Regulation of Communications Surveillance and Access to Internet in Selected African States

International Commission of Jurists

Composed of 60 eminent judges and lawyers from all regions of the world, the International Commission of Jurists promotes and protects human rights through the Rule of Law, by using its unique legal expertise to develop and strengthen national and international justice systems. Established in 1952 and active on the five continents, the ICJ aims to ensure the progressive development and effective implementation of international human rights and international humanitarian law; secure the realization of civil, cultural, economic, political and social rights; safeguard the separation of powers; and guarantee the independence of the judiciary and legal profession.

® Report on Regulation of Communications Surveillance and Access to Internet in Africa

International Commission of Jurists
P.O. Box 91
Rue des Bains 33
Geneva
Switzerland

This publication has been produced with the financial support of the Konrad-Adenauer-Stiftung Foundation.
The contents of this publication are the sole responsibility of the ICJ and can in no way be taken to reflect the views of the Konrad-Adenauer-Stiftung Foundation.

Report on Regulation of Communications Surveillance and Access to Internet in Africa

Contents

Acknowledgements

This report is published by the International Commission of Jurists (ICJ) with generous support from KAS Rule of Law Program for Sub-Saharan Africa. The report was drafted by Justice Alfred Mavedzenge with research support from Alison Tilley, Sanja Bornman, Mitchelle Debora Asiyo and Nigel Chidombwe. The final review was conducted by Ian Seiderman. Tanveer Rashid Jeewa proofread and formatted the report.

Preface

Human dignity, transparency, accountability and public participation are important normative values which underpin democracy. These normative values are protected by and activated through the exercise of certain fundamental rights and freedoms. In the context of this publication, these rights and freedoms include the right to privacy, freedom of expression, the right of access to information and freedom of assembly.

Amongst other objectives, the right to privacy is meant to protect human dignity by guaranteeing that certain personal information about individuals is kept private and is not made public without the concerned persons' consent. Through freedom of expression, individuals have the right to express their opinions to contribute towards public policy development or as means to demand accountability from government on any aspect which involves the exercise of public power. The right of access to information places a duty on governments to ensure transparency by making certain information publicly available or by providing certain information upon request. Crucially, access to information also works as a leverage right which can be used to obtain information that is necessary to exercise, protect or enjoy other rights as well as enforce government accountability.

These rights must be realized both offline and in the virtual sphere (online). Access to internet and certain digital information technologies is critical for the exercise of the right of access to information and freedom of expression. Social media platforms such as WhatsApp, Facebook, Instagram and Twitter, have become important platforms for accessing and sharing information or opinions worldwide.

Restrictions on physical human interaction, imposed by many governments around the world as a result of the Corona Virus Disease (COVID-19) pandemic in 2020, further underscored the prominent role that internet and other digital information technologies play in the modern global space, particularly for the exercise of the freedom of expression, the right of access information and the right to privacy. Many people have since turned to the use of the digital space and digital information technologies as means for accessing and sharing information, soliciting public input on various issues, mobilising and organising communities.

Many African States just like the rest of the world, are faced with the rising challenge of combatting organised crimes and terrorism as well as addressing threats against public order. Some governments have resorted to conducting surveillance, intercepting private communications and restricting access to internet, ostensibly as means to gather information needed to combat organised crimes, terrorism and addressing threats against public order. By their very nature, surveillance, interception of

private communications and restrictions on access to internet constitute serious limitations on freedom of expression, the right of access to information, the right to privacy and many other related human rights. Under international human rights law, States have an obligation to respect, protect and fulfill these rights. The imposition of restriction on these rights, including through surveillance, interception of private communications and restrictions on access to internet must meet certain minimum international human rights law standards namely:(a) the restrictions may be imposed only for purposes of protecting legitimate purposes, (b) they must be lawful, (c) they may be imposed only if they are strictly necessary for the protection of legitimate purposes, (d) they must comply with the principle of non-discrimination both in their design and application and (e) they must be proportionate.

This joint publication of the International Commission of Jurists and KAS Rule of Law Program for Sub-Saharan Africa (KAS) identifies the protection gaps that exist in laws in selected seven African States, which allow for the undermining of the enjoyment of freedom of expression, the right of access to information, the right to privacy and other related human rights. These deficiencies in the legal frameworks engender real or potential non-compliance with the legal principles of lawfulness, non-discrimination, necessity and proportionality in the implementation of communication surveillance and internet restrictions in these countries. Selected on the basis of the recent reports of draconian restrictions introduced by their governments and reports of abuse of communications surveillance powers, these countries are Ethiopia, Uganda, Kenya, Tanzania, Zimbabwe, South Africa and Nigeria.

Considering the significance of the freedom of expression, the right of access to information, the right to privacy in holding governments accountable and given the importance of the digital space as a form of civic space, we hope that this publication will be useful to all key stakeholders, particularly the civil society and lawyers in Africa, as a resource for their advocacy. Specifically, KAS and ICJ hope that the findings made in this publication will be used to advocate for the reform of retrogressive laws which are inconsistent with international law standards and by implication which unduly constrain public access to the digital space.

Dr. Stefanie Rothenberger
Director
Rule of Law Program for Anglophone Sub-Saharan Africa

Sam Zarifi
ICJ Secretary General

Methodology

This report was drafted from a research study conducted of existing legislation, international instruments and jurisprudence, policy documents and court decisions on interception of communications and regulation of access to internet. In addition, key informant interviews were conducted with practitioners and experts from the seven countries selected for this study. A total of seven key sources were interviewed to verify some of the analysis generated from the desktop review as well as to provide any other views which they had on the regulation of interception of private communications and access to internet in the seven countries of study. The seven countries are Ethiopia, Kenya, Nigeria, South Africa, Tanzania, Uganda and Zimbabwe.

Background and Introduction

With the generous support of the KAS Rule of Law Program for Sub-Saharan Africa (KAS), the International Commission of Jurists (ICJ) conducted a scoping study to identify the protection gaps that exist in laws in selected seven African States, which allow for the undermining of the enjoyment of human rights such as freedom of expression and information and the right to privacy. These deficiencies engender real or potential non-compliance with the legal principles of lawfulness, non-discrimination, necessity and proportionality in the implementation of communication surveillance and internet restrictions in these countries. Selected on the basis of the geographic spread of both ICJ and KAS's current programming on freedom of expression in sub-Sahara Africa, these countries are Ethiopia, Uganda, Kenya, Tanzania, Zimbabwe, South Africa and Nigeria. Further, these countries have been targeted for this research because of recent reports of draconian restrictions[1] introduced by their governments, which severely undermine human rights including the freedom of expression and the right to privacy.

Under international human rights law, States have an obligation to respect, protect and fulfill the rights to freedom of information and association, and related fundamental freedoms such as freedom of association and assembly. These rights must be realized online and in the virtual sphere as much as much offline.

As the ICJ has consistently emphasized for nearly 70 years "the Rule of Law is inextricably linked to and interdependent with the protection of human rights, as guaranteed in international law and there can be no full realization of human rights without the operation of the Rule of Law, just as there can be no fully operational Rule of Law that does not accord with international human rights law and standards.

Rule of law principles include law made through democratic governance applying democratic processes, transparency, accountability, access to justice, the functioning of a free and pluralistic media and the independence of the judiciary.

