AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: HW Gebreegziabher 'The right to privacy in the age of surveillance to counter terrorism in Ethiopia' (2018) 18 *African Human Rights Law Journal* 392-412
http://dx.doi.org/10.17159/1996-2096/2018/v18n1a18

The right to privacy in the age of surveillance to counter terrorism in Ethiopia

Hiruy Wubie Gebreegziabher
PhD Candidate, Faculty of Law, Monash University, Melbourne, Australia

Summary

Despite being a useful tool to prevent and prosecute terrorism, surveillance is increasingly being utilised as an excuse for infringements on privacy in several jurisdictions. Laws governing counter-terrorism surveillance either are not in compliance with human rights standards governing privacy or inappropriately implemented. Research on the relevant law and practice in Ethiopia is limited. This article identifies legal and practical problems causing violations of the right to privacy while countering terrorism in Ethiopia. In doing so, it evaluates the human rights compatibility of the relevant law and practice mainly based on article 17 of the ICCPR. The analysis is substantiated by an empirical study involving key informant interviews and case file reviews from Ethiopian courts. Legitimate counter-terrorism surveillance should respect the right to privacy. A state may implement counter-terrorism surveillance only when it is properly defined by law and reasonably applied. Prior judicial authorisation of covert interceptions is usually regarded as a safeguard to prevent the misuse of counter-terrorism surveillance. Ethiopia does not have a law regulating mass surveillance in the absence of a specific terrorism threat. However, reports suggest that the Ethiopian government has unrestricted access to private communications since it monopolises telecommunications and postal services. Counter-terrorism related surveillance, however, is legally regulated in Ethiopia. Ethiopian law requires that law enforcement agencies may conduct the interception of communications on terrorist suspects upon getting a court warrant. Nonetheless, evidence suggests that, in practice, there is widespread use of warrantless interceptions

* LLB LLM (Addis Ababa); hiruy.wubie@gmail.com. I am grateful to my PhD supervisors, Prof Sarah Joseph and Dr Joanna Kyriakakis, for their constructive comments on section four of this article. I acknowledge Monash University for financially supporting this research.

which are used as prosecution evidence in defiance of the law. This article may serve to assess and improve counter-terrorism surveillance in Ethiopia so that the law and its implementation reflect the values of a democratic society based on the rule of law and respect for the right to privacy.

Key words: *Ethiopia; Anti-Terrorism Proclamation; counter-terrorism surveillance; mass surveillance; targeted surveillance*

1 Introduction

Counter-terrorism-related surveillance is one of the prominent contemporary challenges in the exercise of the right to privacy. This article examines state surveillance in Ethiopia and assesses its compatibility with the right to privacy. The use (abuse) of surveillance and intercepted communications in terrorism-related criminal proceedings will particularly be analysed based on relevant Ethiopian laws and international human rights instruments ratified by Ethiopia. Ethiopia is a party to the International Covenant on Civil and Political Rights (ICCPR)[1] and the African Charter on Human and Peoples' Rights (African Charter).[2] International human rights instruments ratified by Ethiopia form part of the law of the land.[3] Indeed, the Federal Democratic Republic of Ethiopia Constitution (Ethiopian Constitution)[4] provides that its human rights provisions should be interpreted in conformity with international human rights covenants adopted by Ethiopia.[5]The human rights compatibility assessment in the article, therefore, will be done by analysing the relevant provisions of the ICCPR and associated jurisprudence. The African Charter does not specifically recognise the right to privacy. Although the Ethiopian Constitution recognises the right to privacy, there are no relevant cases and jurisprudence.[6] Therefore, due to the depth of the jurisprudence under the ICCPR, most of the analysis in the article draws from the ICCPR. Reference to the African Charter and the Ethiopian Constitution will be made whenever necessary.

In addition to the doctrinal analysis of the relevant Ethiopian laws and international human rights covenants, the analysis in the article will be substantiated by empirical data collected in Ethiopia between

1 International Covenant on Civil and Political Rights, UN General Assembly Resolution 2200A of 16 December 1966 (ICCPR).

2 African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 June 1981.

3 Constitution of the Federal Democratic Republic of Ethiopia Proclamation 1/1995, Federal Negarit Gazeta, 1st Year No 1 (Ethiopian Constitution).

4 Art 9(4) Ethiopian Constitution.

5 Art 13(2) Ethiopian Constitution.

6 G Timothewos 'Freedom of expression in Ethiopia: The jurisprudential dearth' (2010) 4 *Mizan Law Review* 201 231. Timothewos explains that there is a serious lack of cases and jurisprudence explaining the freedom of expression provision of the Ethiopian Constitution. Therefore, the dearth of cases and jurisprudence based on the provision regarding the right to privacy in the Constitution is not unique.

February and May 2016. The empirical data includes interviews with judges, prosecutors, defence lawyers and police officers who have first-hand terrorism-related experience, as well as relevant case file reviews at Ethiopian federal and regional courts. The data collection was made pursuant to a human ethics approval to ensure research integrity and participants' safety.[7] The interviews accordingly are anonymised to prevent interviewees from being identified.

The article begins with a brief overview of terrorism threats in Ethiopia and the Anti-Terrorism Proclamation, which regulates criminal justice responses to counter-terrorism in Ethiopia. It then explains the necessity of adherence to the rule of law as an important feature of an effective counter-terrorism strategy. Adherence to the rule of law requires that counter-terrorism laws and their implementation should not set aside relevant international human rights standards. Hence, the next section of the article evaluates the human rights compatibility of Ethiopia's laws regulating surveillance and interception of communications and the consequent practices. Lastly, the article finalises its arguments with concluding remarks and recommendations.

2 Brief overview of Ethiopia's terrorism threats and the Anti-Terrorism Proclamation

Terrorism is a contested subject. Attempts to adopt a universal definition of terrorism are generally unsuccessful.[8] The political risk of taking positions on the various elements of a definition of terrorism is one of the most significant factors inhibiting agreement on a universal definition of terrorism.[9] One of these divisive issues is whether terrorism should be defined in a manner that includes both state and non-state terrorism. Some scholars argue that terrorism should be defined in an actor-neutral approach, including state terrorism.[10] Others argue against the inclusion of state terrorism, alleging that it will only complicate efforts in defining terrorism. It has also been argued that state terrorism should be excluded since it is already regulated by rules of international humanitarian law in the context of

7 Monash University Human Research Ethics Committee approved the project for data collection in a project with reference number CF15/2367-2015000953.

