AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: D Basimanyane 'The peril of digital privacy and free speech in Uganda ' (2025) 25 *African Human Rights Law Journal* 852-885
http://dx.doi.org/10.17159/1996-2096/2025/v25n2a16

The peril of digital privacy and free speech in Uganda

*Dorcas Basimanyane**
Post-Doctoral Fellow and Project Manager, Centre for Human Rights, Faculty of Law, University of Pretoria, South Africa
https://orcid.org/0009-0001-3566-3272

Summary: *Digital privacy and freedom of expression in Uganda are in peril. Despite subscribing to the basic tenets of democracy, social justice and the rule of law, the Ugandan government has emerged as one of the modern-day digital space tyrants, becoming infamous for exercising excessive powers over digital spaces for political reasons. Such notoriety has been compounded by the continued deployment of surveillance equipment to enable extensive spying on civilians, members of opposition, and activists to silence them. The 1995 Constitution guarantees protections for the rights to privacy, freedom of conscience, expression, movement, assembly and association, and it reiterates the state's obligation to respect, uphold and promote these rights. Similarly, the constitutional general limitation clause under article 43 provides that the rights may be limited for reasons of 'public interest'. However, recourse to public interest may not permit political persecution, detention without a trial or any curtailment of the enjoyment of human rights and freedoms beyond what is acceptable and demonstrably justifiable in a free and democratic society. Yet, revelations on the ground prove that there are several incidents where the 'public interest card' has been invoked beyond what is reasonably admissible in a free and democratic society.*

* LLD (Pretoria); basimanyane.k@up.ac.za

Key words: *digital privacy; free speech; communications surveillance; Uganda*

1 Introduction

The opportunity to deter terrorism and counter crime through enhanced surveillance and other measures of intrusion presented itself as an opportunity for another war against civilians by states.[1] It opened a door to the arbitrary use of state power, stifling constitutional values of democracy, accountability and transparency, among others, and resulting in the unrelenting stifling of privacy and freedom of expression rights.[2] Through the card of public interest and national security, states undermine their democracy and human rights obligations towards citizens.[3]

The primary challenge behind the use of invasive communications surveillance as a convenient tool for ensuring public order or national security is that, even though the reason behind its adoption may seem benign, they have a very intrusive effect on the right to privacy and freedom of expression.[4] Therefore, they must be used with caution, where necessary and proportionate, and a balancing exercise must be conducted.[5] Hence, while reinforcing national security measures is necessary and remains a legally sound ground for limiting the rights and freedoms of the people, the state equally remains obligated to uphold the rule of law, ensure social justice and uphold human rights in the process.[6]

On the ground, the existing surveillance laws enacted by African governments enable communications surveillance of people without their knowledge. Such actions have been exacerbated by the phenomenal contemporary growth and prevalence of mobile and internet technology.[7] The more citizens acquire and use such

1 P Kimumwe 'Digital authoritarianism hurting democratic participation in Africa' Collaboration on International ICT Policy in East and Southern Africa 22 June 2022, https://cipesa.org/2022/06/digital-authoritarianism-hurting-democratic-participation-in-africa/ (accessed 3 June 2023).
2 As above.
3 B Kabumba and others *Militarism and the dilemma of post-colonial statehood* (2017) 9-20.
4 D Basimanyane 'The regulatory dilemma on mass communications surveillance and the digital right to privacy in Africa: The case of South Africa' (2022) 30 *African Journal of International and Comparative Law* 361-382.
5 As above.
6 S Yusuf 'Protecting human rights while countering terrorism' *E international relations* 14 February 2012, https://www.e-ir.info/2012/02/14/protecting-human-rights-while-countering-terrorism (accessed 2 June 2023).
7 As above.

technologies, the more vulnerable they become to derogations of their rights.[8]

Many African countries continue to strategically enable the harvesting of data by demanding the mandatory surrender of personal information to merchants during the purchase of sim cards for e-commerce, and to open social media accounts capable of being harvested, stored and processed.[9] Yet, these same laws fail to correspondingly impose limitations and controls over personal data handling by merchants and governments. Ultimately, the same information facilitates unlawful communications surveillance activities that have proven nothing but grievous stifling of rights and freedoms without accountability.

Similarly, the nature of modern communication surveillance systems operated by intelligence services, as exposed by United States (US) whistle blower Edward Snowden in 2013,[10] can harvest data from outside their borders, from the confines of their home countries. This raises serious questions of jurisdiction and state sovereignty rights under international law. International cooperation in addressing crimes such as terrorism and cybercrime facilitates the conclusion of formal agreements with other states to expedite the sharing of the harvested and stored information in their servers.[11] However, the effectiveness of existing safeguards for the purposes of transferring this data across borders has remained questionable. Given all these concerns, the following explores the Ugandan communications surveillance landscape and the historical background.

2 Ugandan communications surveillance landscape: Historical background

Although the 60 years of British colonial rule should rightly be blamed for the skewed developments in the country, poor governance structures, ethnic divisions, elite polarisation and other challenges inherited by the country, post-colonial rule did little towards reversing these proclivities, and instead exacerbated them.[12] Due to the power struggles resulting from the successive repressive regimes in the

8 Kimumwe (n 1).
9 Basimanyane (n 4).
10 G Greenwald 'Edward Snowden the whistle-blower behind the NSA surveillance revelations' *The Guardian* June 2013 9, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed 20 April 2020).
11 As above.
12 F Golooba-Mutebi 'Collapse, war, and reconstruction in Uganda: An analytical narrative on state-making' (2008) 2 *Makerere Institute of Social Research Crisis States Research Centre* 1.

post-colonial era, Uganda struggled to restore national security for its people, in particular respect for human rights and protection of respect for the rule of law.[13] For a long time, the country suffered massive political turbulence, civil war, contested electoral outcomes, military invasions and dictatorships.[14]

The situation apparently calmed only after 1987 under the rulership of President Yoweri Kaguta Museveni, who passed laws regulating the activities of the Internal Security Organisation (ISO) and External Security Organisation (ESO). Laws such as the Constitution[15] and the Security Organisation Act (SOA)[16] compelled the ISO and the ESO to observe and respect human rights in the process of carrying out their national security duties. Although the SOA maintained excessive presidential controls and vague provisions pertaining to their accountability and oversight, such institutionalisation marked the beginning of democratisation of the country's intelligence security.[17]

Other progressive pieces of legislation that followed included the Whistle-Blower's Protection Act;[18] the Public Access to Information Act;[19] the Regulation of Interception of Communications Act; the Data Protection and Privacy Act;[20] and others. These Acts significantly showed a shift from an authoritarian intelligence security regime towards a democracy. However, a persistent lack of political will to implement these laws, and the challenge of lack of harmony between these pieces of legislation and the SOA above, have meant that there is little to show by way of progress. For instance, SOA has repressive provisions that punish by death any reporting of the activities or giving out any information about the intelligence security organisations and their staff, which renders the above legislative democratisation efforts futile.[21]

Under Museveni, the country has managed to align most of its national policies with the basic tenets of the rule of law, social justice and human rights. However, it remains stuck with numerous problems, including the continuous rigging of elections to remain

13 Golooba-Mutebi (n 12) 1-2.
14 Kabumba and others (n 3).
15 The Constitution of Republic of Uganda, 1995 art 221.
16 Chapter 305 of 1987.
17 Golooba-Mutebi (n 12) 1.
18 Act 6 of 2010.
19 Act 4 of 2005.
20 Act 9 of 2019.
21 Chapter 305 of 1987, sec 10(2).

in power, significant human rights violations, misuse of the police, army and intelligence security systems and dictatorship.[22]

3 Incidences of communications surveillance misuse by the Ugandan government

While intelligence services go way back to the era of British colonial rule,[23] the current legal regime was established in 1987 through the aforementioned Security Organisations Act. As the main bodies entrusted with ensuring national security and stability in the country, intelligence security organisations are allowed to gather intelligence through monitoring and surveillance. However, the law now imposes restrictions on their work, and compels them to have due regard to fundamental human rights. However, oversight and accountability have remained a challenge.[24]