The right to privacy is "an expression of human dignity and is linked to the protection of human autonomy and personal identity." It is meant to protect human dignity by guaranteeing that certain personal information about individuals is kept private and is not made public without the concerned persons' consent.[2] In a recent report, the Special Rapporteur on the right to privacy underscored the significance of privacy by noting that:

[1] These are discussed under each country profile.
[2] UN General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) 8 April 1988.

> *[the right to] Privacy enables the full development of the person, while protecting against harms that stunt human development, innovation and creativity, such as violence, discrimination and the loss of the freedoms of expression, association and peaceful assembly.*[3]

Through exercising their freedom of expression, individuals contribute their views to influence and shape public policy development or as means to demand accountability from government on any aspect which involve the exercise of public power.[4] The right of access to information places a duty on government to ensure transparency by making certain information publicly available or by providing certain information upon request.[5]

Crucially, access to information also works to facilitate the exercise and enjoyment of other rights as well as enforce government accountability.[6] For example, in accordance with a State's obligations under the International Covenant on Economic, Social and Cultural Rights, in order to protect the right to health care, people must have access to the relevant information so that they know the steps they need to take in order to protect their health or to seek health care. [7] Similarly, persons' capacity to exercise or enjoy the right to education, the right to a fair trial and other rights in the administration of justice is dependent upon their ability to access the relevant information.

Equally and more generally, the ability of individuals to enjoy the right to political participation, express or contribute their views during policy development or a law-making process is dependent on the information they have regarding the policy, law or practices concerned. Thus, the right to privacy, freedom of expression and the right of access to information compliment the enjoyment of other rights, and advance democratic normative values of human dignity, transparency, accountability and public participation.[8]

For these and other reasons, these rights are protected in both the regional and global treaties and other instruments. Globally, the main instruments

---

[3] See UN Human Rights Council "Report of the Special Rapporteur on the right to privacy" A/HRC/43/52, March 2020 at para 16.
[4] UN General Comment No. 10 Art. 19 (Freedom of expression) 1983.
[5] General Comment No.34: Article 19: (Freedoms of opinion and expression) 2011
[6] Saras Jagwanth and Richard Calland. "The Right to Information as a Leverage Right". *University of Cape Town* (2002)
[7] UN Committee on Economic, Social and Cultural Rights (CESCR), *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12 of the Covenant)*, 11 August 2000, E/C.12/2000/4, available at: https://www.refworld.org/docid/4538838d0.html [accessed 17 July 2020], para 12(b).
[8] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), para 2 and 3

which protect these rights are the Universal Declaration of Human Rights[9] (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[10] They are also protected further both directly and indirectly in specific contexts by economic, social and cultural rights in terms of the International Covenant on Economic, Social and Cultural Rights (ICESCR). Regionally, these rights are protected in the African Charter on Human and Peoples' Rights (African Charter).[11] These instruments are discussed in greater detail later in this section of the report.

The advent of the "Fourth Industrial Revolution" (4IR)[12] has brought with it technological advancements including in artificial intelligence (AI), robotics, communication gadgets and the Internet of Things (IoT). These advancements (especially the communication gadgets and internet) have become important modalities through which the right of access to information and freedom of expression is often exercised. For example, due to increased internet connectivity, social media platforms (such as WhatsApp, Facebook, Instagram and Twitter) have become important virtual platforms for accessing and sharing information or expressing opinions. Reliance on these virtual platforms has increased for many reasons, including as a result of the outbreak of the COVID-19 pandemic.

A number of governments, globally and in Africa, have introduced legal and policy measures to regulate access to and the use of digital information technologies, including access to internet, the use of social media and privacy of electronic communications.[13] These measures come in the form of legislation such as cyber-crimes laws, anti-terrorism laws or communication surveillance laws.[14] For example, in Africa at least 13 States have enacted communications surveillance laws which allow governments to access and monitor private communications and other personal information.[15]

---

[9] See Art 12 and Art 19 of the ICCPR
[10] See Art 17 and art 19 of the ICCPR
[11] See Art 9(2)
[12] The Fourth Industrial Revolution refers to the convergence and complementarity of emerging technology domains, including nanotechnology, biotechnology, new materials and advanced digital production (ADP) technologies. For a more detailed discussion see https://iap.unido.org/articles/what-fourth-industrial-revolution

[13]See report by Access Now as written by Berhan Taye, available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf
[14] Justice Alfred Mavedzenge 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance' (2020) *African Journal on legal studies*, pp 360–390
[15] Some of these laws have been applied during the COVID-19 pandemic to conduct contact tracing. However, there have also been reports of abuse of these laws leading the United Nations Special Rapporteur to issue relevant guidelines reminding States of their obligations. See "UN Resources on Privacy, COVID-19 and the Right to Health" available at https://www.unglobalpulse.org/policy/covid-19-data-protection-and-privacy-resources/. Also see "Draft Recommendation On The Protection And Use Of Health-Related Data (4 October2019), available at

In some cases, governments have resorted to highly restricting or even shutting down internet for prolonged periods of time. For example, in January 2019 the Zimbabwean government shut down the internet for a week in response to mass anti-government protests.[16] In July 2020, the government of Ethiopia shut down internet for two weeks following popular protest actions demanding justice for the killing of Oromo musician, Haacaaluu Hundeessaa.[17] In 2021 in Uganda and Zambia, the government shut down internet in the period towards and after general elections.[18] Cumulatively, since 2019 more than 25 incidents of internet shutdown by governments were recorded in 14 African countries.[19]

In addition to enacting communication surveillance laws and shutting down internet, some governments have suspended access to specific social media or digital information platforms. For example, in 2021 the government of Nigeria took a decision to indefinitely suspend Twitter.[20] The government of Chad suspended access to social media platforms (including WhatsApp, Twitter, Facebook, Instagram, and YouTube) for 472 days between 2018 and 2019. In some States, governments have gone further to introduce laws which require certain categories of social media users to register and obtain license from government as well as pay tax. For example, in Uganda the government has introduced a law which requires social media bloggers to obtain a licence from government and to pay registration fees and tax.[21] In Lesotho, government has published a Bill which seeks to introduce similar requirements.[22]

Governments argue that undertaking restrictive measures such as communication surveillance and shutting down internet is necessary for purposes of protecting "law and order" as well as combatting organized crime and terrorism.[23] The United Nations Human Rights Council,[24] and the

---

https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemorandum1.pdf.

[16] See Aljazeera report available at https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests

[17] See Access Now report available at https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/

[18] https://www.businesslive.co.za/bd/world/africa/2021-01-21-internet-shutdown-for-uganda-election/

[19] These include Benin, Gabon, Eritrea, Liberia, Malawi, Mauritania, and Zimbabwe. See https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[20] See Reuters report available at https://www.reuters.com/technology/nigeria-indefinitely-suspends-twitter-operations-information-minister-2021-06-04/

[21] See Mwesigwa, D. 2021. *Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data.* Available from: https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/

[22] See Media Institute report available at https://zimbabwe.misa.org/2020/10/06/lesotho-proposed-internet-broadcasting-rules-will-stifle-free-speech/

[23] See Justice Alfred Mavedzenge 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance' (2020) *African Journal on legal studies*, pp 360–390

[24] See UN Human Rights Council "The promotion, protection and enjoyment of human rights on the Internet" A/HRC/38/L.10/Rev.1 available at https://undocs.org/A/HRC/38/L.10/Rev.1.