8 See B Saul 'Attempts to define "terrorism" in international law' (2005) 52 *Netherlands International Law Review* 57 57-83; see also E Herschinger 'A battlefield of meanings: The struggle for identity in the UN debates on a definition of international terrorism' (2013) 25 *Terrorism and Political Violence* 183.

9 S Zeidan 'Desperately seeking definition: The international community's quest for identifying the spector of terrorism' (2004) 36 *Cornell International Law Journal* 491.

10 See, eg, M Stohl 'Yes: State terror: The theoretical and practical utilities and implications of a contested concept' in R Jackson & SJ Sinclair (eds) *Contemporary debates on terrorism* (2012) 43 44.

an armed conflict.[11] For any violence perpetrated by the state outside of the context of an armed conflict, the concepts of 'human rights abuses'[12] and 'crimes against humanity'[13] regulate state actions. The term 'terrorism' is used in this article without reference to arguments pertaining to state terrorism.

The Eastern African region, where Ethiopia is located, is considered one of the major sources of global terrorism, particularly after the 1990s.[14] The existence of several social and political problems creates a comfortable breeding ground for terrorism in the Eastern African region.[15] In light of the complicated social, economic and political problems in the region, some have even doubted if parts of Africa, including the Eastern African region, have any hope of overcoming terrorism at all.[16]

The sources of the terrorism threat in Ethiopia may be summarised in three categories. These are the proliferation of insurgent groups and other political groups aiming at unconstitutional change; Somalia-based radicalised Islamic groups such as Al-Shabaab; and the threatening inter-ethnic conflicts.[17] The most common source of the terrorism threat in Ethiopia is that of rebel political groups that use 'all possible means' to topple the Ethiopian government.[18] The use of violence to settle political differences is not uncommon in Ethiopia.[19] The relations between the government and the political opposition is

11 M Williamson *Terrorism, war and international law: The legality of the use of force against Afghanistan in 2001* (2009) 67.

12 See United Nations Office of the High Commissioner for Human Rights *Training manual on human rights monitoring* (2001)10.

13 See G Werle & B Burghardt 'Do crimes against humanity require the participation of a state or a 'state-like' organisation?' (2012) 10 *Journal of International Criminal Justice* 1151.

14 RI Rotberg (ed) *Battling terrorism in the Horn of Africa* (2005) 94; United States Institute of Peace workshop, Special Report: Terrorism in the Horn of Africa, Washington DC January 2004 2.

15 PN Lyman & JS Morrison 'The terrorist threat in Africa' (2014) 83 *Foreign Affairs* 75 76.

16 See, generally, RL Feldman 'The root causes of terrorism: Why parts of Africa might never be at peace' (2009) 25 *Defence and Security Analysis* 355.

17 Rotberg (n 15 above) 99. See also D Feyissa 'The experience of Gambella regional state' in D Turton (ed) *Ethnic federalism: The Ethiopian experience in comparative perspective* (2006) 208.

18 See, eg, a leading opposition group in exile named Ginbot 7, which is proscribed as a terrorist organisation, which officially proclaimed the following in its political strategy: 'Owing to the peculiar situation in Ethiopia, it will be using *all possible means* as its political strategy without being constrained by the threatening measures based on "law" and other ways by the authoritarian leaders and their constituency.' Ginbot 7 official website, http://www.ginbot7.org/ (accessed 21 October 2014). There are also a number of ethnically-organised large and small insurgent groups, all aiming at overthrowing the government with armed struggle demands ranging from secession to claims of democratic inclusion.

19 See, eg, P Toggia 'The revolutionary endgame of political power: The genealogy of "red terror" in Ethiopia' (2012) 10 *African Identities* 265.

usually depicted as a mutually-destructive culture of political violence.[20]

Terrorism-related court cases in Ethiopia to date under the Anti-Terrorism Proclamation indicate that the most common type of terrorism-related cases that reach courts is membership or participation in the activities of proscribed rebel political groups.[21] The rebel political groups use various strategies to destabilise the Ethiopian government, including armed resistance, violent public protests and sporadic bombings. In interviews, a senior police officer at the Ethiopian Federal Police Commission stated that terrorism threats related to these groups were the most complicated and controversial type of terrorism in Ethiopia.[22]

With a declared objective to prevent and prosecute acts of terrorism, the Ethiopian Parliament adopted the Anti-Terrorism Proclamation in August 2009.[23] The Proclamation is the primary legal instrument adopted to regulate terrorism-related criminal justice matters in Ethiopia. The provisions of the Ethiopian Criminal Code and Criminal Procedure Code may be applied in terrorism-related cases only when they are not inconsistent with the Proclamation.[24] The Proclamation defines terrorist acts and prescribes severe penalties, including capital punishment.[25] It criminalises the planning, preparation, conspiracy and attempt of terrorist acts, which are punishable in the same way as the actual commission of the crime.[26] The Proclamation also provides for other lists of criminalised activities in the context of countering terrorism in Ethiopia.[27]

---

20 See, generally, N Ayele 'Legitimacy, culture of political violence and violence of culture in Ethiopia' in JE Rosenfeld (ed) *Terrorism, identity and legitimacy: The four waves theory and political violence* (2011) 212-231.

21 See, eg, *The Federal Public Prosecutor v Abebe Kassie Belay & Others* Ethiopian Federal High Court, Criminal file 149911; *The Amhara Region Public Prosecutor v Awoke Lakew Dasew & Others* Amhara Regional State Supreme Court, Criminal file 12526; *The Amhara Region Public Prosecutor v Belachew Awoke Mengist & Ashenafi Shewarke Tessema* Amhara Regional State Supreme Court, Criminal file 13952; *The Amhara Region Public Prosecutor v Taye Derbe Temeslew & Tariku Yalew Ali* Amhara Regional State Supreme Court, Criminal file 13164; *The Amhara Region Public Prosecutor v Tilahun Abebe & Others* Amhara Regional State Supreme Court, Criminal file 12527; *The Federal Public Prosecutor v Afendi Farah Mohammed Isa & Others* Ethiopian Federal High Court, Criminal file 97453; *The Federal Public Prosecutor v Abdi Mohammed Adem & Adem Ibro Mohammed* Ethiopian Federal High Court, Criminal file 124505.