As a countermeasure to terrorist attacks that continued to trouble the country, Uganda decided to reinforce its intelligence equipment to improve the monitoring and surveillance systems.[25] Hence, the government allegedly rolled out a multibillion dollar project with the Chinese tech giant, Huawei, which installed several pervasive cameras believed to have facial recognition and artificial intelligence capabilities across prominent cities in the country.[26] While the police claimed that the new surveillance system would help alleviate crime in the country, critics feared that the surveillance system was upgraded to completely silence opposition actors, especially during the run-up to the 2021 elections.[27]

During the 2021 elections, the Chieftaincy of Military Intelligence (CMI) and the Uganda Police Force (UPF), acting on the directions of the President, allegedly operated the pervasive malware, Finfisher, under a secret coding of *Fungua Macho* ('open your eyes' in

22 A Agaba 'Intelligence sector reform in Uganda: Dynamics challenge and prospects' in S Africa & J Kwadjo (eds) *Changing intelligence dynamics in Africa* (2009) 41-60.
23 Agaba (n 22) 42.
24 AS Muchwa 'Intelligence oversight systems in Uganda: Challenges and prospects' (2021) 36 *Intelligence and National Security* 670.
25 S Hayden 'Chinese surveillance systems appear across Ugandan capital Kampala: Rights groups fear Huawei facial-recognition devices part of sinister clampdown on dissent' *Kampala Irish Times* 21 Aug 2019, https://www.irishtimes.com/news/world/africa/chinese surveillance-systems-appear-across-ugandan-capital-kampala-1.3993297 (accessed 23 June 2020).
26 BH Oluka 'Govt spends Shs 200bn on spying gadgets' *The Observer* 19 October 2015, https://www.observer.ug/news-headlines/40521-govt-spends-shs-200bn-on-spying-gadgets (accessed 20 May 2020).
27 Privacy International *For God and my president: State surveillance in Uganda* (2015) 6.

Swahili).[28] The latter, if infected into a device, arguably is capable of remotely monitoring a person's activities in real-time, including accessing passwords, files, microphones and cameras without the person's knowledge.[29] The above surveillance apparatus provided by Huawei is not regulated by the Regulations of Interception of Communications Act (RICA) or any law in the land, whereas they are being planted across the country without any accountability or oversight.

Consequently, President Museveni was re-elected to power for the fifth time, since 1986, with widespread evidence showing gross manipulation of the electoral process through vote buying and misuse of state funds.[30] The Activists for Change (A4C) embarked on a peaceful protest against this to draw the government's attention to the police brutality and the rising cost of living, but the government reacted violently. This resulted in the killing of nine unarmed people, with 100 injured, and more than 600 detained without charge.[31] Members of parliament and opposition leaders were also arrested, detained and placed under 24 hours' surveillance.[32]

However, this is a common practice in the country: Uganda has become infamous for its anti-opposition crackdowns and protest practices in the region for many years.[33] In 2011, a full 'Fintrusion suite' was allegedly purchased by the CMI and the (UPF) to strengthen their intelligence system, to enable monitoring of dissent, and all those who oppose the President during the elections.[34] Therefore, the FinFisher malware was ostensibly secretly infected into the communication devices of members of the opposition, activists, journalists, media houses and establishment insiders.[35] This

28 Privacy International, https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda (accessed 20 May 2020).
29 As above.
30 A Oba 'Human rights concerns in Museveni's Uganda' (2005) 47 *Journal of the Indian Law Institute* 351-360.
31 Privacy International (n 28).
32 S Kafeero 'Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests' *Quartz Africa* 27 November 2020, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/ (accessed 15 May 2021).
33 S de Vogel 'Anti-opposition crackdowns and protest: The case of Belarus, 2000-2019' (2022) 28 *Post-Soviet Affairs* 9-25.
34 Privacy International, https://privacyinternational.org/press-release/1036/ugandan-government-deployed-finfisher-spyware-crush-opposition-track-elected (accessed 21 May 2020).
35 Unwanted witness 'State of digital rights in Uganda 2019, surveillance and democracy: Uganda's chilling tales, https://www.unwantedwitness.org/surveillance-is-prejudicial-to-ugandas-democracy-says-unwanted-witness-report/ (accessed 3 June 2023).

allegedly was attained through several bribes to gain access to the communication devices of the targets.[36]

It is alleged that the secret government documents accessed by Privacy International revealed further that malware access points were installed in parliament, prominent government institutions, private homes of suspected government opponents and 21 hotels.[37] The latter was installed in the form of fake Local Area Networks (LANs) and wireless hotspots, after bribing all those who cooperated to give access. The main objective behind using the intrusive surveillance on the citizens is to obtain their personal information, monitor their activities to be able to intimidate, manipulate, blackmail and execute citizens in order to keep them silent.[38]

Although strengthening intelligence systems in Uganda may be considered inevitable in light of previous experiences, it is of concern when the intelligence apparatus is consistently and inappropriately used against civilians;[39] that is, where used to monitor citizens for political reasons with the aim of turning them into docile citizens in a democratic state.[40] This contravenes the Constitution, which upholds democratic principles, and the policy of zero tolerance for opposition while ensuring prolonged rule by a single individual is a serious affront to democracy. Article 221 of the 1995 Constitution requires all security forces to observe and respect human rights and freedoms in the performance of their functions. This implies that all security forces in the country should operate under civilian authority and be accountable to parliamentary oversight.[41]

4 Legal framework for communication surveillance in Uganda

Despite the absence of universal treaties on communications surveillance and cyber terrorism, as in other countries, Uganda has resorted to the reinforcement of national intelligence security

36 As above.
37 J Parkinson and others 'Huawei technicians helped African governments spy on political opponents' *The Wall Street Journal* 15 August 2019.
38 Agaba (n 22) 41-60.
39 R Kagungulu-Mayambala 'Examining the nexus between ICTS and human rights in Uganda: A survey of the key issues' (2009) International Workshop on The Nexus Between ICT and Human Rights, Human Rights and Peace Centre, Faculty of Law, University of Makerere 16.
40 R Kakungulu-Mayambala 'Phone-tapping and the right to privacy: A comparison of the right to privacy in communication in Uganda and Canada' British and Irish Law Education and Technology (BILETA) Conference, Law shaping technology: Technology shaping the law, Glasgow Caledonia University (2018).
41 The Constitution of the Republic of Uganda, 1995, art 221.

systems facilitated by intrusive technologically-enabled surveillance systems. These are regulated by a blend of several pieces of cyber legislation, such as the Anti-Terrorism Act (ATA);[42] the Computer Misuse Act (CMA);[43] the Electronic Transactions Act (ETA);[44] the Uganda Communications Act (UCA);[45] and the Regulations of Interception of Communications Act (RICA).[46]

As its name suggests, the ATA aims at suppressing terrorism at domestic level and essentially ensuring that perpetrators are brought to justice. The Act defines crimes of terrorism and prescribes punishment for planning, instigating, supporting, financing or executing acts of terrorism. In recognition of changing times, the Act also enables the investigation of terrorism through monitoring and surveillance, including the monitoring of bank accounts, emails, telephone calls and other cybercrime-related acts.[47]

RICA is the main law for communications surveillance aimed at strengthening national security in Uganda. It gives effect to the provisions of communications surveillance under ATA and CMA above, by enabling and governing their operations. It plays a significant role in investigating, deterring and curbing cybercrime and maintaining national security through communications surveillance on a wider scale, underscoring its relevance to this article.

5 Protection of the right to privacy and free speech under the Ugandan legal regime

Article 27 of the Constitution of Uganda guarantees an inherent right to privacy of homes, properties, bodies, correspondence, communications or other property.[48] The law proscribes unlawful entry into and searching of people's dwellings, premises, their persons or other property. Additionally, the government passed the Data Protection and Privacy Act (DPPA) in 2019 to give effect to data privacy, which falls under article 27(b) of the Constitution. Accordingly, section 10 of DPPA proscribes data collection, processing and controlling in a manner that encroaches upon the privacy of data subjects.

42 Act 14 of 2002.
43 Act 2 of 2011.
44 Act 8 of 2011.
45 Act 1 of 2013 secs 79 & 80.
46 Act 18 of 2010.
47 Act 14 of 2002 Preamble.
48 Art 27 Constitution of the Republic of Uganda, 1995.