OHCHR, have observed that some of these measures unnecessarily and disproportionately restrict the right to privacy, the right of access to information and freedom of expression, raising the suspicion that these measures are undertaken for political or other improper reasons, rather than for a legitimate purpose under human rights law.

In the following paragraphs, this report summarizes the substantive content of the State obligations regarding freedom of expression, access to information and right to privacy, and identify and demarcate the boundaries of permissible restrictions to these rights.

Freedom of expression and information

All States have an obligation to respect and ensure the right of every individual to freedom of opinion and expression, including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Article 19 of ICCPR is the authoritative international treaty provision which protect these rights. It provides that:

> *1. Everyone shall have the right to hold opinions without interference.*
> *2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
> *(a) For respect of the rights or reputations of others;*
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals.*

The authoritative interpretation of article 19 has been produced by the UN Human Rights Committee, the supervisory body for the ICCPR, in its General Comment 34. The Committee has clarified that protections for freedom of expression and opinion must extend to "political discourse, commentary… on public affairs, canvassing, discussion of human rights, journalism… and religious discourse", including through non-verbal means and "electronic and internet-based modes of expression".[25] The former UN Special Rapporteur on the right to Freedom of expression and opinion has further noted that the internet has become a key means by which

[25] See UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), para 11.

individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the UDHR and the ICCPR.[26]

At the regional level in Africa, freedom of expression and the right of access to information are protected in article 9 of the *African Charter on Human and Peoples Rights (the African Charter)* which states that:

> *(1) Every individual shall have the right to receive information.*
> *(2) Every individual shall have the right to express and disseminate his opinions within the law.*

The African Commission on Human and Peoples' Rights (the African Commission) has interpreted the content and implication of these rights in the *Declaration of Principles of Freedom of Expression and Access to Information in Africa*, adopted in 2019. In particular, the African Commission has noted as follows under Principle 37 of the Declaration:

> *1. States shall facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights.*
> *2. States shall recognise that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.*

Thus, at both the international and African regional law level, access to internet is recognized as a necessary element of the right of access to information and freedom of expression because, internet has become a mechanism through which people communicate their views and obtain information.

The right to privacy

The right to privacy is recognized by the UN General Assembly as "one of the foundations of a democratic society", and a pre-requisite to the free and independent exercise of the rights to expression and to hold opinions without interference.[27] Article 12 of the UDHR and article 17 of the ICCPR are the main international law instruments which protect the right to privacy.[28] States have an obligation under Article 17 (1) to guarantee that

[26] See para 20 of Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, available at https://www.ohchr.org/en/issues/freedomopinion/pages/opinionindex.aspx
[27] UN General Assembly, 'The right to privacy in the digital age', A/RES/68/167 ('A/RES/68/167'), 18 December 2013, Available at: https://undocs.org/A/RES/68/167
[28] Article 17 of the ICCPR reads "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and

"[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

An authoritative interpretation of the scope of the right to privacy as it relates to "the right to privacy in the digital age" can be found in a series of analytical reports issued by the UN Office of the High Commissioner on Human Rights (OHCHR), pursuant to a mandate by the UN Human Rights Council.[29]

At the regional law level, the African Charter does not contain express provisions on the right to privacy. However, the *African Union Convention on Cyber Security and Personal Data Protection* (the Malabo Convention) adopted in 2014 expressly recognizes the right to privacy in the context of the collection and processing of personal information. Article 25(3) of the Convention provides that:

> *In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples" Rights, and other basic rights such as freedom of expression, the right to privacy…*

States have the obligation to respect, protect and promote the freedom of expression, right to privacy and right of access to information. Necessary domestic laws and policies must be enacted to protect these rights and provide remedies when they are violated.[30] However, neither of these rights is absolute and under narrowly prescribed circumstances and for limited and legitimate purposes States may adopt measures that restrict these rights.

Potential limitations on freedom of expression, privacy and access to information

While the freedom of expression, the right of access to information and the right to privacy must be respected and protected, they, like other

---

reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".

[29] See United Nations Human Rights Council "The right to privacy in the digital age (Artificial intelligence)" A/HRC/48/31, September 2021. Also see United Nations Human Rights Council "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests" A/HRC/44/24, June 2020 and United Nations Human Rights Council "The right to privacy in the digital age " A/HRC/39/29, August 2018. Also see United Nations Human Rights Council "The right to privacy in the digital age (Surveillance) " A/HRC/27/37, June 2014

[30] See UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), para 8.

fundamental freedoms, are not absolute rights and may be subjected to narrowly tailored exceptions in limited situations. Article 19(3) of the ICCPR provides that the freedom of expression and right of access to information can be "subject to certain restrictions" but that these restrictions must be provided by law and necessary only for the following legitimate purposes: (i) ensuring respect for the rights or reputations of others, or (ii) protecting national security, public order or public health or morals. In addition, any restrictions must comply with the requirement of non-discrimination.

Equally, these requirements of legality, necessity, proportionality, legitimate purpose, and non-discrimination have been affirmed by the UN Human Rights Council and the Human Rights Committee as applying to restrictions on the right to privacy.[31] In its recent report on the right to privacy the OHCHR noted that:

> *Any interference with the right to privacy must not be arbitrary or unlawful. The term "unlawful" means that States may interfere with the right to privacy only on the basis of law and in accordance with that law. The law itself must comply with the provisions, aims and objectives of the International Covenant on Civil and Political Rights and must specify in detail the precise circumstances in which such interference is permissible….Accordingly, any interference with the right to privacy must serve a legitimate purpose, be necessary for achieving that legitimate purpose and be proportionate. [32]*

These principles are also set out in other regional African instruments. For example, Principle 9 of the *Declaration of Principles of Freedom of Expression and Access to Information in Africa* states that:

> *States may only limit the exercise of the rights to freedom of expression and access to information, if the limitation: (a) is prescribed by law; (b) serves a legitimate aim; and (c) is a necessary and proportionate means to achieve the stated aim in a democratic society.*

This principle is also set out in the AU Declaration on Cyber Security with respect to restrictions on the right to privacy, which may arise as a result of the collection and processing of personal data.[33]Therefore, communication surveillance and any restrictions on access to the internet and digital privacy may only be introduced if they are lawful, necessary,

[31] The Human Rights Committee and the Human Rights Council have both affirmed that the principles of legality, necessity, and proportionality, apply to the right to privacy in the same manner as they do to freedom of expression and other fundamental freedoms.

[32] See United Nations Human Rights Council "The right to privacy in the digital age (Artificial intelligence)" A/HRC/48/31, September 2021, para 8.