22 Interview with police officer 2, Investigation of International Crimes division, Ethiopian Federal Police Commission, 24 March 2016.

23 Anti-Terrorism Proclamation 652/2009, Federal Negarit Gazeta 15th Year, No 57 (Anti-Terrorism Proclamation) Preamble.

24 Art 36 Anti-Terrorism Proclamation (n 23 above).

25 Art 3 Anti-Terrorism Proclamation.

26 Art 4 Anti-Terrorism Proclamation.

27 These offences include rendering support to terrorism; encouragement of terrorism; participation in a terrorist organisation; possessing or using property for terrorist acts; possessing and dealing with proceeds of terrorist acts; the false threat of terrorist acts; and a failure to disclose terrorist acts.

The Proclamation authorises the Ethiopian Federal Parliament with a power to proscribe and de-proscribe terrorist organisations.[28] Accordingly, Parliament to date has proscribed five domestic and international groups in 2011 as terrorist organisations. The proscribed groups are Ogaden National Liberation Front (ONLF); Oromo Liberation Front (OLF) and Ginbot 7 Movement for Justice, Freedom and Democracy (Ginbot 7); Al-Qaeda; and Al-Shabaab.[29] Although they pose security threats to Ethiopia, Al-Qaeda and Al-Shabaab are not local groups. ONLF, OLF and Ginbot 7 are domestic political groups whose leaders are in exile. These groups have committed sporadic bombings in public places, assassinated civilian government agents and attempted to destroy state-owned infrastructure.[30]

The decision to proscribe these rebel groups is often a subject of controversy. By the time the Ethiopian Federal Parliament made the decision about proscription, the Ethiopian Peoples' Revolutionary Democratic Front (EPRDF) – the leading political party in Ethiopia since 1991 – and its affiliates controlled all but two seats in Parliament. An independent member and a member of the opposition coalition, the Ethiopian Federal Democratic Unity Forum (MEDREK), were the only non-EPRDF-affiliated members of Parliament. All the EPRDF members of the House of Peoples' Representatives (HPR) and the independent candidate voted for the resolution, contending that the proscription would help in combating terrorism by the proscribed groups, which they referred to as 'anti-peace' and 'anti-development' elements.[31] The only opposition political party member of the HPR voted against the resolution, arguing that proscription should look beyond specific actions of the nominated groups and consider the overall features of Ethiopian politics. He further noted that the proscription would be a negative step against his political party's vision to create tolerance and national consensus between political groups in Ethiopia.[32] The proscription of terrorist organisations and the consequent targeted surveillance of terrorist suspects as per the Proclamation, therefore, are a subject of political controversy.

28 Art 25 Anti-Terrorism Proclamation.

29 See A media (Diretube) video report of the proscription process, http://www.diretube.com/ethiopian-news-ethiopian-parliament-named-five-groups-as-terrorist-video_6e6bc3d3c.html (accessed 9 November 2016).

30 See, eg, *The Guardian* news article, https://www.theguardian.com/world/2007/apr/25/ethiopia (accessed 22 October 2016), where it is stated that the ONLF attack at a Chinese-run mining site in Ethiopia killed 74 Ethiopians and foreigners working on site; *The Federal Public Prosecutor v Fekede Abdisa Gusu & Others* Ethiopian Federal High Court, Criminal file 104548 (an OLF attempt to bomb public places was foiled by the police); Patriotic Ginbot 7 official website, http://www.patriotg7.org/?p=1101 (accessed 9 November 2016) (Ginbot 7 leader Birhanu Nega mentioned in a video message, later transcribed by his organisation's website, that roads and other infrastructure are facilitating government repression and they will be targets for destruction); Patriotic Ginbot 7 official website, http://www.patriotg7.org/?p=1285 (accessed 16 January 2017) (Ginbot 7 takes responsibility for assassinating civilian government agents).

31 A media (Diretube) video report of the proscription process (n 30 above).

32 As above.

The Proclamation incorporates provisions aimed at facilitating state efforts to prevent, control and foil terrorism. The incorporation of such provisions is one of the justifications for the adoption of the Proclamation as a separate criminal legislation which differs from the ordinary Criminal Code, which was adopted in 2004.[33] The provisions in the Proclamation relating to surveillance and interception of communications of terrorist suspects, therefore, are considered 'new legal mechanisms' to enhance terrorism-related investigation and prosecution.[34]

3 Adherence to the rule of law while countering terrorism

Counter-terrorism refers to the overall process to prevent terrorism, including the criminal justice and the 'war-on-terror' approaches. Former United Nations (UN) Secretary-General, Kofi Annan, identified five strategies for an effective counter-terrorism strategy. These are dissuading people from resorting to terrorism or supporting it; denying terrorists the means to carry out an attack; deterring states from supporting terrorism; developing state capacity to defeat terrorism; and defending human rights.[35] Mindful of the fact that many states may lack the requisite capacity and commitment, Kofi Annan identified promoting the rule of law and respect for human rights as one of the priority areas where state capacity to defeat terrorism has to be strengthened.[36]

Terrorism is a term which is 'emotionally charged, morally laden and politically contentious'.[37] Efforts to counter terrorism, therefore, are most likely to be reflections of the political controversy characterising the overall terrorism and counter-terrorism narrative.[38] In this context, adherence to the rule of law may serve as a safeguard to prevent counter-terrorism measures from being arbitrary and unpredictable. Sellers explains how adherence to the rule of law may minimise arbitrary and unpredictable actions as follows:[39]

> The rule of law signifies 'the empire of laws and not of men': the subordination of arbitrary power and the will of public officials as much as possible to the guidance of laws made and enforced to serve their proper

33 Preamble, para 4 Anti-Terrorism Proclamation (n 23 above).

34 As above.

35 United Nations General Assembly, Report of the Secretary-General, Uniting against terrorism: Recommendations for a global counter-terrorism strategy, A/60/825, 2006.

36 UNGA Report (n 35 above) 15.

37 VJ Ramraj et al 'Introduction' in VJ Ramraj et al (eds) *Global anti-terrorism law and policy* (2005) 2.

38 Compare B Saul *Defining terrorism in international law* (2006) 1.

39 MNS Sellers 'What is the rule of law and why is it so important?' in JR Silkenat et al (eds) *The legal doctrines of the rule of law and the legal state (Rechtsstaat)* (2014) 4.

purpose, which is the public good (*res publica*) of the community as a whole.