Equally, articles 29(1)(a) and (b) of the Constitution provide protection for free speech, which include freedom of the press and other media, freedom of thought, conscience and belief, and academic freedom in institutions of learning.[49] The digital free speech has also recently been affirmed by the Constitutional Court in the case of *Karamagi & Another v Attorney-General*.[50]

5.1 Limitation of rights in Uganda: National security as an admissible ground

According to Ugandan law, despite the explicit protection of data privacy, as with other rights above, privacy rights and freedoms are not absolute, and may be limited in a legally justifiable manner according to the prescriptions of the law. While article 43 of the Constitution explicitly forbids stifling of any of the chapter 4 fundamental rights, freedoms and public interests, article 43(2)(c) allows the rights to be limited for public interest purposes. However, public interest shall not include political persecution,[51] detention without trial,[52] and any limitation must not exceed what is reasonable and demonstrably justifiable in a free and democratic society, or what the Constitution permits.

The implementation of the Ugandan Constitution is driven by values such as democracy and accountability, among others. It also borrows from the Lockean social contract theory[53] by recognising that all authority in the state emanates from the people of Uganda who shall be governed through their will and consent.[54] Furthermore, it stipulates that '[p]ublic offices are held in trust for the people, and those in authority shall be answerable to the people, and all measures shall be taken to combat and eradicate corruption, abuse or misuse of power'.[55]

Article 20 of the Constitution also cements the protection of the rights and freedoms of individuals, and the obligations of the state to respect, uphold and promote fundamental rights. Above all, the Constitution remains the supreme law of the land which legally binds all persons and authorities in the country, and any law

49 Arts 29(1)(a) & (b) Constitution of the Republic of Uganda, 1995.
50 Constitutional Petition 5 of 2016 [2023] UGCC 2.
51 Art 43(2)(a) Constitution of the Republic of Uganda, 1995.
52 Art 43(2)(b) Constitution of the Republic of Uganda, 1995.
53 A Tuckness 'Locke's political philosophy', https://plato.stanford.edu/entries/locke-political (accessed 20 May 2021).
54 Art 1(1) Constitution of the Republic of Uganda, 1995.
55 Art 1(4) Constitution of the Republic of Uganda, 1995.

or custom incompatible with it shall be voided to the extent of its inconsistency.[56]

Uganda is also a state party to the African Charter on Human and Peoples' Rights (African Charter), the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration on Human Rights (Universal Declaration), which guarantee the right to privacy and other freedoms. By virtue of being a state party to these international legal instruments, Uganda has obligations to protect, promote, fulfil and respect the human rights of people at the domestic level. This encompasses a negative duty to refrain from engaging in any activities, or enacting laws or policies that are inconsistent with these instruments or that contribute to the violation of protected human rights.

Even though international law recognises grounds of national security as a valid ground for the limitation of rights by states, it also prescribes guidance and criteria on how such limitations should be carried out. It prescribes the principles of proportionality and the necessity as the yardstick for limiting rights to curb the chances of unreasonable and unjustifiable erosion of fundamental rights. This is due to the intrusive measures that states often employ to maintain national security, such as communication surveillance. An introduction of the United Nations (UN) Human Rights Council's international principles on the applications of human rights to communications surveillance follows.

5.2 Principle of legality in Uganda's RICA and ATA provisions

Subsequent to witnessing the growing trend of the war of state authorities against civilians through the deployment of repressive surveillance measures, more than 40 international privacy experts, lawyers and civil society actors came together and formulated 'the necessary and proportionate principles' (Principles).[57] The Principles are firmly rooted in established international human rights law and jurisprudence, and they especially guide the formulation and reformation of surveillance laws in line with the rule of law, democracy, international law, and a human rights-based approach.

The Principles further clarify the concept of protected information and define admissible limitations through technology-enabled

56 Art 2 Constitution of the Republic of Uganda, 1995.
57 Electronic Frontier Foundation, https://www.ohchr.org/Documents/Issues/Privacy/ ElectronicFrontierFoundation.pdf (accessed 25 May 2020).

surveillance in a manner that balances competing interests of national security and the exercise of human rights. Although the Principles are non-binding, they have been adopted worldwide by more than 400 organisations, and continue to be used as a basis for interpretation of the protections enshrined under the bill of rights in the digital context.[58]

The Principles comprise 13 sub-principles, namely, legality; legitimate aim; necessity; adequacy; proportionality; competent judicial authority; due process; user notification; transparency; public oversight; integrity of communications; safeguards for international cooperation; and illegitimate access. These will be used as the basis for critical analysis of the Ugandan RICA.

The legality principle provides that states must ensure that the measures employed to limit protected rights are operated in accordance with a clear, precise, accessible and formally codified law. The laws must also have foreseeable effects to enable the governed to accordingly conduct themselves in a lawful manner. In addition, the principle demands the laws to have clear definitions, the scope of applicability of the law, the scope of enforcement and implementation powers, and the admissible scope of limitation of rights through the surveillance measures.[59]

Therefore, the state must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.[60]

However, RICA states that the warrant for interception of communications may be acquired by application to a designated judge and only an authorised person can do so. The latter include the chief of defence forces or a nominee, the director-general of an external security organisation or their nominee, the director-general of an internal security organisation or nominee and the inspector-general of the police or their nominee.[61]

58 The drafting process, led by Access Now, EFF and Privacy International, along with several NGOs, criminal lawyers, human rights advocates and privacy advocates was finalised and published for the first time on 10 July 2013 online at www.necessaryandproportionate.org. 8 (Principles).
59 Principles (n 58) Principle 1 14-18.
60 Principles (n 58) Principle 1 4.
61 Sec 4 Act 18 of 2010.

The list above essentially consists of highly-ranked officers in all the organisations tasked with the maintenance of national security and public order. Despite the offices they hold, they are compelled to submit a written application for warrants of communications surveillance before they proceed with it. This does not apply to cases of urgency or in the existence of exceptional circumstances, rendering normal procedures impracticable in these circumstances. Hence, the designated judge may permit an oral application. The point of significance under this provision is that communications surveillance may not be carried out without a warrant, except if ATA allows it.[62]

The designated judge has the discretion to grant the requested warrant if satisfied that there is a reasonable belief that there is an offence threatening life, or there is a probability that drug trafficking or human trafficking crimes have been, are being or are likely to be committed.[63] Furthermore, a warrant may also be issued where there is reasonable belief that it is necessary to obtain information relating to potential threats to national security, the national economy, public safety, or the state's international relations obligations. However, RICA also grants the designated judge the discretion to issue an order rejecting an application for a warrant or to revoke or amend the warrant issued, if they are of the view that the circumstances so require.[64]

In terms of decoding the above provisions in line with the legality principle, it could be affirmed that efforts to fulfil the first leg of the principle of legality are *prima facie* apparent in the provisions of RICA. Thus, there is an existing codified law regulating communications surveillance and authorising it. The exceptional grounds allowing the practice of surveillance are also stated in the law. However, a closer examination of the law's provisions, particularly the enumerated grounds for permissible surveillance, reveals that they do not meet the second limb of the aforementioned principle, which demands precision, clarity, and intelligibility in the law.

The law uses broad and vague terms such as national security, economic interests, public safety and state international obligations, but fails to further elucidate the ambit and meaning of these terms under the same law for the understanding of the governed.[65] Conversely, the law has made it easier for the government to

62 Act 18 of 2010.
63 Sec 5 Act 18 of 2010.
64 As above.
65 Sec 5(d) Act 18 of 2010.

encroach upon democracy, fundamental rights and freedoms through the deployment of intrusive surveillance facilities behind these vague terms. The use of overly broad terms allows room for misinterpretation and arbitrary enforcement of the law, which may threaten human rights. This situation is further compounded by the law's failure to guarantee adequate safeguards or restrictions on the use of surveillance under the listed legitimate grounds to curb the chances of abuse. The latter renders the listed exemptions incongruent with the principle of legality for lack of clarity and precision.