[33] See article 13.

and they must be proportionate. The restrictions must be non-discriminatory.

a) Lawfulness

Article 19(3) of the ICCPR expresses the general principle of lawfulness, which mandates that any restriction on a right be provided by law. The UN Human Rights Committee has provided guidance that laws imposing restrictions on the rights to free expression and access to information and the right to privacy must be promulgated with enough precision to enable individuals to adjust their conduct accordingly, and provide relevant guidance to those charged with executing the laws to ensure they can clearly ascertain which kinds of expression fall under restrictions and which do not. Such laws should not allow for "unfettered discretion for the restriction of freedom of expression on persons charged with its execution", and the laws must not otherwise contravene international human rights law or standards.[34]

In addition, decisions to impose these restrictions must be taken only by authorized persons, following all the procedures set out in the law.[35] The circumstances under which such restrictions can be imposed must be clearly set out in the law.[36] For example, as was noted by the OHCHR in its 2014 report,[37] the law must clearly set out circumstances under which communication surveillance may be undertaken and or restrictions on access to internet (for example internet shutdown) may be implemented.

b) Non-discrimination

In terms of article 2(1) and 3 of the ICCPR, States have an obligation to ensure that the rights recognized in the Covenant are accessible to and enjoyed by all individuals within their territory and those subject to their jurisdiction, without discrimination. These rights include freedom of expression, access to information and the right to privacy.[38] Both the design and the implementation or application of the restrictions against these rights must be non-discriminatory. Regarding the principle of non-discrimination as applied to such restrictions, the Human Rights Committee has made clear that these apply to discrimination "on the basis of race,

[34] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), paras 25 and 26.
[35] Ibid. Also see United Nations Human Rights Council "The right to privacy in the digital age (Surveillance) " A/HRC/27/37, June 2014 at para 23.
[36] Ibid.
[37] See United Nations Human Rights Council "The right to privacy in the digital age (Surveillance) " A/HRC/27/37, June 2014 at para 23.
[38] See also United Nations Human Rights Council "The right to privacy in the digital age (Artificial intelligence)" A/HRC/48/31, September 2021, para 9.

colour, ethnicity, age, sex, language, property, religion or belief, political or other opinion, national or social origin, birth, minority, indigenous or other status, disability, sexual orientation or gender identity, or other status."[39]

Necessity and proportionality

Any restriction must be for a legitimate purpose, and, in the express terms of article 19(3) of the ICCPR, must be necessary, and be the least restrictive means, to achieve that purpose. The principles of necessity and proportionality must therefore guide the imposition of communication surveillance and any internet restrictions, even where a legitimate purpose has been identified for such restrictions.

The UN Human Rights Committee clarifies that the test for necessity entails that, limitations cannot be imposed where protection can be provided through other measures that do not restrict fundamental freedoms.[40] The test for proportionality implies that limitations should be proportionate to their function, not be overbroad and be the "least intrusive instrument amongst others to achieve their protective function".[41]

The UN Human Rights Council has further clarified that States seeking to impose limitations on these rights must "demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat".[42] Restrictions must "not put in jeopardy the right itself" and must be implemented narrowly for the legitimate purposes provided for under article 19 of the ICCPR.[43]

These tests for necessity and proportionality, formulated by the UN Human Rights Council, have been underscored by the African Commission on Human and Peoples' Rights in the *Declaration of Principles of Freedom of Expression and Access to Information in Africa* as follows:

> *"To be necessary and proportionate, the limitation shall:(a) originate from a pressing and substantial need that is relevant and sufficient; (b) have a direct and immediate connection to the expression and disclosure of information and be the least restrictive means of achieving the stated aim; and (c) be such that the benefit of protecting the stated interest outweighs the harm to the expression*

[39] See United Nations Human Rights Council General Comment No. 37: The right of peaceful assembly (article 21), 29 June–24 July 2020) at para 25.
[40] Ibid, paras 33 to 35
[41] Ibid, paras 33 to 35.
[42] Ibid, para 35.
[43] Ibid, paras 21 and 22.

and disclosure of information, including with respect to the sanctions authorised."[44]

Applied in the context of communication surveillance and restrictions on access to internet, the test for necessity, therefore, implies that communication surveillance and restrictions on access to internet must not be imposed where there are other means of achieving the legitimate purpose which do not undermine human rights. The proportionality test requires that the law must not permit overbroad powers to conduct communication surveillance or impose access to internet restrictions. Communication surveillance and any restrictions on access to internet may be imposed only if they are the least restrictive means for achieving the stated legitimate purpose; and the law must not permit indiscriminate imposition of restrictions on access to the internet and digital privacy. The duration of these restrictions must not go beyond the existence of the threats. For example, where internet shutdowns or communication surveillance are deemed necessary to address a security threat, these restrictions must be conducted within a defined period of time during which the threat is still to be addressed. In addition, the law must provide for mechanisms for checks and balances when decisions are being made to impose these restrictions. The imposition of the restrictions must be subject to periodic review to ensure adherence to these legal standards.

Procedural safeguards and effective remedies

States have an obligation to establish mechanisms and institutions which provide certain procedural safeguards in order to ensure that the above highlighted standards of lawfulness, necessity, proportionality and non-discrimination are adhered to when restrictions are imposed against these rights. Article 17 (2) of the ICCPR states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their rights. This is achieved through the provision of "*effective procedural safeguards, including effective, adequately resourced, independent institutional arrangements.*"[45] Thus, there must be accessible institutions of oversight with adequate mandate to enforce these legal standards whenever restrictions are imposed. As was noted by the OHCHR in the 2014 report on the right to privacy, *"While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law*."[46] In addition, the laws, policies and decisions which authorize these restrictions must be subject to judicial review by independent and impartial courts with

[44] See article *9(4) of the Declaration of Principles of Freedom of Expression and Access to Information in Africa*

[45] United Nations Human Rights Council "The right to privacy in the digital age (Surveillance) " A/HRC/27/37, June 2014 at para 37.

[46] Ibid.

adequate mandate to grant appropriate relief against any established violations.[47]

In the following sections, this report profiles each of the seven African States studied in this research, by briefly reviewing the main domestic laws governing freedom of expression, access to information and right to privacy in each State and identifying the main gaps in the laws which have potential to undermine adherence to the legal principles of lawfulness, necessity and proportionality in the implementation of communication surveillance and internet restrictions. Each country profile ends with a brief discussion of recommendations. The briefing does not purport to analyze how the laws have been applied in practice.

[47] Ibid. Also see United Nations Human Rights Council "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin", A/HRC/13/37, December 2009 at para 62.

1. Ethiopia

1.1 Main Applicable Laws

The Federal Democratic Republic of Ethiopia (Ethiopia) acceded to the ICCPR on 11 June 1993, and ratified the ACHPR in 1998. It has neither signed nor ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

The **Federal Constitution of Ethiopia**[48] protects the right to privacy,[49] freedom of expression[50] and the right of access to information. It also guarantees freedom of the press and mass media as well as freedom of artistic expression as a separate right, specifically prohibiting any form of censorship and guaranteeing individuals access to information that is of public interest.[51]

There are a number of rules set out in various proclamations[52] regulating both freedom of expression and access to the internet. The **Ethiopian Aviation Security Proclamation**[53] empowers the Security, Immigration and Refugee Affairs Authority and the Federal Police Commission to intercept and conduct surveillance to prevent unlawful acts against aviation institutions and flight safety equipment.

The **Ethiopian Anti-Terrorism Proclamation**[54] of 2020 authorizes the police to conduct surveillance of communications, subject to obtaining prior authorization from a court of law through issuance of a warrant.[55] Where there are urgent terrorism related threats, surveillance is permitted without the court's warrant, but a warrant must be obtained from a designated public prosecutor. Further, in these circumstances, the police are required to notify a court of law within 48 hours of commencing the surveillance. The court may validate, vary, or set aside the warrant issued by the prosecutor.[56]

Communication surveillance is also regulated by the **National Intelligence & Security Re-establishment Proclamation.**[57] This legislation establishes the National Intelligence and Security Service (NISS) of Ethiopia. The Act empowers the NISS to "conduct surveillance, in

[48] Proclamation of the Constitution of the Federal Democratic Republic of Ethiopia. Proclamation No.1/1995
[49] Article 26 of the Constitution
[50] Article 27 of the Constitution
[51] Article 29(3) of the Constitution
[52] Acts of Parliament.
[53] Proclamation No. 432/2004
[54] Proclamation No.1176/2020
[55] Article 42(2) of the Proclamation
[56] Article 42(3) of the Proclamation
[57] Proclamation No 804/213

accordance with court warrant, on any person suspected of criminal activities."[58] The NISS may conduct such surveillance by entering any premises, or employing any other mechanism, including electronic mechanisms.