In a similar vein, renowned scholars in counter-terrorism and human rights studies consider respect for the rule of law as one of the most important pillars of effective counter-terrorism interventions. For example, Schmid contended that 'when rulers stand above the law and use the law as a political instrument against their opponents, the law loses its credibility'.[40] Counter-terrorism law and practice generally has been regarded as an area where governments are tempted to trespass legal limits protecting human rights in the name of countering terrorism.[41] This is particularly true in the context of the right to privacy, where increasing counter-terrorism surveillance may result in unlawful and arbitrary interferences in private communications.[42]

The concept of the rule of law is helpful to protect individuals from unconstrained governmental power.[43] Respect for and the protection of human rights are prominent means of ensuring restraint on governmental power and protecting individuals from abuse of power by the government.[44] States that ratify international human rights covenants have a legal duty to ensure that their counter-terrorism legislation is human rights-compliant. The practical implementation of counter-terrorism legislation, furthermore, should be in accordance with the law. While explaining the various moral traits that characterise the internal morality of the law, Fuller identified 'congruence between official action and declared rule' as the most complex of all.[45] An assessment of congruence between counter-terrorism laws and the consequent practice requires a meticulous approach. In the following sections, the law and the practice of surveillance and interception of communications to counter terrorism in Ethiopia will be assessed for compatibility with the right to privacy, as recognised in the ICCPR and the Ethiopian Constitution.

40 See, eg, AP Schmid 'United Nations measures against terrorism and the work of the terrorism branch: The rule of law, human rights and terrorism' in W Benedek & A Yotopolous-Marangapoulos (eds) *Anti-terrorist measures and human rights* (2004) 53 60.

41 See, eg, N Hicks 'The impact of counter terror on the promotion and protection of human rights: A global perspective' in RA Wilson (ed) *Human rights in the "war on terror"* (2005) 209 212.

42 See, eg, S Sottiaux *Terrorism and the limitation of rights: The ECHR and the US Constitution* (2008) 308.

43 G Lautenbach *The concept of the rule of law and the European Court of Human Rights* (2013) 23.

44 As above.

45 LL Fuller *The morality of law* (1969) 81.

4 Surveillance to counter terrorism in Ethiopia: A challenge to the right to privacy?

4.1 Right to privacy

The notion of privacy may be defined differently based on one's interpretation of what amounts to an 'individual's sphere of autonomy'.[46] It refers to an individual's 'desire for independence of personal activity, a form of autonomy'.[47] Cannataci, the UN Special Rapporteur on the Right to Privacy, noted that despite the absence of a universally-agreed definition, the concept of privacy is related to individual autonomy and self-determination.[48] He recommends that our conceptualisation of privacy be 'framed in the context of a discussion of the protection and promotion of the fundamental right to dignity and the free, unhindered development of one's personality'.[49] Privacy mainly involves what should be left only to the individual concerned. However, the conceptual understanding of the right to privacy is further obscured in this era of digital communications where the right to privacy can only protect anonymity instead of not being observed at all.[50]

The African Charter does not explicitly recognise the right to privacy. However, the African Commission on Human and Peoples' Rights (African Commission) notes in a guideline[51] that components of the right to privacy may be inferred from other provisions of the African Charter, which emphasise state non-interference on individual matters.[52]

Article 26 of the Ethiopian Constitution on the right to privacy reads 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.

46 See S Joseph & M Castan *The International Covenant on Civil and Political Rights: Cases, materials and commentary* (2013) 533-534.

47 P Rosenzweig 'Privacy and counter-terrorism: The pervasiveness of data' (2010) 42 *Case Western Reserve Journal of International Law* 625 641.

48 Joseph A Cannataci, United Nations Special Rapporteur, 'Report of the Special Rapporteur on the Right to Privacy', UN Doc A/HRC/31/64 (2016) 10.

49 As above.

50 Rosenzweig (n 47 above) 646.

51 Art 45(1)(b) of the African Charter mandates the African Commission to formulate rules, principles and standards relating to human and peoples' rights upon which African governments may base their legislation. Such guidelines are designed in accordance with the Commission's case law and resolutions as well as international human rights treaty law.

52 African Commission on Human and Peoples' Rights Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa, adopted in Banjul, The Gambia, 56th ordinary session, May 2015, part 11(A).

(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.

Given the limited jurisprudence on the subject of the African Commission and the Ethiopian Constitution, the following commentary therefore will concentrate on the ICCPR.

Article 17 of the ICCPR provides as follows:

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

In its General Comment on the right to privacy,[53] the Human Rights Committee (HRC) stated that the ICCPR protects individuals from unlawful and arbitrary interferences with their privacy interests from state authorities or other persons.[54] The right to privacy, thus, is not absolute and is subject to the concept that any interference must not be 'unlawful' or 'arbitrary'.

Interference in private communications is considered 'unlawful' when it is not authorised by law.[55] Any interference in private communications which is not authorised by law is a breach of the right to privacy. The mere existence of a law authorising interference in private communications, however, is not enough to comply with the ICCPR's requirement of legality. The HRC requires that a law authorising an interception in private be 'precise and circumscribed'.[56]

In the case of *Pinkney v Canada*,[57] the applicant, a detainee at a regional correction centre, claimed that his correspondence had been subjected to arbitrary and unlawful interference by state authorities. The then relevant legislation provided that 'every letter to or from a prisoner shall … be read by the warden or by a responsible officer

53 General Comments contain the Human Rights Committee's interpretations and commentaries on the various provisions of the ICCPR that address matters relevant to all state parties. General Comments are based on art 40(4) of the ICCPR and they make a significant contribution to interpreting the rights recognised in the ICCPR.

54 Human Rights Committee General Comment 16 art 17 (The right to respect of privacy, family and correspondence, and protection of honour and reputation) 1988 para 1.

55 General Comment 16 (n 54 above) para 3.

56 Joseph & Castan (n 46 above) 536; see also (1995) UN Doc CCPR/C/79/Add.54 para 19.

deputed by him for the purpose'.[58] The HRC stated that this provision failed to provide satisfactory legal safeguards against arbitrary application of the warden's power to censor mail. The HRC noted that subsequent legislation, which contained specific provisions regulating censorship of prisoners' communications, was compatible with article 17 of the ICCPR.[59] Therefore, domestic legislation authorising interception in private communications should have specific provisions to prevent an uncircumscribed application.