The revelations above also prove that there are many cases in which the 'public interest card' has been invoked beyond what is reasonably admissible in a free and democratic society. Evidence on the ground also reveals that the problem is not the lack of legal protection for human rights, but a matter of lack of faithful enforcement of the law, rather turning a blind eye to the explicit provisions of the law driven by the lack of political will. The revelations above attest to the existing probabilities of unlimited mass surveillance activities by intelligence security, which implies that they operate in a legal vacuum, as RICA does not regulate them – a situation that also contravenes the principle of legality. The unjustifiable encroaching of the protected fundamental rights, through enforcement of the vague grounds as those listed under RICA above, is unconstitutional and, therefore, should be voided to the extent of their inconsistency.[66]

Similarly, the provisions of ATA may also not pass the legality test. The main issue of concern is the lack of a narrowly tailored definition of terrorism under the Act, for purposes of defining the scope of the legislation. The Act also fails to define prominent terms listed under section 7 such as, *influencing the government, intimidating the public or section of the public*, and it fails to clearly stipulate the degree of damage to persons or property that qualifies as an act of terrorism. Consequently, this gap has fuelled fears of abuse and misinterpretation by security officers. It creates opportunities for expanding 'acts of terrorism' to include democratic movement activities and activism, including democratic actions of freedom of expression advocating change of policies, legal strikes, protests, other forms of association, and trade unions.

Furthermore, the use of vague legal rules is also incompatible with the tenets of a free and democratic society. This is because the

66 Art 2 Constitution of the Republic of Uganda, 1995.

citizenry cannot engage in public debates and participatory legal review over the laws, of which they lack a prudent understanding.

5.3 Principles of adequacy and legitimate aim in RICA

Due to the invasive nature of communications surveillance, the legitimate aim principle requires that the legally admissible use of communications surveillance by authorised officials must be for a valid objective, which directly corresponds with the legally protected interest necessary for a democratic society.[67] Furthermore, the principle proscribes any discriminatory application of the surveillance measures, either towards a group of individuals because of their race, gender, sexual orientation, religion or any other ground of discrimination.[68]

To further elaborate on the above, putting people under surveillance who are in the process of instigating terrorist attacks, or planning to commit crimes in a country, may be considered a legitimate aim necessary to counter the plans of such perpetrators, which is essential to ensure the national security of a democratic state.[69] Terrorism remains a great enemy for democracies, and due to the systemic instabilities it causes in a country, it is considered a legitimate aim allowing for the use of repressive measures such as communication surveillance to suppress it.[70] However, countering terrorism may not always be used as a leeway to unjustly use communication surveillance on the people. This is because these measures have a repressive impact on constitutional rights and freedoms.[71] According to international law, adherence to human rights law by states when effecting counter-terrorism measures is not a mere option for states or a recommendation, but an obligation.[72]

While it remains an international law obligation for democratic states to guarantee adequate national security for their people and to invoke the right of self-defence against heinous attacks,[73] combating terrorism may only be considered a legitimate aim if it is imminent. Hence, there is a need for sufficient evidence to be

67 Principles (n 58) Principle 2 18.
68 As above.
69 P Margulies 'The NSA in global perspective: Surveillance, human rights, and international counterterrorism' (2014) 82 *Fordham Law Review* 2137.
70 AKK Mukwaya 'The politics of international terrorism in the security complexes in the Greater Horn of Africa: An overview from Uganda under the Movementocracy' (2004) 7 *African Journal of International Affairs* 35–56.
71 *Bureau of Investigative Journalism and Alice Ross v The United Kingdom* 62322/14*; 10 Human Rights Organisations & Others v The United Kingdom* 24960/15.
72 Yusuf (n 6). See also CCPR/CO/75/NZL, para 11 (2002).
73 Art 51 Charter of the United Nations, 1945.

adduced to prove that, not mere subjective assumptions based on unfounded allegations. Furthermore, communication surveillance will also not satisfy the legitimate aim requirement if it is applied only to certain groups of people such as foreigners, or sexual and religious minority groups in the country.[74] The latter rather qualifies as a form of discrimination prohibited under international law. In addition, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has asserted that the legitimate aim of national security should rather be restricted to situations where the whole nation's security is at risk.[75] Thus, it is not for individual persons, government regimes or power groups.[76] This is meant to reduce the chances of governments taking advantage while using national security as a scapegoat.[77]

Accordingly, Ugandan law does not prescribe surveillance over minorities or of people belonging to opposition parties. However, there have been revelations about the rolling out of the pervasive spyware in the country targeting members of the opposition and minority groups in the name of maintaining public order and national security.[78] Such practices clearly are discriminatory and driven by nefarious political agendas that encroach upon several constitutional democratic principles and international law.[79] Hence, any national security or maintenance of order regime having the effect of targeting innocent minority groups and authorising monitoring and surveillance over them, for reasons that they are not citizens, belong to certain political groups, or religious denominations, should be voided for their illegitimacy.[80]

The principle of adequacy, on the other hand, requires that the legally admissible communications surveillance must be an appropriate and effective measure to attain the legitimate aim. There remains scant evidence of the effectiveness of communications

74 T Christakis & B Katia 'National security, surveillance and human rights' in R Geiss & N Melzer (eds) *The Oxford handbook of the international law of global security* (2020) 1-16.

75 United Nations Office of the Commissioner 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2022) A/HRC/35/22.

76 R Kakungulu-Mayambala 'Privacy, data protection and national security: Analysing the right to privacy in correspondence and communication in Uganda' (2009) 25 *Human Rights and Peace Centre, Faculty of Law, Makerere University*.

77 United Nations 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Retreating spaces? Contemporary challenges to freedom of expression' 6 September 2016 UN Doc. A/71/373 para 18.

78 Privacy International (n 34).

79 In Uganda, these laws include the Regulation of Interception of Communications Act, 2010 and the Computer Misuse Act, 2011.

80 Privacy International (n 34).

surveillance in curbing crime, countering terrorism or ensuring national security.[81] Rather, there is an enormous amount of evidence on the negative impacts of communications surveillance on democracies and fundamental human rights.[82] This can be attested by their failure to counter the main event of September 11, despite the US's most widespread pervasive communication surveillance's ability to monitor the entire world.[83]

Uganda has unique problems of its own. Concerns have been raised about the lack of sufficient technical skills in the law enforcement sector in the past, which continue to be proven by the scarcity of recorded data on cybercrimes prosecuted at the domestic level on an annual basis.[84] The government continued to turn a blind eye to the need to train officials to be able to use the apparatus for their official duties, but rather continued to invest public funds in surveillance apparatus for political reasons.[85]

However, despite such intensified surveillance in the country, there is persistent occurrence of insecurities, whereas several sector agencies, both civilian and military, daily collect intelligence. Ugandan society has also begun to question the effectiveness of the ISO, more specifically its task in assisting the local police with the maintenance of law and order. The country continues to experience a wave of vicious murders and kidnappings. In 2017, 28 women were murdered and mutilated, and their naked bodies discarded in different locations. Unfortunately, the lack of intelligence information to facilitate the apprehension of the culprits crippled the whole process. This has left many Ugandans feeling unsafe in their own country.[86] Security forces lack adequate answers for common crimes, organised criminal activities and others while they have been granted the tools and power to ensure national security.[87] To a greater extent this exposes the ineffectiveness of the surveillance apparatus used by the intelligence security for crime control and national security.

81 Principles (n 58) Principle 4 20-22.
82 KD Haggerty 'Ten thousand times larger … Anticipating the expansion of surveillance' in DJ Gool & D Neyland (eds) *New directions in privacy and surveillance* (2009)159-177.
83 G Greenwald *No place to hide: Edward Snowden, the NSA, and the US surveillance state* (2014) 1-10.
84 Overseas Security Advisory Council, Bureau of Diplomatic Security, US Department of State 'US Department of State diplomatic security Uganda 2019 crime and security report', https://www.osac.gov/Content/Browse/Report?subContentTypes=Country%20Security%20Report (accessed 20 July 2021).
85 Oluka (n 26).
86 https://issafrica.org/chapter-one-private-and-public-security-in-uganda-solomon-wilson-kirunda (accessed 20 May 2021).
87 As above.