The **Hate Speech and Disinformation Prevention and Suppression Proclamation** prohibits the dissemination of hate speech and false information through broadcasting, the print or social media, using text, image, audio or video.[59] Hate speech is defined in Article 2 of the Proclamation as including "*speech that deliberately promotes hatred, discrimination or attacks against a person or a discernible group of identity, based on ethnicity, religion, race, gender or disability*."

The **Computer Crime Proclamation**[60] empowers the investigatory organs of the State to request a court warrant to intercept in real-time or conduct surveillance on computer data, data processing service, or internet and other related communications of suspects, to prevent computer crimes and collect evidence related information.[61] The Minister of Justice may also give permission to the investigatory organ to conduct interception or surveillance without court warrant, where there are reasonable grounds to believe that a computer crime that can damage critical infrastructure is, or is about to be, committed.[62] The Minister must then present the reasons for interception or surveillance without court warrant to the President of the Federal High Court within 48 hours, and the president must give an appropriate order immediately.[63]

1.2 Key issues relating to interception of communications and surveillance

There are consistent and credible allegations of the Ethiopian government using surveillance powers not only to combat terrorism and organized crime, but to monitor bloggers, journalists, and members of the opposition as a key tactic in its efforts to silence freedom of expression, including of disfavoured or dissenting voices in the country.[64] Persons or groups who criticize government policies, or who are perceived to be doing so, are often targeted as "anti-peace elements", or "terrorists."[65] It is reported[66] that

[58] Article 8(7) of the Proclamation
[59] Article 4 and 5 of the Proclamation
[60] Proclamation No. 958/2016
[61] Article 24(1) of the Proclamation
[62] Article 24(3) of the Proclamation
[63] Article 24(4) of the Proclamation
[64] See "Ethiopia: New Spate of Abuse of Surveillance" by Human Rights Watch, available at https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance
[65] The Intercept. 2017. *How the NSA Built a Secret surveillance network for Ethiopia*. Available at https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/
[66] The Intercept. 2017. *How the NSA Built A Secret Surveillance Network for Ethiopia.* Available at https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/

the United States National Security Agency (NSA) provides Ethiopia with technology and training on electronic surveillance necessary to combat terrorism. However, the US NSA is said to have established an intelligence facility which is conducting mass surveillance of communications by Ethiopians and their neighbours across the Horn of Africa.[67] These claims were also confirmed by key sources interviewed during this study. The typical methods used in such surveillance on their face are incompatible with the principles of legality, non-discrimination and legitimate purpose because of its alleged indiscriminate nature. The necessity of communication surveillance must be demonstrated on a case-by-case basis and such restrictions must be implemented narrowly and thus, mass surveillance cannot be permitted. [68] Some defenders of mass surveillance have contended that the mere gathering of information is distinct from the use of that information and that collection of information alone does not impair the right to privacy or other rights. This view has been emphatically rejected by human rights law authorities.[69]

The National Intelligence & Security Re-establishment Proclamation (NIS Proclamation) confers a wide range of powers and duties on the NISS, including the power to "follow up and investigate any internal and external activity intended to overthrow the Constitution and the constitutional order unlawfully, threats against the national economic growth and development activities, serious good governance problems and conspiracies, and collect intelligence and evidence and present it to the appropriate body."[70] As indicated above, the NISS may conduct surveillance to this end.[71] However, the Proclamation is silent on what constitutes a "threat to economic growth," "development activities," or "serious good governance problems." This means there is insufficient legal clarity on the criteria under which surveillance may be done, in contravention of the principle of legality. The absence of a strict legal definition of these terms confers overbroad surveillance powers to the authorities and leaves individuals in Ethiopia vulnerable to arbitrary and/or unnecessary surveillance. For instance, any peaceful protest action which seeks to expose government corruption, and which inevitably may be perceived as tarnishing government's image in the eyes of investors may be interpreted as posing a threat to the economic growth or development of Ethiopia. Yet the right to protest, is a protected right as part of freedom expression, association, assembly and political participation and should generally not be a target of State surveillance.

---

[67] The Intercept. 2017. *How the NSA Built A Secret Surveillance Network for Ethiopia.* Available at https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/

[68] UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), para 21, 22 and 35.

[69] See United Nations Human Rights Council "The right to privacy in the digital age (Artificial intelligence)" A/HRC/48/31, September 2021. Also see United Nations Human Rights Council "The right to privacy in the digital age (Surveillance) " A/HRC/27/37, June 2014

[70] Article 8(1) of the Proclamation

[71] Article 8(7) of the Proclamation

The NIS Proclamation provides for oversight in Part IV. Under Article 24, "(t)he Service shall obtain court warrant in order" to carry out digital or other surveillance. This is the full extent of the provisions relating to judicial oversight. It appears that the Act does not provide for criteria that must be applied by the court when determining applications for warrant of surveillance. The law ought to set out objective criteria to be applied on a case-by-case basis in order to determine the necessity of surveillance in each application for a warrant. As has been confirmed by some of the key sources interviewed during this study, the absence of such criteria has led to court sanctioned arbitrary and unnecessary surveillance in Ethiopia.

In addition, the NIS Proclamation does not make any provision for post-surveillance notification to targets, or provide them the right to seek remedial action to challenge the surveillance.. Post-surveillance notification is the principle that those who would have been subjected to surveillance must be informed after the fact, in order to ensure transparency and accountability in the application of these restrictions. Given that an application for a surveillance warrant is made *ex parte*, the target of state surveillance will have no opportunity to become aware that they are, or were, being subjected to surveillance by the State under the Proclamation. Without such information, it will often be impossible for an aggrieved targeted person to exercise any right to legal recourse. Thus, the absence of a mandatory obligation for post surveillance notification undermines individuals' ability to demand accountability from government for arbitrary, unnecessary and/or disproportionate violations of their right to privacy. Key informants who were interviewed during this study identified this problem as one of the key issues which undermine efforts to enforce government accountability for arbitrary state surveillance in Ethiopia.

Further, there is no independent body, established by law specifically to monitor or oversee state surveillance activities and operations. An independent oversight body is necessary for purposes of ensuring State compliance with all the legal standards, including lawfulness, necessity, and proportionality, when exercising powers to impose communication surveillance and other related restrictions.

1.3 Key issues relating to restrictions on access to internet

Internet freedom in Ethiopia has increasingly been restricted over the past two decades as the government continued to adopt aggressive and sophisticated measures that curtail free access to internet to the general public. In addition to adopting repressive policies and laws that effectively criminalize online communication perceived as threatening, the government has resorted to filtering and blocking internet shutdowns to stifle internet freedom. The Ethiopian government has, over the years, implemented multiple and long-running internet network disruptions.

