.\textsuperscript{66}

Though the Ugandan Bill of Rights as seen in Art.27 of the Constitution is very explicit on the right to privacy in communication, the Canadian Charter of Rights and Freedoms only talks of an infringement of the protected right against unreasonable seizure. However, based on s.8 of the Canadian Charter, it is possible that the criminal interception of a private communication would be regarded as an infringement of the protected right against unreasonable seizure. It seems thus that the right to privacy in communication is an implicit right as opposed to the explicit nature the right takes in Uganda.

Accordingly, s.184.4, which purports to admit such illegally, obtained evidence on the basis of consent would presumably have to yield to s.24(2) of the Charter which conditions admissibility of the evidence on the very different consideration as on whether its admission “would bring the administration of justice into disrepute”. Interception of communication is only in exceptional circumstances otherwise it is prohibited.

S.184.4 A peace officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where

\begin{itemize}
\item [a] the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;
\item [b] the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and
\item [c] either the originator of the private communication or the person intended by the originator to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.\textsuperscript{[1993, c.40, s.4.]}\end{itemize}

S.184.5 permits a judicial review of the process of interception of private communication here in Canada. Such an application may be made ex parte to a judicial officer, a judge of a superior jurisdiction in criminal proceedings. However, this Canadian position is radically different from the position advocated for in the Regulation of Interception of Communication Bill in Uganda which empowers the Security Minister to intercept communication upon request from the Chief of Defence Forces, the Inspector General of Police and the Director of Internal Security if terrorism, serious crimes such as robber, or a threat to the State is

suspected. It is thus possible to see that the abuse to the right to privacy in Uganda does not have a judicial review like is the case here in Canada but shall be at the whelm of the Security Minister. The Bill is welcome in so far as it seeks to provide for a law regulating the interception of private communication, and for the Government of Uganda to regulate interception of private communication, for the people of Uganda to know who can lawfully intercept their private communication, for what purpose, and who issues warrants to do so. In Uganda, once again, in the Bill, the bizarre thing is that the warrants are to be signed by the Minister for Security. The Bill seeks to make a provision for lawful interception and monitoring of certain communications in the course of their transmission through telecommunication, postal or any other related service or system in Uganda.

Owing to the fact the Bill on the Regulation of Interception of Communications in Uganda gives too much power to the Minister of Security, human rights activists have criticized the Regulations saying that the Bill will be used to target people with dissenting views from those of the Government.

It is also apparently clear that the proposed law to legalize phone tapping in Uganda infringes on people’s rights to privacy and freedom of expression.

S.186 of the Canadian Criminal Code (CCC), states that a judicial official must be satisfied before authorizing a wire tap and any wire tap done without authorization is null and void and such evidence shall not be admissible in Court. Any one who wants to wire tap including the government or security agencies in Canada must apply for authorization under s.185 of the CCC.

4.2. The Right to Privacy in Communication in Canada and Lessons for Uganda

The jurisprudence right to privacy in communication is more developed in Canada than in Uganda. Canada is a leading example in this area of safeguarding citizens’ rights on the wire tap with several safeguards including judicial review.

The variation between the privacy regimes of Canada and Uganda can also be symptomatic of differences in perceptions of the degree to which interests that compete with privacy, such as public safety and national security, warrant protection at the expense of privacy interests. In other words, it can be symptomatic of differing perceptions of the need for surveillance and control

68 Sewanyana, L., Executive Director, Foundation for Human Rights Initiative, delivering a paper on the Proposed Regulation of Interception of Communications Bill to Law Students at Kampala International University, Friday, April 18th, 2008.
measures.\textsuperscript{71} This is seen most clearly in the impact on U.S. regulatory policy of the terrorist attacks of 11\textsuperscript{th} September 2001. In the wake of those attacks, the U.S. has been more prepared than many other countries to curb domestic civil liberties, including privacy rights.\textsuperscript{72} This very attitude led to the hurried passing of the Anti-Terrorism Act in 2002 in Uganda as a result of the twin bombings of the cities of Nairobi and Tanzania by alleged terrorists targeting the American embassies there. There were also widespread reports of bomb blasts in Kampala. The proposed law on phone tapping is inimical to the enjoyment of the right to privacy in correspondence and communication in Uganda.\textsuperscript{73}

Despite the fact that both Uganda and Canada are members of the United Nations and several fundamental human rights multilateral instruments like the Universal Declaration of Human Rights (U.D.H.R.), the International Covenant on Civil and Political Rights (I.C.C.P.R.), from which the formal normative basis for privacy and protection laws derives, most Uganda has failed to adhere to a strict observance of the right to privacy in communication and also requiring the strict national implementation of the basic principles of privacy in communication laws.\textsuperscript{74} This is the case in Uganda despite the Constitutional provision in Art 221 which states:

"It shall be the duty of the Uganda Peoples’ Defence Forces and any other armed force established in Uganda, the Uganda Police Force and any other police force, the Uganda Prisons Service, all intelligence services and the National Security Council to observe and respect human rights and freedoms in the performance of their functions".

The intelligence agencies continue to tap peoples phones articles 27 and 221 notwithstanding.