The above argument can also be applied to mass communications surveillance practices that continue to operate under a legal black hole, mostly used to advance political agendas.[88] The use of bulk surveillance turns every person who owns a communications device into a suspect, raising many questions related to necessity and proportionality. In this case, communication surveillance ceases to be a means to an end but rather an end in itself. It turns from being a measure of control to a form of punishment for civilians which will continue to be feared by everyone and turn society into docile citizens.[89]

Consequently, courts are increasingly shunning mass surveillance practices in democratic states, even when invoked under the pretext of national security or crime control, and are instead favouring targeted surveillance.[90] Equally, the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism also urges states to use targeted surveillance measures to counter terrorism.[91] The latter must be carried out based on a warrant issued by a judge after establishing the factual evidence showing the existence of probable cause or reasonable grounds. Also, there must be tangible proof of an imminent threat in the form of suspicious behaviour of a person targeted, for instance, justifying a reasonable suspicion that they may be engaged in instigating a terrorist attack.[92]

5.4 RICA and ATA and the principles of necessity and proportionality

The fundamental principle of necessity demands that the law must restrict communications surveillance to that which is strictly and demonstrably necessary to attain the legitimate aim. Hence, there should be no other less repressive method capable of effectively producing the same results as the surveillance. The strict necessity for employing communications surveillance must be demonstrable from tangible and objective evidential proof meriting the limitation of rights. This principle also extends to lawfulness in the sense that

88 United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, https://www.ohchr.org/en/issues/terrorism/pages/srterrorismindex.aspx (accessed 23 May 2020).
89 Agaba (n 22).
90 *Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & Others* [2021] ZACC 3. See also *Big Brother Watch & Others v The United Kingdom* (58170/13).
91 The United Nations Special Rapporteur (n 88).
92 As above.

strictly necessary surveillance for a particular legitimate interest can only be employed for a specific period. It cannot continue to be used indefinitely despite the falling away or expiry of the prevailing circumstances or legitimate grounds that made it strictly necessary.[93] Necessity works with time as well: The harvested information from the intelligence processes cannot be retained by the security officers for an unreasonable time; this may trigger chances of abuse.[94]

RICA proscribes communications surveillance without a warrant, except in cases of consent and where the party intercepting communications is a party to the conversation. The Act prescribes a cumbersome procedure for attaining a warrant, which is subjected to thorough judicial checks and balances.[95] According to section 5 of RICA, the designated judge has the discretion to grant or refuse a warrant for surveillance after assessing the evidence filed supporting the application. The judge also has the power to amend the warrant after having issued it or to simply revoke it. The law requires that the warrant may only be granted if the designated judge has established from the facts and evidence provided that a reasonable belief exists necessitating the need to use communications surveillance such as threats to national security or to prevent or detect crime.[96]

RICA prescribes the use of electronic surveillance for serious crimes such as threats to life, drugs or trafficking, national security or economic interests, and to public safety for which the warrant for communications surveillance may be granted.[97] This includes cases where the crime may either be in the process of being committed, may have been committed or is likely to be committed. However, this process makes the filing of evidential proof supporting the application necessary, as the judge relies on it to establish the necessity of granting an order for electronic surveillance. Under these circumstances, the burden of proof lies with whoever alleges and, in this case, it is the authorised law enforcement official. Therefore, the evidential value must carry sufficient weight to cast any possible doubt on the necessity for the usage of surveillance measures and also because the other party would not be present to discredit it. While the Act does not expressly state this, the court's decision to grant a warrant is normally influenced by factors such as whether there are any alternative means less rigorous than electronic surveillance or if it is in the interests of justice to issue such warrants.

93 Principles (n 58) Principle 3 20-22.
94 As above.
95 Sec 5 Act 18 of 2010.
96 As above.
97 As above.

According to section 6 of RICA, the warrant shall only be valid for three months and may be renewed for good cause shown by the authorised person. The above excludes cases considered urgent or exceptional under section 6(2), where the traditional procedures for warrant application may be excused. Under the latter, an oral application may suffice if the judge is of the view that the situation renders the traditional procedures impracticable. However, the law further states that a formal application may then be filed later within 48 hours.[98]

From the above, the law attempted to put in place some safeguards in the form of judicial checks and balances. However, the reasonableness of the time frames for the warrant may still be questioned in line with the principle of necessity. Situations classified as legitimate grounds may expire in a shorter time than the prescribed three months. In addition, the law ought to have provided that where the grounds justifying the use of surveillance cease to exist, the surveillance and the warrant must expire with immediate effect. The effort to consider the need to set time frames on the validity of a warrant in the law marked a progressive step, which could nevertheless be improved.

The crimes listed above may be classified as serious crimes, reasonably necessitating the use of communications surveillance, which is admissible and justifiable in democratic society. This development can be applauded as it is rare for communications surveillance laws in the region.[99] However, the challenge lies in the continued use of vague terminology – such as 'threat to national security' and 'threat to economic interests' – which invites the risk of abuse and misinterpretation. Further, the law remains silent on the handling of the intelligence information harvested, how it should be stored, for how long, and how it should be disposed of, which is an essential ingredient of the necessity requirement. This principle demands that the intelligence information acquired through this means should not be stored, processed and retained longer than necessary. Furthermore, it is necessary for the law to clearly classify the kind of data eligible for processing by the security agencies when conducting search and seizures. Under RICA above, and section 17 of ATA, almost anything is eligible for search and seizure by the security agencies. The law uses vague terms such as 'an article of any kind which could be used for terrorist activities'.[100] This leaves the authorised security officers with wider powers for search and

98 Sec 86 Act 18 of 2010.
99 Basimanyane (n 4).
100 Sec 17 Act 14 of 2002.

seizures, with the potential of severely encroaching upon the human rights of the citizens more than what is necessary in a democratic society.

On the other hand, proportionality demands a balancing exercise between the competing legally protected interests.[101] In the case of communications surveillance practices for national security or public order, the principle primarily focuses on balancing the means employed against the legitimate aim pursued. The two must directly correlate with each other. The principle also discourages the case where the disadvantage of exercising the right outweighs the advantages due to limiting the right. Therefore, the seriousness of the suspected offence must be weighed against the limitation of the privacy rights, and the two must be proportionate to each other.[102] Limitation of the right in this case can also be justified by putting in place adequate safeguards in the process of limiting the right to privacy through communications surveillance.

There should be evidence that the use of communications surveillance on the suspect is the most adequate means to acquire concrete evidence relevant to the case. Primarily, the principle seeks to do away with cases of 'killing a fly with a hammer' where there are other more adequate and less rigorous methods to achieve the same aim.[103]

In cases of the harvesting of intelligence information and data processing, the principle of proportionality works hand-in-hand with the principle of adequacy. It only allows the harvesting and processing of adequate and relevant intelligence information directly correlating with the legitimate aim and only for that purpose. Storing intelligence data for longer periods than necessary and using it for other purposes falling outside the terms of the warrant will be disproportionate and can also have other human rights implications for the targeted person. Additionally, proportionality also needs justification in the form of tangible evidence to prove the seriousness of the suspected crime, and the need for communications surveillance. It also demands that safeguards be put in place to mitigate the repressiveness of the measures used.

From the description above, it could be established that the principle invalidates the practices of indiscriminate bulk harvesting

101 Principles (n 58) Principle 5 20-21.
102 J Sieckmann 'Proportionality as a universal human rights principle' in D Duarte & J Silva Sampaio (eds) *Proportionality in law* (2018) 3-24.
103 Sieckmann (n 102) 3-4.

of intelligence data in the name of legitimate interests. The principle of proportionality indirectly affirms the targeted surveillance over the latter. To be proportionate, only the suspected person who has become the target may be intercepted, not the whole population in the country, and this may only be conducted by the authorised person. Only relevant information directly linking the person to the protected legitimate interest may be accessed, harvested and processed. Such information must only be used for a legitimate purpose. Intelligence data harvested cannot be retained for a longer period than necessary and must be destroyed or returned to the data subjects after use or after expiry of the legitimate aim.

To ensure the effective implementation of this principle, the law must in addition put restrictions on the use of surveillance by authorised officials, and clearly prescribe the boundaries within which the lawful interception may be conducted.[104] Those boundaries should be reasonably proportionate to achieving the legitimate protected aim. RICA requires a warrant of application to state the full particulars of the target if known, as well as the manner of interception to be used. In the case of using the service provider, they are required to comply with the technical requirements specified in the order as strictly as necessary to facilitate the interception.[105] This implies that legally permissible communications surveillance may be conducted only on a specific individual or group of suspects.