Following uprisings in some regions, the government continuously blocked social media sites and carried out national and regional internet blackouts, often citing "national security threats" or the need to "stem cheating" during national exams as the basis for the disruptions.[72]

The Ethiopian government has ordered internet shutdown pursuant to vaguely formulated laws and regulations. For instance, in 2016 the government issued a State of Emergency Directive which purported to allow the government to block mobile services and internet access. Article 4(2) of the Directive provided that:

> *"When the Emergency Command Post believes that it is necessary for the observance of the constitutional order and for the maintenance of peace and security of the public and citizens, it may cause the closure or termination of any means of communication."*[73]

This Directive[which does not appear to be issued pursuant to a declared state of emergency] did not provide any definition or list of activities that should be deemed as a threat to the constitutional order, peace or national security. It gave the State overbroad powers to shut down internet without setting out clear and objective criteria to be applied and satisfied before such drastic powers can be exercised. Similar directives were issued to authorize internet shutdowns in 2019 and 2020.

A further challenge is that, authorities have often cited national security concerns as a basis to shut down internet during mass anti-government protests. However, they have neither been able to show any evidence that the anti-government protests were a threat to national security, nor that there was no other way of protecting national security without resorting to internet shutdown. Even if there had been such a threat, a full internet shutdown is the most intrusive, rather than least intrusive interference on expression, in patent violation of the principle of proportionality. States seeking to impose restrictions such as internet shutdown to combat threats against national security must "demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat".[74]

---

[72] CIPESA. 2019. *State of Internet Freedom in Ethiopia 2019.* Available from: https://cipesa.org/?wpfb_dl=409 [30 June 2021]

[73] Ayalew, Y E. 2020. *Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights,* African Human Rights Law Journal Vol. 20 No. 1. Available from: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1996-20962020000100013

[74] CCPR/C/GC/34, para 35. UN HR Council

Furthermore, recent internet shutdowns[75] in Ethiopia appear to be disproportionate as they were imposed nationwide including in regions where there were no protest actions, and for inordinately long periods of time. The authorities did not provide any information to the public to demonstrate that such restrictions on access to internet were necessary in those regions where there was no protest action. In 2019, the government shut down the internet for two weeks. No evidence was provided to the public to demonstrate that the length of the period of internet shutdown was proportionate to the existence of any threat to national security. Following the end of this internet shutdown, the government continued to intermittently restrict access to social media platforms such as Facebook, Instagram, and YouTube, as well as messaging applications such as Messenger, the WhatsApp browser client, and Telegram.[76] No official reasons for these subsequent restrictions on social media was offered to the public by the responsible authorities.

1.4 Recommendations

I. The Ethiopian Parliament should promptly review and amend all legislation, including the National Intelligence & Security Re-establishment Proclamation, which provide public officials with overbroad powers to conduct surveillance. The law must be amended to ensure that such powers are provided to be exercised in specific and narrowly defined cases. The law must also be amended to set out objective criteria to be applied on a case-by-case basis in order to determine the necessity of surveillance in each application for a warrant of surveillance. It should establish that powers be exercised with full respect for the principles of legality, necessity, proportionality and non-discrimination. All such legislation must be compliant with Ethiopia's obligations under the ICCPR and ACHPR

II. Parliament should enact a law to provide for a mandatory obligation of the government to ensure post-surveillance notification, as means of providing targets of surveillance with information that is necessary for them to exercise their right to legal recourse and an effective remedy.

III. The legal framework must be amended to provide for the establishment of an independent oversight body specifically mandated to ensure State compliance with all the legal standards, including lawfulness, necessity, and proportionality, when exercising powers to impose communication surveillance and other related

[75]Freedom House.2020. *Freedom in the World*. Available from: https://freedomhouse.org/country/ethiopia/freedom-world/2020
[76] Freedom House. 2020. *Freedom on the Net.* Available from https://freedomhouse.org/country/ethiopia/freedom-net/2020 [1 August 2021]

restrictions. This body, if it is not a judicial body, should be subject to judicial review.

IV. Ethiopia should ratify the Malabo Convention and ensure that its organs comply with the obligations imposed under this Convention, including those relating to the duty of the State to ensure that the collection and processing of personal data through state surveillance powers is done in a manner that complies with international legal standards and is subjected to oversight by an independent body.

V. Specific legislation should be enacted which regulates the imposition of internet restrictions through provisions which safeguard against arbitrary, unnecessary and disproportionate measures. The legislation must confer powers on accountable public authorities to restrict access to internet only for legitimate purposes, as identified in ICCPR article 19(3) and must set out clear and objective criteria to be met before such powers can be exercised, set out mechanisms for ensuring state transparency and accountability whenever such powers are exercised and establish an oversight body to monitor compliance and ensure effective responses against possible abuse of powers.

VI. The responsible authorities should account for recent internet restrictions. In particular, the government must publicly disclose adequate reasons and evidence which demonstrate its claims that recent internet restrictions were lawful, necessary and proportionate to the security threats posed.

2. Kenya

2.1 Applicable Laws

Kenya has ratified the African Charter and acceded to the ICCPR, but has neither signed nor ratified the Malabo Convention.[77]

Kenya's most recent **Constitution** was adopted in 2010. The Constitution protects the right to privacy,[78] freedom of expression[79] and the right of access to information.[80] These rights are expressly subject to limitations. Article 24(1) states that:

> "*A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors including the nature of the right or fundamental freedom, the importance of the purpose of the limitation, the nature and extent of the limitation, the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose".*

The **National Intelligence Service Act**[81] establishes the National Intelligence Service (NIS).[82] Part IV of the Act places limitations on fundamental rights and freedoms, where such limitations are "necessary for purposes peculiar to intelligence services and operations, based on human dignity."[83] This includes limitations on the freedom of expression,[84] the right to privacy,[85] and the right of access to information.[86] However, any limitation of these rights must satisfy the criteria set out in Article 24(1) of the Constitution, and may only be done to: "*ensure the protection, maintenance of and promotion of national security, public safety, public order and protection of the rights and freedoms of others; be necessary to achieve the mandate of the NIS ; be done without discrimination; and be exceptional and not derogate the core or essential content of the right or*

---

[77] Greenleaf, G and Cottier, B 2020 *Comparing African data privacy laws: International, African and regional commitments* Available at: http://www5.austlii.edu.au/au/journals/UNSWLRS/2020/32.pdf [31 July 2021]
[78] Article 31 of the Constitution
[79] Articles 32 and 33 of the Constitution
[80] Article 35 of the Constitution "
[81] National Intelligence Service Act 28 of 2012
[82] Article 4 – 26 of the Act
[83] Article 32(1) and (2) of the Act
[84] Article 33 of the Act
[85] Article 36 of the Act
[86] Article 37 of the Act

freedom being limited."[87] While there is a necessity element in this provision, it is not connected to legitimate purposes for restriction, but rather of ensuring the purposes of the National Service Act.

The **Prevention of Terrorism Act**[88] empowers a police officer above the rank of Chief Inspector of Police to apply *ex parte*, to the High Court, for an order permitting the surveillance of communications, when this is necessary for obtaining evidence of the commission of an offence under the Act.[89] The police require the prior written consent of the Inspector-General of Police or the Director of Public Prosecutions for such an application to be made in court.