Across the Atlantic, Canada offers very good jurisprudence for safeguarding the right to privacy in communication from which Uganda can emulate. Save for the constitutional provision in Art 27 on the right to privacy, Uganda generally lacks a major legislation protecting the right to privacy in communication. The only legislation available such as the Anti-Terrorism Act is only for further suppression of the right. Uganda should borrow a leaf from Canada and pass a comprehensive law on the protection of the right to privacy.

\textsuperscript{72} See generally Mamdani Mahmood, Good Muslim, Bad Muslim: America, the Cold War, and the Roots of Terror, Fountain Publishers, Kampala, 2004.
\textsuperscript{73} Mr. Wafula-Oguttu [Spokesperson, FDC Party] in an interview with the author on 9\textsuperscript{th} August, 2007.
\textsuperscript{74} In relation to Article 17 of the I.C.C.P.R., see General Comment 16 issued by the Human Rights Committee on 23\textsuperscript{rd} March 1988 (U.N. Doc. A/43/40, p. 180-183), paragraphs 7 & 10.
In Uganda, phone-tapping has not been tested in court. In Canada, the Supreme Court of Canada in the case of *R.v.Wong*\(^75\), held *inter alia* that evidence of gambling obtained by unconstitutional video surveillance not to be excluded under s. 24(2) of Charter where officers acting in good faith, upon reasonable and probable cause and breach stemming from reasonable misunderstanding of law obtained such evidence.

In the earlier case of *R. v. Duarte*\(^76\), the Supreme Court of Canada emphasised judicial review in wire tapping. The Supreme Court concluded:

“If privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself; a reasonable expectation of privacy would seem to demand that an individual may proceed on the assumption that the State may only violate this right by recording private communication on a clandestine basis when it has established to the satisfaction of a detached judicial officer that an offence has been or is being committed and that interception of the private communications stands to afford evidence of the offence.”\(^77\)

Further, Justice Iacobucci, in *R. v. Oickle*\(^78\), observed thus:

“…..the Charter is not an exclusive catalogue of rights. Instead, it represents a bare minimum below which the law must not fall. A necessary corollary of this statement is that the law, whether by statute or common law, can offer protections beyond those guaranteed by the Charter.”\(^79\)

From the aforegoing, it can clearly be seen that the Canadian and Ugandan conceptions of privacy interests differ from one another and these conceptions affect the practical articulation of this right as discussed above.

---

\(^75\) [1990] 3 S.C.R. 36, paras.56-57.
\(^76\) [1987] 3 C.C.C. (3d) 1.
\(^79\) S.189 (1) of the Canada Criminal Code (CCC) on automatic exclusion of private communication evidence unless the interception had been lawfully made or consent for admissibility was expressly given by neither the originator or the person intended by the originator to receive the communication. It also provided that “evidence obtained directly or indirectly as a result of information acquired by interception of a private communication is not inadmissible by reason only that the private communication is itself inadmissible as evidence”. S.189 (1) to (4) was repealed in 1993. This eliminated the automatic exclusionary rule if an interception was unlawful. Now s.24 (2) of the Charter governs the admissibility or exclusion of all intercepted private communications and evidence gained directly or indirectly by an unlawful interception. However, even if the interception is lawful within the provisions of Part VI of the CCC, it is still subject to Charter standards including s.8. *See, also* Hubbard, R.W., Brauti, P.M., Fenton, S.K., *Wiretapping and Other Electronic Surveillance*, 2007, Canada; and McWilliams, *Canadian Criminal Law*, 4\(^{th}\) Ed., Vol.2.
V. Conclusion

The response to the threat of terrorism and national insecurity should go beyond military and police action and address the root causes of the increasing use of terrorist methods. In addition to the unresolved conflict in Northern Uganda and the denial of self-government/power sharing between the central and the regional governments, there seem to be many other causes of terrorism and threats to national security in Uganda. The blind pursuit of the structural adjustment policies of the IMF and the World Bank coupled with the poverty and denial of human rights as a result of globalization driven by neo-liberalist policies (mostly pursued by the WTO and WIPO) certainly figures prominently among the root causes of present day terrorism in Uganda much of which is foreign sponsored. Uganda too should avoid a policy of aggression similar to that taken in the 1990s against neighboring countries such as DRC, Sudan, and Rwanda as this aggravates the likelihood of terrorist attacks by those countries and their allies against Uganda. Open alliance with terrorist prone/target countries such as the U.S.A. and the U.K. in turn makes Uganda a soft target by the many enemies of the two superpowers who may opt to vent their anger on the defenceless Uganda after missing their targets on the U.S.A. or the U.K. Mere legislation alone will not help but these factors too need be looked into in the fight against terrorism and other threats against national security in Uganda. Canada offers much to Uganda to learn in form of safeguarding to the right to privacy in communication in this era of terrorism and increased organized crime.

References

Hubbard, R.W., Brauti, P.M., Fenton, S.K., *Wiretapping and Other Electronic Surveillance*, 2007, Canada
Mamdani, Mahmood, Good Muslim, Bad Muslim: America, the Cold War and the Root of Terror (Kampala, Fountain, 2004).