In contrast, the revelations above demonstrated that mass communications surveillance has been conducted behind closed doors.[106] Uganda is also listed among the 74 countries that requested access to mass Facebook records of its citizens in 2013.[107] In fact, this implies that these disproportionate practices also operate outside the precept of legality.

The law is also very broad in terms of what may be intercepted, whereas there are no sufficient safeguards. The list under schedule 5 of ATA is very broad and accommodates almost any document. This results in the law centralising powers in authorised officials, enabling them to conduct surveillance over all data connected to the suspect, on their premises, and any data or communication devices linked to them, without consideration of other rights affected in the process. The necessary timeframes for storing the intelligence data or the

104 Principles (n 58) 20-21.
105 Sec 4(3) Act 18 of 2010.
106 Privacy International (n 34).
107 'Facebook: 74 countries sought user data' *Aljazeera* 28 August 2013, https://www.aljazeera.com/news/2013/8/28/facebook-74-countries-sought-user-data (accessed 20 May 2021).

need to dispose of or return it are not mentioned, which may expose people to further derogations of their privacy rights. Furthermore, the law does not prescribe stronger safeguards to balance the limitations of rights to privacy through surveillance means, despite their repressive nature.

5.5 Competent judicial authority and RICA provisions

Given the potential for governments to abuse intelligence systems, the principles further prescribe the need for an impartial and independent judicial organ to oversee the mechanisms.[108] The latter's role is to exercise its democratic role of conducting checks and balances over communications surveillance and interception systems conducted by government officials on civilians. Specifically, they must ensure that due process is adhered to when acquiring warrants for surveillance or interception.[109]

As stated by the Principles, a judicial officer can only be competent to effectively carry out the function in this area provided they have knowledge of surveillance issues, including the technologies used, and their impact on the legally protected human rights. The competence of this judge should be visible from their ability to independently function without fear, favour or prejudice, notwithstanding who is behind the application for a warrant of surveillance brought before them. They should be able to exercise fairness and impartiality when hearing the applications for warrants on surveillance and interception, bearing in mind that the proceedings are brought *ex parte* without the knowledge of the targeted party. Therefore, some applications brought before this court should be refused if there is insufficient evidence proving the existence of a legitimate aim that needs surveillance to be protected or if the correct legal procedures have not been adequately followed.

As with other judiciaries in democratic states, this judicial authority must be separate from the authorities conducting communications surveillance. In sum, they must not be an arm of or be subjected to the control of the executive. In terms of resources, it is also the responsibility of the state to ensure that this arm of the state is sufficiently resourced to be able to independently carry out its functions.[110] Democracy also recognises financial autonomy

108 Principles (n 58) Principle 6 22.
109 As above.
110 A Oluseyi 'The feasibility of judicial autonomy in the face of the Nigerian judiciary reality' (2021) Social Science Research Network, https://ssrn.com/abstract=3924899 (accessed 20 May 2021).

as the main pivot on which judicial independence turns. Courts cannot function independently from the executive if they are not also financially independent.[111] Hence, when drawing up national budgets, sufficient funding must be allocated for the functioning of the courts, including the RICA court, for its effectiveness.[112] In terms of human resources, people with relevant skills must be employed to assist in the administration of this court.

However, RICA does not lay down the procedures of the RICA court or its constitution, and whether or not there should be independent expert advisers. RICA is also not clear as to how the proceedings should be conducted or how an application is brought before the judge.[113] The Act merely speaks of the designated judge appointed by the chief justice to perform the RICA functions, and what should be in the application when brought before the judge.[114] This has left room for a lack of transparency and secrecy in the proceedings of the court.

The impartiality and independence of the court are also difficult to establish due to the lack of information on the functioning of the court and its operations. The reports that the designated judge is required to draft and file with Parliament are not mentioned.[115] Without a prescription for reporting RICA operations by a designated RICA judge who issues warrants, there cannot be accountability. It also remains very difficult to establish the competence of the judges dealing with RICA matters with no accessible detailed reports about the orders and rulings made. This includes information on how many applications have been made, how many were rejected or successful, and an explanation of how the decisions to grant or refuse warrant applications were reached.[116] All that can be established is the highest level of secrecy maintained at this court, which raises an alarm.

111 As above.
112 KS Shapkova 'Judiciary independence, impartiality, the court budget: Understanding outcomes from economic constraints to court performance' (2019) in *Iuridica Prima – 5th International Scientific Conference, Ohrid School of Law, Abuse of the Law and 'Abnormal' Law versus Rule of Law* 91-205.
113 Secs 1 & 4 Act 18 of 2010.
114 As above.
115 Tshwane Principles on national security and the right to information for a discussion of the state authority to withhold information from the public on national security grounds, http://right2infor.org/nationalsecurity/Tshwane_principles (accessed 20 April 2021).
116 Tshwane Principles (n 115) Principles 1 & 2.

5.6 Principles of due process, user notification and transparency

The Principles compel governments to follow due process when limiting rights for legitimate aims through surveillance measures.[117] This is supported by article 2 of ICCPR, which accordingly obliges all state parties to respect and guarantee human rights of everyone in their territories without discrimination.[118] Therefore, states may not interfere with the protected rights of individuals without a lawful, legitimate or necessary cause.

With the above as a foundational basis, due process commands the faithful and consistent application of the laws and processes drafted to guide the limitation of rights through surveillance measures.[119] This should be authorised by a competent, independent and impartial judicial body that will conduct checks and balances on the enforcement authorities.

The courts must grant authorisation for surveillance in accordance with the laid-down rules, regulations and international human rights law standards. They must decide on the most appropriate and suitable restrictions, as well as the manner, place, scope and time limitations over which the surveillance measures should be used upon the targeted person in each given case.[120] While surveillance can be used for serious cases that also require secrecy to avoid defeating the ends of justice, the rule of law and due process, in addition, compel adherence to the rules of natural justice. This includes the right of every individual to be notified of the limitation of their rights, and the right to be heard in a public hearing, with fairness and within a reasonable time. The state, therefore, must accord the victims the right to an effective remedy. This is to allow affected persons the opportunity to challenge the orders for targeted surveillance granted against them, and whether or not the measures were successful.

Due process further requires adequate oversight measures to be applied when granting the orders having the effect of limiting the rights of individuals, especially through surveillance measures, which is essential for reducing arbitrariness in the processes.[121] This may be satisfied by having advisory independent experts, oversight organisations or civil societies tasked with conducting reviews of

117 Principles (n 58) Principle 7 22-25.
118 Art 2 ICCPR.
119 Principles (n 58) Principle 7 22-25.
120 As above.
121 Principles (n 58) Principle 10 27.

the applications and orders granted by the designated judge in order to ensure appropriate limitations of rights in accordance with international human rights standards.[122]

Further, note should be taken of the existence of private surveillance in communities, which makes adequate regulation of this area prominent. States must ensure that the private corporations capable of conducting these practices are held accountable. They should be obligated to uphold the tenets of the rule of law and to respect human rights in accordance with national laws or the UN Guiding Principles on Business and Human Rights Principles on Business and Human Rights (Ruggie Principles).[123] It is also consistent with the due process principle that surveillance measures must be subjected to human rights impact assessments, periodic independent audits, safeguards ensuring adequate user notice and consent, and robust oversight, including public oversight.[124]

However, RICA merely mentions the designated judge, and since the application can only be brought by the authorised officer, who normally is a law enforcement officer, the proceedings remain shrouded in the highest level of secrecy.[125] The fact that the proceedings are brought *ex parte*, and the law fails to provide rights of redress and notification to the targeted persons of the surveillance or interception conducted against them, leaves wider room for bias in the proceedings. The party to be monitored is not granted an opportunity to oppose the application, before or even afterwards, even on cases where the processes have the potential to arbitrarily cause prejudice to them or contravening the rules of natural justice.[126]

While the lack of notification may be excused for intent and purposes of preserving the ends of justice, the persons must at least be notified of their surveillance after a reasonable time has elapsed.[127] They should also have the right to an effective remedy in case they suffered any prejudice resulting from wrongful surveillance conducted on them.[128] The absence of these provisions in the law reveals a lack of willingness on the part of the state to take responsibility for their

122 Congregational Research Service 'Reform of the intelligence surveillance courts: Introducing a public advocate' 21 March 2014, http://www.fas.org/sgp/crs-csc/enitem13327/intel/R43451.pdf. (accessed 20 April 2023).
123 United Nations 'Guiding Principles on Business and Human Rights Principles on Business and Human Rights' (2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (accessed 25 May 2020).
124 As above.
125 Sec 10 Act 18 of 2010.
126 Principles (n 58) Principle 8 25.
127 Principles (n 58) Principle 8 25-27.
128 As above.

actions or to be accountable for unjust human rights breaches. This view is complemented by the legally prescribed weak safeguards and the fewer restrictions on the use of surveillance measures by the enforcement officials on civilians.