In addition to being lawful, an interference with private communications must not be 'arbitrary'. A lawful interference may potentially enable a 'highly oppressive invasion' of the right to privacy.[60] The HRC commented that an interference with private communications may be regarded as arbitrary even when it is envisaged by law. The requirement of non-arbitrariness means that an interference with privacy, even when authorised by law, must always be applied in a way that is reasonable in the particular circumstances of a given case.[61] For instance, in *Toonen v Australia*,[62] the HRC stated that any interference with privacy 'must be proportional to the end sought and be necessary in the circumstances of any given case'. Therefore, an interference with privacy may be considered arbitrary if those empowered to authorise the interference do not apply it with restraint. The prohibition on arbitrariness is meant to ensure reasonable applications of interferences with private communications.[63]

The reasonableness of particular interferences with the right to privacy is determined on a case-by-case basis. The ICCPR does not list the permissible grounds that validate restrictions on the right to privacy. The HRC stated that an interference with privacy interests may be allowed only if it 'is essential in the interests of society as understood under the Covenant'.[64] Joseph and Castan argue that permissible grounds for restriction under article 17 should probably be 'proportionate measures designed to achieve a valid end'.[65] In

57 Communication 27/1978, *Larry James Pinkney v Canada*, UNHR Committee 29 October 1981 UN Doc CCPR/C/OP/1 95 (1985).The first Optional Protocol to the ICCPR gives the HRC a mandate to receive and consider communications from individuals who make complains against a state party to the ICCPR which should also be a party to the first Optional Protocol, and recognises the HRC's mandate to entertain individual communications. When such complaints are submitted, the HRC will decide on the matter after reviewing the arguments from the author and the state party. These decisions may serve as guides to interpret the relevant provision of the ICCPR in a similar setting.

58 As above.

59 As above.

60 Joseph & Castan (n 46 above) 537.

61 General Comment 16 (n 54 above) para 4.

62 Communication 488/1992, *Nicholas Toonen v Australia*, UNHR Committee 25 December 1991 UN Doc CCPR/C/50/D/488/1992 (1994).

63 Joseph & Castan (n 46 above) 537.

64 General Comment 16 (n 54 above) para 7.

65 Joseph & Castan (n 46 above) 538.

contrast, article 26 of the Ethiopian Constitution enumerated a list of compelling circumstances which may be regarded as permissible grounds to restrict the exercise of the right to privacy. These grounds are safeguarding national security or public peace; the prevention of crimes or the protection of health; public morality; and the rights and freedoms of others.

In addition to refraining from unlawful and arbitrary interferences in privacy, state parties to the ICCPR have a positive obligation to take measures to protect privacy. Article 17(2) of the ICCPR requires that there should be a legal framework which prohibits unlawful and arbitrary interferences in privacy by third parties.[66]

4.2 Mass surveillance as a challenge to privacy

Globally, counter-terrorism initiatives have complicated the relations between citizens and governments in the context of respect for and protection of the right to privacy.[67] This is due to the increasingly-expansive surveillance powers that states use with a declared objective of countering terrorism.[68] Increased surveillance powers are often justified to prevent the commission of acts of terrorism by taking pro-active measures based on surveillance data.[69] Surveillance is also helpful to gather evidence which may be used to prosecute perpetrators of terrorist acts. Counter-terrorism is a legitimate objective which may be used to restrict the exercise of the right to privacy. Nevertheless, counter-terrorism surveillance must be regulated by law and applied with proportionate restraint.

Although human rights instruments require that interferences with privacy be legal and reasonable, the practice in different jurisdictions indicates that governments on many occasions employ unnecessarily invasive measures against the right to privacy in the name of countering terrorism.[70] In Africa, one specific criticism against states has been the use of counter-terrorism to prioritise regime survival over human security.[71]

Surveillance may take two forms in the context of counter-terrorism, namely, mass surveillance or targeted surveillance. Mass surveillance refers to 'the general practice of seeking bulk access to digital communications'.[72] Mass surveillance is applied irrespective of

66 General Comment 16 (n 54 above) para 9.

67 F Davis et al 'Mapping the terrain' in F Davis et al (eds) *Surveillance, counter-terrorism and comparative constitutionalism* (2014) 3 4.

68 As above.

69 S Sottiaux *Terrorism and the limitation of rights: The ECHR and the US Constitution* (2008) 265.

70 Sottiaux (n 69 above) 294 308.

71 P Kagwanja 'Counter-terrorism in the Horn of Africa: New security frontiers, old strategies' (2006) 15 *African Security Review* 72 84.

72 Ben Emmerson, United Nations' Special Rapporteur, 'Report of the Special Reporter on the Promotion and Protection of Human Rights while Countering-Terrorism' UN Doc A/69/397 (2014) 5.

whether the subjects of surveillance are suspected of any involvement in terrorism. Some states utilise mass surveillance as a counter-terrorism measure to trace potential threats of terrorism. However, there are arguments that mass surveillance is not particularly helpful in preventing terrorism.[73] If mass surveillance does not have particular benefits in preventing terrorism, it is difficult to imagine justifications to uphold the consequent interference with the right to privacy.

The UN Special Rapporteur on Human Rights and Counter-Terrorism has noted that only a few states have adopted explicit legislation governing mass surveillance.[74] Others rely on older laws which are unable to regulate contemporary surveillance capacities.[75] In the absence of a relevant regulatory regime, mass surveillance programmes are likely to lead to breaches of the right to privacy. The Special Rapporteur on Human Rights and Counter-Terrorism has stated:[76]

> The absence of clear and up-to-date legislation creates an environment in which arbitrary interferences with the right to privacy can occur without commensurate safeguards. Explicit and detailed laws are essential for ensuring legality and proportionality in this context. They are also an indispensable means of enabling individuals to foresee whether and in what circumstances their communications may be a subject of surveillance.

The Special Rapporteur has furthermore indicated that mass surveillance is likely to breach the right to privacy unless a state party can substantively justify the legality, necessity and proportionality of the adoption of such a measure.[77] Since mass surveillance sometimes is utilised against the general public, without necessarily requiring the presence of imminent security threats, mass surveillance is highly problematic with regard to the right to privacy. This is because justifications for the necessity and proportionality of such measures are less likely to be demonstrated in the absence of a specific terrorism threat.