In addition to the above laws, there is the **Computer Misuse and Cybercrimes Act,**[90] which establishes the National Computer and Cybercrimes Committee. This Act provides that, where a police officer or an "authorised person" has reasonable grounds to believe that the content of any specifically identified electronic communications is required for the purposes of a specific investigation in respect of an offence, the police officer or authorized person may apply to the court for an order to compel a service provider, within its existing technical capability: (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system.[91]

On 11 December 2020, President Uhuru Kenyatta signed into law an omnibus bill, the **Statute Law (Miscellaneous Amendment Act)**,[92] amending certain aspects of the **Official Secrets Act.**[93] The Statute Law Miscellaneous Amendment Act empowers the Cabinet Secretary of Interior and National Security Coordination to access data from any phone or computer and imposes severe penalties on anyone who refuses to cooperate.[94] Further, the same amendment provides that when it is in the national interest, "...the Cabinet Secretary may apply to the High Court for an order requiring any person who owns or controls any telecommunication apparatus used for sending or receipt of any data, to produce to the Cabinet Secretary or any person named in the order, the original or transcripts of all such data and all other documents relating to such data."[95]

---

[87] Article 32(3) of the Act
[88] Prevention of Terrorism Act 30 of 2012
[89] Article 36 of the Act
[90] The Computer Misuse and Cybercrimes Act 5 of 2018
[91] Article 53 of the Act
[92] Statute Law Miscellaneous Amendment Act 20 of 2020
[93] Official Secrets Act Cap 187 [Rev 2020]
[94] Andere, B. Kenya's sneak attack on privacy: changes to the law allow government access to phone and computer data 27 January 2021 https://www.accessnow.org/kenya-right-to-privacy/
[95] Article 6(1)

The **Statute Law (Miscellaneous Amendments) Act**[96] also amended the **Kenya Information and Communications Act**,[97] to provide for the mandatory registration of telecommunication subscribers and to require mobile operators to maintain a register of all persons to whom telecommunications services are provided under the licence.

The **Data Protection Act**[98] provides for the rights and freedoms of data subjects. It also provides that a data controller must carry out a data protection impact assessment in consultation with the Data Commissioner.[99] The first Data Commissioner was appointed in November of 2020.[100]

The **National Information Communications and Technology (ICT) Policy** is also worth noting. Clause 6.1.3 provides that the state will seek to ensure that high quality internet access is available everywhere in Kenya, and that every Kenyan can afford a device that they can be used to access the internet.[101]

2.2 Key issues relating to interception of communications and surveillance

In recent years, several problematic aspects of these laws have facilitated the abuse or potential for abuse of communication surveillance powers by state officials in the country. In 2017 the Communications Authority of Kenya established the Device Management System (DMS) that uses mobile networks to identify electronic gadgets and their users while also collecting voice and text data.[102] The government argued that the system was necessary for identifying illegal devices.[103] This was challenged in the High Court and the Court ruled that the system would infringe on subscribers' right to privacy and that there were several less restrictive measures that could have been adopted to achieve the purpose sought to be achieved by the Communications Authority of Kenya.[104] However, key sources interviewed during this research argue that there is suspicion that the government has not complied with this order because of the numerous

[96] Statute Law (Miscellaneous Amendments) Act 12 of 2012
[97] Kenya Information and Communications Act Cap 411A [Rev 2011]
[98] Data Protection Act No. 24 of 2019
[99] Section 24 (7) of the Act
[100] Okwara, E. 2020. *Kenya appoints its first ever data protection commissioner.* International Association of Privacy Professionals Available athttps://iapp.org/news/a/kenya-appoints-its-first-ever-data-protection-commissioner/
[101] Gazette Notice No. 5472 of 2020. Available from: https://ca.go.ke/wp-content/uploads/2020/10/National-ICT-Policy-Guidelines-2020.pdf
[102] Global Freedom of Expression. 2018. *Kenya Human Rights Commission v. Communications Authority of Kenya*. Available at https://globalfreedomofexpression.columbia.edu/cases/kenya-human-rights-commission-v-communications-authority-kenya/
[103] At the time, the state expressed concern about the proliferation of counterfeit and stolen devices in the country.
[104] *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others (2018) eKLR*

reports of abuse of state surveillance powers, targeting civil society and opposition activists.

Communications surveillance under the NISS Act is subject to prior authorization by a court of law. The Director General must approach a High Court judge for an order, on an *ex parte* basis.[105] The judge may issue the warrant and may allow for the monitoring of private communication for a month at a time, subject to renewal, taking into account several factors. However, in practice the NISS can directly access data from the telecommunications networks through the Kenyan Communications Authority, under the Information and Communications (Registration of Subscribers of Telecommunications Services Providers) Regulations of 2013, without obtaining prior judicial authorization.[106] These regulations require that each telecommunication provider give the Kenyan Communications Authority access to "its systems, premises, facilities, files, records and other data" for inspection.[107] When requested for such information by the NISS, the Kenyan Communications Authority is required to comply.[108] In this way, the mechanism for prior judicial authorization is effectively circumvented. A key safeguard against arbitrary interference with the right to privacy is an effective, independent mechanism for prior authorization of surveillance measures, except in urgent circumstances where surveillance may commence but subject to a court of law being informed immediately.

There is also no provision in Kenyan law for mandatory post-surveillance notification to targets. Post-surveillance notification is the principle that those who would have been subjected to surveillance must be informed after the fact, in order to ensure transparency and accountability in the application of these restrictions. Without such information, it may be impossible for an aggrieved targeted person to exercise any right to legal recourse. Thus, the absence of a mandatory obligation for post surveillance notification undermines individuals' ability to access an effective remedy and demand accountability from government for arbitrary, unnecessary and or disproportionate violations of their right to privacy.

Through the Computer Misuse and Cybercrimes Act, the government has censored online expression in a manner that is not compliant with the principles of legality, necessity and proportionality. Under this Act, it is a criminal offence to knowingly publish "information that is false in print,

---

[105] Section 42 of the Act

[106] Privacy International. 2019. *The Right to Privacy in Kenya, Stakeholder Report Universal Periodic Review 35th Session.* Available from: https://privacyinternational.org/advocacy/3299/right-privacy-kenya

[107] Section 13 of the Regulations

[108] The Statute Law (Miscellaneous Amendments) Act of 2020 which amended Section 6 of the Official Secrets Act includes a provision that whichever institution or individual fails to comply with the request for interception of communication by the NISS is guilty of an offence and liable to fine not exceeding one million Kenya Shillings or to imprisonment for a term not exceeding one year or both.

broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person."[109] These provisions are formulated in an overbroad manner, and thus, may be abused to punish anyone who publishes information which can be classified as 'calculated to cause panic or chaos'. Any person guilty of this offence can be sentenced to a fine of as much as USD2 159,87 and up to 10 years in prison. The potential punishment is disproportionately severe and creates a chilling effect on the freedom of expression. Key sources interviewed during this study asserted that the mere existence of this law had led to self-censorship amongst certain groups in Kenya for fear of being prosecuted and punished under the Act.[110]

The Kenyan legislature is currently considering enacting the Kenya Information and Communications Amendment Bill. If this Bill as it stands is enacted into law, it will introduce a requirement of mandatory registration and licensing for all users of social media platforms.[111] Such a requirement does not appear to serve any legitimate purpose allowed under ICCPR article 19 (3) and thus raises concerns about its necessity as a restriction on internet freedoms.

2.4 Key issues relating to restrictions on access to internet

Kenya has not experienced internet shutdowns or any known restrictions on the provision of internet services. It appears that access to the digital space in Kenya is threatened by arbitrary censorship, surveillance and clampdowns on disfavoured opinions including political dissent, as discussed above.