The Ugandan legal framework for surveillance does not recognise the need to notify victims, and they are not accorded the right to effective remedies or to be heard in an open, impartial and competent court of law. In fact, the duty of non-disclosure bestowed upon communications service providers and authorised officials compels them to remain quiet at all costs to safeguard the identities of the monitoring agents and ensure confidentiality of the investigation proceedings.[129] RICA states that all interceptions must be carried out in such a way that neither the subject of the interception nor any other person becomes aware of any alterations made to comply with the warrant.[130]

Equally, transparency is one of the cornerstones of democracy and is also included as one of the principles that states must observe when conducting surveillance and monitoring civilians. This principle compels the government to be transparent and effectively engage with citizens about developments that affect them.[131] This implies that they must be informed and consulted about plans to purchase surveillance apparatus, their use, scope, purpose, powers, and their potential impact on their rights as well as the safeguards to be put in place to ensure that they are appropriately utilised.[132]

Transparency also requires adequate reporting and record keeping of warrants and orders issued by the designated court, and those rejected. The reports must be comprehensive and publicly accessible in democratic states. The public must know how many requests have been made before the judge, how many were rejected or granted each year, and the reasons therefor. This helps those tasked with the oversight mandate to efficiently carry out their duties and functions.

Further, taking into consideration the intricacy of communications surveillance and its operations, only a few civilians would understand the technicalities, and the language used in this field. Hence, governments must draft surveillance laws in a manner, terms and

129 Secs 8(1)(h)(ii) & 15(3) Act 18 of 2010.
130 Sec 8(1)(i) Act 18 of 2010.
131 Principles (n 58) Principle 9 27.
132 A Mubita and others 'The importance and limitations of participation in development projects and programmes' (2017) 13 *European Scientific Journal* 241.

language that are easily understandable to people, as stated under the principle of legality above.[133]

On a similar note, service providers are pioneers in the field of surveillance and must be encouraged to publish procedures they follow when conducting surveillance for states.[134] They must ensure that the due procedures are accordingly adhered to and, more importantly, publish records on the surveillance they have conducted for easy access by the public.[135] However, RICA provides the duties of the service provider only, but there is no duty to report.[136]

Importantly, transparency works in tandem with accountability to reduce abuses of human rights and promote observance of the rule of law. They empower civilian oversight practices in a democratic community. However, transparency and accountability remain the taboos when it comes to surveillance regimes and their enforcement. The Ugandan RICA similarly does not prescribe any reporting of surveillance practices, either by the designated judge, law enforcement or communications service providers. The state also unilaterally spends substantial public funds on the surveillance apparatus in a utilitarian manner: Whatever the political leaders deem fit for the public goes without the prior consent of the people. Therefore, there is serious impunity and tyranny in this sector with no clear accountability.[137]

This is why surveillance is referred to as a war against civilians, as no civilian is allowed to know how the apparatus works or how to utilise it, and it is only the private sector and government that have that power and knowledge.[138] This has come to the point of criminalising disclosures by the private sector of any surveillance operations conducted against civilians, behind the cloak of mandatory obligations to uphold the secrecy of the state's critical information and investigations.[139] Almost all the publicly available information about the government surveillance and private surveillance industries has been gathered during the forensic work carried out by non-governmental investigative organisations and academic institutions,

133 Principles (n 58) Principle 1 14.
134 Tshwane Principles (n 115) Principles 1 & 2.
135 As above.
136 Sec 8 Act 18 of 2010.
137 Unwanted Witness 'Parliament endorses unregulated surveillance amidst risks to human rights' (2022), https://www.unwantedwitness.org/download/Surveillance-State-Parliament-Endorses-Unregulated-Surveillance.pdf (accessed 4 July 2023).
138 Kimumwe (n 1).
139 Kabumba and others (n 3).

such as Citizen Lab, Wiki Leaks and Privacy International.[140] This indicates a clear lack of transparency and accountability over the surveillance operations in the country.[141]

5.7 Integrity of communications and systems

Consistent with the rights-based approach to communication surveillance, the Principles demand that the state should refrain from using the private sector as its extended arm to conduct surveillance practices.[142] States must not compel communications service providers to build surveillance or monitoring measures into their systems to harvest information or conduct interception of communications for the state.[143] This is due to the possibility of breaching the integrity, security and privacy of communications systems, which may have harmful implications for human rights. This supports the reality that information harvested by the private sector without oversight measures and accountability can easily be processed and manipulated, which can result in bad decision making against innocent citizens.[144]

In cases where intelligence information is admissible as evidence in courts, this may prompt abuse, as technologically harvested data may also be tampered with.[145] Critical dissent, members of opposition parties, investigative journalism and activists who oppose leading governments may easily be silenced through wrongful detainment resulting from tampered intelligence evidence for political reasons.[146] Further, the principle denotes that states should refrain from compelling communications service providers to retain information for them. Further, the surveillance and collection of personal data must not be made a conditional attachment to issuing a licence for services provision.[147]

The situation in Uganda, however, is that citizens are compelled to surrender their personal information to the service providers when purchasing sim cards and mobile telephones and other

140 United Nations Human Rights Council 41st session 24 June-12 July 2019 Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development surveillance and human rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.
141 As above.
142 Principles (n 58) Principle 11 28.
143 As above.
144 As above.
145 Sec 7 Act 18 of 2010.
146 R Kakungulu-Mayambala & S Rukundo 'Digital activism and free expression in Uganda' (2019) 19 *African Human Rights Law Journal* 185-189.
147 Principles (n 58) Principle 11 28.

telecommunication services, yet with no legal safeguards as to how this information should be handled, stored, and for how long.[148] RICA states that telecommunications service providers must keep proper records of the personal information of the civilians even when it changes.[149] The above may trigger opportunities for abuse, especially in the current era where data harvesting has become a highly commercialised commodity.

In addition, section 8 of RICA requires communication service providers to have systems that are capable of supporting the lawful interception of communications. They are mandated to install hardwires and software facilities and devices in their systems to always enable the interception of communications.[150] Their services must have the ability to conduct real-time and full-time monitoring, interception of communications,[151] and store call-related information in accordance with section 11 at their own cost.[152] The above demonstrates a significant lack of compliance of Uganda's surveillance law with international law and best practices, which calls for reforms.

5.8 Principle of public oversight and RICA and ATA

As submitted by Gill and Phythian, oversight over intelligence services is a necessity for a democratic country. This ensures the effectiveness of the sector and accountability.[153] It allows overseers to watch over the security sector when carrying out their tasks using rigorous equipment, such as surveillance, to ensure that they do not unjustly threaten the security and lives of individuals in the process.[154] They ensure that the intelligence security operations are conducted in accordance with the rule of law.