In Ethiopia, a state-owned corporation enjoys a monopoly over all telecommunications services.[78] A state-owned provider also predominantly controls postal services.[79] Ethiopia does not have specific legislation regulating the government's access to private communications through these mediums. Ethiopia has no laws specifically regulating the use of mass surveillance. In practice, the Ethiopian government has unrestricted access to all telephone call recordings and metadata, in defiance of the right to privacy.[80] It is

73 Cannataci (n 48 above) 6.
74 Emmerson (n 72 above) 14.
75 As above.
76 Emmerson (n 72 above) 14-15.
77 As above.
78 Ethio-Telecom Establishment Council of Ministers Regulation 197/2010, Federal Negarit Gazeta, 17th Year, No 11.
79 Ethiopian Postal Service Enterprise Establishment Council of Ministers Regulation 165/2009, Federal Negarit Gazeta, 15th Year, No 29.

alleged that the government abuses this access as a partisan instrument against political dissidents.[81] In some cases, the political dissidents allegedly affected by intrusive surveillance are individuals who have alleged contacts with proscribed terrorist groups based in the diaspora. Some of them are leaders of registered opposition political parties with alleged links to the proscribed organisations.[82] The level of governmental control in telecommunications is so enormous that it has created a public perception that the government monitors everyone's movements.[83]

Mass surveillance may be an acceptable means of anticipating future security risks in some circumstances, provided that the Ethiopian government offers a particular justification. In such a case, there should be a legislative framework to regulate its application and provide a chance for an open evaluation of the system from a human rights perspective.[84] The practice of mass surveillance without a legal basis circumscribing its application does not comply with requirements regarding lawfulness in article 17(1) of the ICCPR. Furthermore, the absence of a legislative framework to regulate mass surveillance by the government and other persons is a breach of article 17(2) of the ICCPR and article 26 of the Ethiopian Constitution.

4.3 Targeted surveillance as a challenge to privacy

Targeted surveillance refers to the process whereby law enforcement agencies survey an individual or a group with a view to monitoring and documenting their activities.[85] Such surveillance generally is regarded as legitimate as long as a person is reasonably suspected of involvement in terrorism.[86] However, targeted surveillance should be implemented with restraint and be applied only when necessary.

As opposed to cases of mass surveillance, which are not addressed in the Ethiopian Anti-Terrorism Proclamation or elsewhere in Ethiopian law, the Proclamation places limits upon the exercise of targeted surveillance against terrorist suspects in Ethiopia. Specifically, the Proclamation empowers the police and the National Intelligence and Security Services (NISS) to intercept the communications of, or conduct surveillance on, anyone suspected of terrorism.[87] The police and NISS may enter into any premises in secret or install or remove instruments to enforce or enable the interception.[88] The Proclamation

80 Human Rights Watch Report *They know everything we do: Telecom and internet surveillance in Ethiopia* (2014) 36.
81 HRW Report (n 80 above) 14-19.
82 As above.
83 As above.
84 See Ben Emmerson, United Nations Special Rapporteur, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' UN Doc A/HRC/34/61 (2017) 12.
85 Emmerson (n 72 above) 3.
86 Emmerson 12.
87 Art 14(1) Anti-Terrorism Proclamation (n 23 above).

obliges all communication service providers to co-operate with the NISS to conduct interceptions.[89] It provides that the purpose of the interception or surveillance should be the prevention or control of acts of terrorism.[90] To prevent misuse of surveillance data, the Proclamation requires that 'information obtained through interception shall be kept in secret'.[91] It should be noted that the requirement of secrecy will not be relevant if evidence based on interception is later made part of prosecution evidence in a terrorism-related trial. In all other cases, the police and NISS should prevent intercepted data from being made publicly available.

One of the procedural safeguards established by the Proclamation to ensure the legality and reasonableness of an interference with privacy in the context of counter-terrorism is the requirement of independent prior authorisation of the interference.[92] In Ethiopia, a court warrant is required for the police or the NISS to conduct interception and surveillance against a terrorist suspect.[93] The Proclamation requires that the court consider two factors before issuing a warrant for a covert search and seizure. The first is the gravity of the suspected or committed terrorist act; second, the court will consider the contribution of the warrant to the prevention of an act of terrorism or in order to apprehend a terrorist suspect.[94]

The UN Special Rapporteur on Privacy indicates that a reasonable suspicion of involvement in terrorism and prior judicial authorisation may constitute a valid reason to interfere in privacy.[95] However, the Proclamation fails to specify the standard of suspicion in this regard. It is thus not clear whether courts should consider a reasonable standard of suspicion as the acceptable ground to seek a warrant for covert interception of communications, or whether something short of this would suffice. In the absence of express language regarding the standard of suspicion required, unsubstantiated or unreasonable suspicions arguably could be used as justifications to interfere in privacy under Ethiopian law.

The Proclamation states that evidence gathered through interception or surveillance is admissible in terrorism-related criminal proceedings.[96] Indeed, intercepted communications form part of the evidence in many terrorism-related cases.[97] However, it appears that

88 As above.
89 Art 14(3) Anti-Terrorism Proclamation.
90 Art 14(4) Anti-Terrorism Proclamation.
91 Art 14(2) Anti-Terrorism Proclamation.
92 Compare Emmerson (n 77 above) 3.
93 Art 14 Anti-Terrorism Proclamation.
94 Art 18(1) Anti-Terrorism Proclamation.
95 Cannataci (n 48 above) 13.
96 Art 23(3) Anti-Terrorism Proclamation.
97 Interview with Judge 2, Ethiopian Federal High Court judge, Lideta sub-city, Addis Ababa, Ethiopia 9 March 2016. See also the following cases: *The Federal Public Prosecutor v Elias Kifle & Others* The Ethiopian Federal High Court, Criminal file

there are times when the police and the NISS do not conduct the relevant interceptions based on a court warrant as required by the Proclamation. From the more than 30 terrorism-related court cases reviewed for this research, in only one case did the prosecution include a court warrant for the interception in the list of evidence presented to the trial court.[98] In the rest of the cases, the prosecutors did not provide evidence of a court warrant to perform the interception. This is so, despite a police officer asserting in interviews that police only ever intercept communications after obtaining a court warrant.[99]

Moreover, it is not clear which court has jurisdiction to entertain court warrant requests for interception and surveillance. In the absence of a specific provision in this regard, it appears that the Proclamation envisages that such requests should be presented to courts hearing terrorism-related trials: the Federal High Court or the Federal Supreme Court. The Vice-President of the Ethiopian Federal High Court stated in an interview that the police or the NISS could request the warrant either from the terrorism bench or the president or vice-presidents of the Federal High and Supreme Courts.[100] He further explained that if the alleged offence is punishable with less than 15 years' imprisonment, the application for an interception warrant may be decided by one judge. In all other cases, three judges have to sign the warrant.[101] Nevertheless, all but one of the five judges interviewed for this research stated that they did not remember any request for interception either from the police or the NISS.[102] The fact that judges presiding on the terrorism bench of the Federal High Court, with long years of experience, did not encounter any request for interception may further indicate that the police or the NISS have implemented warrantless interceptions.

One of the most common types of evidence produced by prosecutors in terrorism-related trials in Ethiopia is a copy of

124062 (*Elias Kifle & Others* case); *The Federal Public Prosecutor v Andualem Arage Wale & Others* The Ethiopian Federal High Court, Criminal file 112546 (*Andualem Arage & Others* case); *The Federal Public Prosecutor v Zelalem Wokagegnehu & Others* The Ethiopian Federal High Court, Criminal file 158194.

98 *Elias Kifle & Others* case (n 97 above).

99 Interview with police officer 1, Investigation of Terrorism-Related Crimes division, Ethiopian Federal Police Commission 22 March 2016.

100 Interview with Judge 5, judge and Vice-President of the Federal High Court of Ethiopia, Lideta sub-city, Addis Ababa, Ethiopia 12 May 2016. However, see interview with Judge 1, Ethiopian Federal High Court judge, Lideta sub-city, Addis Ababa, Ethiopia 2 March 2016. While attempting to justify why interception warrants are not presented to the terrorism bench of the Federal High Court, the judge stated that '[s]ince such kind of interception occurs before the filing of a criminal charge, the police and the NISS may be requesting such warrants from Federal First Instance courts which entertain pre-trial issues including remand'.

101 Interview with Judge 5 (n 100 above).

102 Interview with Judge 1 (n 100 above); interview with Judge 2 (n 98 above); interview with Judge 3, Oromia Regional Supreme Court Judge, Arada sub-city, Addis Ababa, Ethiopia 12 May 2016; interview with Judge 4, Amhara Regional Supreme Court judge, Bahirdar, Ethiopia 5 April 2016.

intercepted communications by terrorist suspects or their associates. In addition to intercepted telephone communications, the police and prosecutors often rely on electronic media accounts of terrorism suspects as evidence in trials. It is particularly common for transcripts from e-mail and private Facebook messages with members of banned political groups in the diaspora to form part of the evidence in terrorism trials.[103] In most of these cases, the prosecution did not provide evidence of the proper authorisation for the interception of communications. The absence of evidence to prove the judicial authorisation of intercepted communications, which are later used as part of the prosecution evidence, is a strong indicator that the police sometimes implement warrantless interceptions in private communications.

In practice, intercepted communications are procured in two ways. First, public prosecutors use intercepted audio records of suspected terrorists allegedly recorded as part of the criminal investigation process. Second, while investigating a terrorism-related crime, the police routinely check e-mail and private messages within social media accounts belonging to the suspect with a view to finding something that may be used as evidence. In interviews, a lawyer explained how the police organise transcripts of electronic communications for terrorism-related investigations pending a criminal trial as follows:[104]

> If terrorism suspects have e-mail or Facebook accounts, the police will mostly require them to give their passwords and look into the files for anything which may be used as evidence. The police will first look at the accounts. If they find something that they may use as evidence, they will invite witnesses and research the accounts to have a witness observe that a given document is printed from a suspect's account.

Defence lawyers usually challenge the admissibility of intercepted evidence when there is no proof of a court warrant to undertake the interception.[105] When confronted with such objections, prosecutors present findings of such an interception as part of intelligence reports.[106] The Proclamation exempts intelligence reports prepared in relation to terrorism from disclosing the source or the method of its gathering.[107] The practice of evading the requirement of a warrant for interception, or at least the requirement of proof of a warrant, is an inappropriate deviation from the Proclamation and seems to amount to an unlawful interference in the privacy interests of the

103 See, eg, the *Andualem Arage & Others* case (n 97 above); *The Federal Public Prosecutor v Zemene Kassie Bewke & Others* The Ethiopian Federal High Court, Criminal file 141253 (*Zemene Kassie Bewke & Others* case); *The Federal Public Prosecutor v Hassen Jarso Setolu & Others* The Ethiopian Federal High Court, Criminal file 119650; *The Federal Public Prosecutor v Desalegn Embiale Kebede & Others* The Ethiopian Federal High Court, Criminal file 124062.

104 Interview with lawyer 1, defence lawyer of terrorist suspects, Addis Ketema sub-city, Addis Ababa, Ethiopia 19 March 2016.

105 Interview with Judge 1 (n 100 above).

106 As above; interview with Judge 2 (n 100 above).

107 Art 23(1) Anti-Terrorism Proclamation.

suspects implicated in the particular case. If so, such instances are breaches of the right to privacy.

As noted above and confirmed in interviews, police officers require suspects to provide their e-mail and Facebook passwords during investigation. Responding to critics alleging that the police use force to obtain passwords from suspects, a police officer stated that 'when we have enough information regarding terror-related electronic communications, we do interrogate suspects to voluntarily give their e-mail and Facebook passwords as a gesture of co-operation'.[108] If suspects decline to give their passwords, the police 'use their own ways to access the electronic communications'.[109] This expression may suggest that the police practically implement unauthorised interceptions of communications. It appears that the police do not generally request court warrants to examine electronic communications, which instead is regarded as a routine part of investigations during the pre-trial stage of criminal proceedings against terrorist suspects. The UN Special Rapporteur on Privacy identified practices of warrantless interceptions as violations of the right to privacy.[110]

However, there are a number of cases where evidence based on intercepted communications of terrorist suspects is admitted by trial courts without proof that the interception took place based on prior judicial authorisation.[111] Trial courts have a duty to ensure the protection of terrorist suspects' right to privacy.[112] The prevalent use of illegally-obtained intercepted communications of terrorist suspects at trial courts, without confirmation of its having been obtained legally, is likely to be a breach of the state's duty to protect the right to privacy which is recognised in article 17(2) of the ICCPR.