In line with the above, democracy demands independent public oversight measures that work in tandem with accountability and transparency. However, communications surveillance raises a battle of interests.[155] On the one hand, the state aims to protect its legitimate interests and, on the other, democracy necessitates the protection of online rights and freedoms, with the central challenge being to strike a proportionate balance between the two. For this

148 Sec 9 Act 18 of 2010.
149 Sec 9(3) Act 18 of 2010.
150 Secs 8(1)(a) & (b) Act 18 of 2010.
151 Sec 8(1)(c) Act 18 of 2010.
152 Sec 11 Act 18 of 2010.
153 P Gill & M Phythian *Intelligence in an insecure world* (2013) 149.
154 Gill & Phythian (n 153)150.
155 Article 19 'The public's right to know: Principles on right to information legislation (2019), https://www.article19.org/data/files/RTI_Principles_Updated_EN.pdf (accessed 13 April 2023).

reason, there is ample need for independent oversight measures in the form of civil society organisations or independent experts in the field to play a watchdog role. They must monitor and evaluate the effectiveness of surveillance and its compliance with the rule of law, social justice, democracy and respect for human rights.[156]

However, public oversight and transparency are intertwined. For the former to be able to effectively function, the government should be transparent regarding the records and all other relevant information on the national surveillance operations. This includes reports on requests made before the RICA judge, the purchase of surveillance apparatus, reports on their effectiveness, and others.[157] Another role played by public oversight in a democracy as far as surveillance is concerned is that it can push the government to keep adequate and correct records, and publish periodic reports.[158] This will make communications surveillance information accessible to the public.

However, RICA contains no provisions on independent public oversight for communications surveillance. Only the designated judge conducts checks and balances on law enforcement, but no one monitors or evaluates orders authorising communications surveillance, despite being brought on an *ex parte* basis.[159] The law does not consider the need for independent experts in the field to advise a designated judge or review the orders granted to ensure that the human rights of civilians are appropriately limited in accordance with the legal precepts. Further, there is no provision on any oversight measures applied during the implementation of the warrants or in the actual carrying out of the communications surveillance operations by the law enforcement and the private sector.[160] Further, the Anti-Terrorism Act (Amendment) of 2015 grants the minister almost unfettered discretion to order mobile communications surveillance without the need to obtain judicial authorisation.[161] Therefore, there is no oversight to ensure strict compliance with the orders. While the need for secrecy is being hailed as a necessary tool for these offices to carry out their mandates, this view expires in democratic settings.

156 N Wegge 'Intelligence oversight and the security of the state' (2017) 30 *International Journal of Intelligence and Counter Intelligence* 687-700. See also 'The role of civic tech in consolidating democracy in Africa', https://www.democracyworks.org.za/the-role-of-civic-tech-in-consolidating-democracy-in-africa (accessed 2 June 2023).
157 Principles (n 58) Principle 9 27.
158 As above.
159 Sec 1 Act 18 of 2010.
160 Secs 4 & 5 Act 18 of 2010.
161 Secs 18(1), 19(4) & (5) Anti-terrorism (Amendment) Act of 2015.

5.9 Safeguards for international cooperation and RICA

The Principles recognise the need for international cooperation in matters of surveillance for legitimate aims such as terrorism, cybercrime and other serious crimes.[162] This is because technology has enabled crimes to be committed in one country with their effects being felt elsewhere and, therefore, assistance from foreign service providers may be required to be able to bring the perpetrators to justice.[163] This is a matter of mutual assistance that should be guided by mutual legal assistance agreements (MLATs) in the form of bilateral treaties or other agreements entered into with other countries.[164]

However, the principle recommends that in cases of such agreements or arrangements, states must apply the available standards between contracting states with greater protections for the individuals.[165] In addition, the principles of dual criminality must be applied where mutual assistance for intelligence data is required for law enforcement purposes.[166] Further, states may not use mutual assistance arrangements to evade compliance with their human rights obligations or domestic legal restrictions on communications surveillance as enshrined under their domestic laws.[167] In accordance with the democratic principles of legality, accountability and transparency, mutual legal assistance processes must be conducted in line with codified agreements. The procedures must be recorded and made publicly accessible, and processes must be subjected to the rules of procedural fairness.[168]

However, RICA makes no mention of foreign assistance. While these may exist, it is impossible to establish their completeness with regard to their compliance with human rights standards, or whether they are faithfully enforced because there is no transparency with regard to these processes. There also is no evidence of any records kept in that regard.

162 Principles (n 58) Principle 12 29.
163 As above.
164 Council of Europe Convention on Cybercrime, 2001, ch III.
165 Principles (n 58) Principle 12 29-31.
166 Principles (n 58) Principle 12 30.
167 Principles (n 58) Principle 12 31.
168 The Right2know 'Stop the surveillance: Activists guide to surveillance under RICA' (2017), https://www.r2k.org.za/wp-content/uploads/R2K-Handbook-Rica-Surveilance-2017.pdf (accessed 3 March 2020).

5.10 Safeguards against illegitimate access

Finally, the Principles recognise the greater chances of abuse of the surveillance systems by the private and public actors, as they are the only parties authorised to conduct surveillance and, therefore, recommend the criminalisation of any unlawful use of state surveillance apparatus by the parties above.[169] In essence, these principles promote accountability, considering the intrusiveness of surveillance apparatus on human rights. After all, no one should be above the law in democratic settings. Public servants remain answerable to the public while the private sector is subject to the rule of law.[170] The principle denotes that the public and private actors must be held both criminally and civilly liable. Additionally, the law must prescribe adequate safeguards to protect the procedural rights of individuals by proscribing admissibility in any proceedings of any evidence acquired contrary to the principles above.[171] Furthermore, states should include in their laws provisions compelling the destruction of or returning to the owner all the information acquired through the surveillance process after having been used for the purpose for which it was granted.[172]

However, the Ugandan RICA's safeguards against illegitimate access are generally weak. There are no legal protections provided for whistle blowers, human rights activists, lawyers and journalists in the Act despite their line of work. All these have the potential to cripple the democratic and human rights movements. The government uses the private sector as its key player in conducting communications surveillance practices with limited oversight and accountability.[173] The law also is not drafted with precision as to whether law enforcement officials and private sector may be held criminally and civilly liable for unlawful interception of communications.[174] Furthermore, the law is silent on mass surveillance practices despite evidence that these are capable of being conducted. Despite many legal inconsistencies, the constitutionality of the Ugandan RICA has not yet been tried or affirmed by the courts.

169 Principles (n 58) Principle 13 31.
170 Constitution of the Republic of Uganda, 1995, political objectives.
171 Principles (n 58) Principle 13 31.
172 Principles (n 58) Principle 13 32-33.
173 Sec 4 Act 18 of 2010.
174 Secs 4 & 9 Act 18 of 2010.

6 Conclusion

The above has demonstrated that the Ugandan surveillance legal regime is defective and in need of legal reforms. The laws contravene the Constitution, the tenet of democracy, social justice and the rule of law to which Uganda subscribes.[175] The safeguards for digital privacy prescribed in the laws are weak and ineffective, while accountability and oversight measures remain at the bare minimum.[176] The laws create impunities for some law enforcement officials authorised to conduct surveillance, as well as the private corporations assisting them, by not adequately regulating their actions.[177] Instead, the practices of surveillance operations are shrouded with the highest level of secrecy. As discussed above, RICA prohibits notifying data subjects; it requires the surrender of personal data to telecommunications service providers and obliges the private communications sector to maintain surveillance capabilities.[178]

Uganda is not among the most technologically advanced countries in Africa but, ironically, the country is being mentioned among those investing heavily in surveillance equipment. Reports and the media continue to report that the government is planning to adopt even more recent and advanced, highly technical and intrusive measures of communications surveillance from Huawei, China.[179] The latter would mean more breaches of the Principles above and, more precisely, the legality principle. Further, as RICA has been in existence for a decade, it is overdue for reforms as new technologies not covered by the law have evolved. Therefore, the study concludes that the Ugandan communications surveillance-enabling laws are draconian.

Civil society and activists need to lobby and strategically litigate to push for the declaration of national security surveillance laws unconstitutional in Uganda and to demand the necessary reforms. A recent best practice in the area is the recent South African Constitutional Court ruling in *Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & Others,*[180] where similar defective provisions were declared unconstitutional and reforms ordered. Furthermore, it is worth noting that the data protection law that Uganda passed in 2019 is more progressive and has adopted

175 Kakungulu-Mayambala & Rukundo (n 146).
176 Sec 15 Act 18 of 2010.
177 Secs 4 & 9 Act 18 of 2010.
178 Secs 8 & 9 Act 18 of 2010.
179 Parkinson and others (n 37).
180 [2021] ZACC 3.

prominent best international practices in the field relevant to the challenges raised under RICA above. Therefore, it would be prudent to align RICA and ATA with the Data Protection and Privacy Act for purposes of consistency.