It was commented above that the failure of the Proclamation to specify the standard of suspicion makes it susceptible to abuse by the police. Judicial practice remains unclear in this regard. Targeted surveillance apparently is implemented without a court warrant. There is no adequate data to determine whether courts authorise requests for interception based on a reasonable suspicion that the subject of the interception is involved in terrorism.

Given the fact that targeted surveillance is usually implemented without a court warrant, it is not clear whether courts authorise requests for interception based on reasonable suspicion that the subject of the interception is involved in terrorism. The failure by the Proclamation to outline the standard of suspicion required in such circumstances might lead to potentially-unsubstantiated suspicions by

108 Interview with police officer 2, Investigation of International Crimes division, Ethiopian Federal Police Commission 24 March 2016.
109 Interview with police officer 1 (n 99 above).
110 Cannataci (n 48 above) 20.
111 See, eg, *Zemene Kassie Bewke & Others* case (n 103 above).
112 Art 13(1) Ethiopian Constitution.

the police to be used as excuses to interfere in privacy. The Ethiopian Parliament should consider revising the Proclamation so that only reasonable suspicions by the police may be used as legitimate grounds to seek judicial authorisation of targeted interference in privacy interests of terrorist suspects. In the absence of such a circumscribed provision, the purpose of prior judicial authorisation – to evaluate requests of interference in privacy on a case-by-case basis – cannot be achieved.

In addition to electronic surveillance, the Proclamation provides a legal basis for sudden and covert searches of persons and premises with a view to prevent acts of terrorism:[113]

> Where a police officer has a reasonable suspicion that a terrorist act may be committed and deems it necessary to make a sudden search in order to prevent the act, with the permission of the Director-General of the Federal Police or a person delegated by him, may stop a vehicle and pedestrian in an area and conduct sudden search at any time, and seize relevant evidences.

The sudden search provided for above does not require a court warrant. However, the requirement of permission from the Director-General of the Federal Police or a delegate limits potential misuse of this power by ordinary police officers. Given the fact that imminent threats of a terrorist attack may have irreversible consequences, it seems that the Proclamation's endorsement of a sudden search without a court warrant is a reasonable interference in privacy through sudden open searches. By contrast, a police officer is required to obtain a court warrant in order to undertake a covert search into any premise to prevent or take action against a terrorist act or a terrorist activity.[114] The police should have reasonable grounds to believe that a resident or possessor of the premise to be searched is related to an act of terrorism that has been or is likely to be committed.[115] Whereas a court warrant for covert physical searches has the requirement of reasonable suspicion of involvement in terrorism, the same standard is absent in the case of a court warrant for electronic surveillance.

5 Conclusion and recommendations

Surveillance and interception of communications are one method of counter-terrorism which is often employed as a means to anticipate, prevent and investigate acts of terrorism. Targeted surveillance against terrorist suspects is particularly identified as an effective intelligence and law enforcement tactic while countering terrorism. Many countries have broadened their surveillance and interception outreach

113 Art 16 Anti-Terrorism Proclamation.
114 Arts 17 & 18 Anti-Terrorism Proclamation.
115 Art 17 Anti-Terrorism Proclamation.

accordingly. While counter-terrorism is an undoubtedly justified objective to authorise legitimate restrictions to privacy, counter-terrorism surveillance should be applied within the limits set by relevant international, regional and national human rights standards. Research suggests that the increasingly-expansive counter-terrorism surveillance, which continues to define counter-terrorism in various jurisdictions, is sometimes applied in ways that negate the essence of the right to privacy.

As a country located in the troubled East African region, where violence is used as a means of settling political differences, Ethiopia faces considerable terrorism threats requiring an effective counter-terrorism strategy. Ethiopia adopted a separate Anti-Terrorism Proclamation in 2009. Accordingly, the Ethiopian government controversially proscribed three violent rebel political groups as terrorist organisations. Individuals who are suspected of terrorism charges, including participation and membership of one of the proscribed groups, face terrorism trials in the country. Surveillance and interception of communications is utilised in the process. This article assessed the human rights compatibility of the counter-terrorism surveillance law and its implementation in Ethiopia from the perspective of the right to privacy as recognised in the ICCPR and the Ethiopian Constitution.

Article 17 of the ICCPR requires that interference in privacy may be justified only when it is applied with restraint, in accordance with law. Ethiopia does not have a law regulating mass surveillance where a specific terrorist suspect is not in sight. Nonetheless, reports suggest that the Ethiopian government has unrestricted access to private communications. If mass surveillance is believed to be an effective means of anticipating future security risks, the Ethiopian government may introduce enabling legislation. In the absence of such legislation, legally-unregulated government access to private communications is a violation of the right to privacy.

Unlike mass surveillance, which is legally unregulated in Ethiopia, the Anti-Terrorism Proclamation regulates the use of counter-terrorism surveillance and interception of communications. While the Proclamation requires prior judicial authorisation of counter-terrorism surveillance and interception against terrorist suspects, it fails to specify the standard of suspicion that must be applied. The failure to specify the 'reasonable suspicion' standard, which is widely recognised, may potentially result in the abuse of counter-terrorism surveillance in cases of unsubstantiated suspicions. The Ethiopian Parliament should consider revising the Proclamation so that it is expressly stated that only reasonable suspicions will be sufficient for the judicial authorisation of targeted interference in the privacy of terrorist suspects.

Ethiopian law requires that covert counter-terrorism surveillance and interception of communications by the police and intelligence officers require a court warrant. However, evidence suggests that

warrantless interceptions are in practice often implemented. Most of the terrorism-related case file reviews undertaken for this research suggest that intercepted communications of terrorist suspects are admitted in trial courts without a corresponding court warrant for the interception. It appears that this practice is not adequately challenged. In a case where defence lawyers of terrorist suspects request evidence containing warrantless interceptions to be inadmissible, public prosecutors present the interceptions as intelligence reports. Intelligence reports are legally exempt from disclosing the source or method of collection. The widespread use of warrantless interceptions and their subsequent admission in terrorism trials are a violation of the right to privacy. It is recommended that police, intelligence officers and public prosecutors should conduct terrorism-related investigations within the bounds of the law. Judges should also defend the right to privacy by rejecting evidence from warrantless interceptions.