2.5 Recommendations

I. Kenya should become party to the Malabo Convention and ensure that its agencies and authorities comply with the obligations imposed under this Convention, including those relating to the duty of the State to ensure that the collection and processing of personal data through State surveillance powers is done in a manner that complies with all the international law and standards and is subjected to oversight by an independent body.

II. Parliament should review and amend the Information and Communications (Registration of Subscribers of Telecommunications

[109] Section 23 of the Act
[110] This law was challenged by the Bloggers Association of Kenya. Unfortunately, the application was dismissed.
[111] Regulation 84IA

Services Providers) Regulations of 2013 and other related laws to ensure that the Kenyan Communications Authority can divulge personal information to third parties (including the national security agencies) only when ordered to do so through a court of law.

III. Parliament should review and amend the Computer Misuse and Cybercrimes Act to decriminalize the sharing or publication of false information. Less restrictive means of protecting the public against disinformation of an administrative rather than criminal nature should be contemplated. These include working with social media service providers to promote verification of information before it is published.

IV. Parliament should enact a law to provide for a mandatory obligation of State authorities to ensure post-surveillance notification, as means of providing targets of surveillance with information that is necessary for them to exercise their right to legal recourse.

V. The Kenyan Legislature should not enact into law the Information and Communications Amendment Bill (of 2019) without substantial amendment, as it seeks to introduce a requirement of mandatory registration and licensing for all users of social media platforms. Such a requirement does not serve any legitimate purpose that would justify the interferences it would pose on the enjoyment of freedom of expression.

3. Nigeria

3.1 Main Applicable Laws

The Federal Republic of Nigeria has ratified the **African Charter** and acceded to the **ICCPR** in 1993. It is not party to the **Malabo Convention**.

Section 37 of the Nigerian **Constitution**[112] protects the right to privacy of individuals, including the privacy of their homes, correspondence, telephonic and telegraphic communications.[113] Sections 39 and 40 of the Constitution guarantee freedom of expression and freedom of assembly respectively. However, these rights are subject to limitations "that [are] reasonably justifiable in a democratic society
(a)in the interest of defence, public safety, public order, public morality, or public health; or (b)for the purpose of protecting the rights and freedom of other persons."[114]

Nigeria has several pieces of legislation that regulate access to the internet and communication surveillance. The **Cybercrimes Act**[115] provides for and regulates the interception of private communication as well as access to computer systems. Where the content of any electronic communication is required for the purposes of a criminal investigation or proceedings, a judge may order a service provider, or authorize a law enforcement officer to intercept, collect, or record specified data.[116]

The **Lawful Interception of Communications Regulations,**[117] which are promulgated by a Cabinet Minister, support the implementation of the Communications Act of 2003. These regulations provide a detailed legal and regulatory framework for the interception of communications. The Communications Act permits any authorized State agent listed in regulation 12(1) to apply before a court for a warrant authorizing the interception of any communication.[118] A judge is only permitted to grant a warrant when it is: in the interest of the national security; for the purpose of preventing or investigating a crime; "*for the purpose of protecting and safeguarding the economic wellbeing of Nigerians; or in the interest of public emergency or safety, or in giving effect to any international mutual assistance agreements*".[119] Any person or licensee who is aggrieved by any interception activity must notify the Communications Commission in writing, and may make a formal application to the Federal High Court for

[112] Constitution of the Federal Republic of Nigeria 1999
[113] Section 37 of the Constitution.
[114] Section 32 of the Constitution.
[115] Cybercrimes (Prohibition, Prevention, ect) Act of 2015
[116] Section 39 of the Act
[117] The Lawful Interception of Communications Regulations of 2019
[118] Section 4 of the Act
[119] Section 7(3) of the Act

judicial review.[120] Every State decision or direction on interception of communications will remain in force until it is set aside by a court of competent jurisdiction, in a final decision of the court.[121]

The **Terrorism (Prevention) Act of 2011** regulates the investigation and prosecution of persons accused of terrorism. Under this Act,[122] the National Security Adviser or the Inspector-General of Police may apply to a court of law for a warrant to intercept private communications for the purposes of investigating a crime related to terrorism. However, state security agencies may intercept private communications[123] without a court warrant, in circumstances where an urgent terror threat is perceived and seeking a warrant would cause a delay which may prejudice the maintenance of public safety. The Attorney-General working together with the National Security Adviser and the Inspector General of the Police is required to compile an annual report of all concluded interception cases.[124] However there is no obligation to publish the report.

The National Information Technology Development Agency has **a framework and guidelines on public internet access** that regulate the provision and use of the internet in Nigeria.[125] The framework and guidelines require internet service providers to grant access to databases of internet users upon request from the National Information Technology Development Agency and/or any other government bodies.

3.2 Key issues relating to interception of communications and surveillance

None of the key legislation[126] regulating the interception of private communications provides for clear and objective criteria to be applied by the courts when adjudicating over applications for warrant of surveillance. They simply require the state security agencies to apply for a warrant from a court of law "for purposes of intelligence gathering", but they do not set out factors to be considered by the court to ensure that surveillance of private communications in those circumstances is permitted only when it is necessary and to the extent that it is proportionate. Under international law, even for purposes of intelligence gathering or in circumstances where information is purported to be needed to protect national security,

[120] Section 20(1) of the Act
[121] Section 20(2) of the Act
[122] Section 29, Terrorism (Prevention) Amendment Act of 2011
[123] With permission from the Attorney General of the Federation. See Section 25 of the Act
[124] See Regulation 19 (3) of the Lawful Interception of Communication Regulations, 2019
[125] National Information Technology Development Agency Framework and Guidelines for Public Internet Access, 2019, section 3. Available at: https://nitda.gov.ng/wp-content/uploads/2020/11/FrameworkAndGuidelinesForPublicInternetAccessPIA1.pdf
[126] Namely the Lawful Interception of Communications Regulations, the Terrorism (Prevention) Act and the Cybercrimes (Prohibition, Prevention, Etc) Act.

restrictions such as communications surveillance may be imposed only if they are demonstrably necessary, and they are the only less restrictive means of addressing the threat. Legislation must provide for clear and objective criteria for the court to establish this before warrants can be issued, and the criteria must be based on the obligation of the state to ensure that restrictions on the right to privacy and freedom of expression are permitted only when they are lawful, necessary proportionate. Alternatively, the courts may develop the criteria through case law. However, there is no known criteria that has been developed by the Nigerian courts on the determination of the application for surveillance warrants, especially given that most of them are made ex-parte.

The Cybercrimes (Prohibition, Prevention, Etc) Act (CC Act) also empowers the President of the Federal Republic , on the recommendation of the National Security Adviser, to designate any computer system or computer network as critical national information infrastructure.[127] Without the need to apply for a warrant from a court of law, state security agencies are permitted to access, monitor, transfer and process data from any computer system or network that has been designated as critical information structure.[128] Thus, the law permits state security agencies to access private personal information contained in these computer systems or networks, without having to demonstrate the necessity and proportionality of such invasion of the right to privacy.

The Communications Act requires that a licensed communications operator (e.g mobile telecommunications companies) must develop the capabilities to intercept and/or allow the interception of private communications on its network.[129] The Act provides for the establishment of the Nigeria Communications Commission.[130] In the interest of protecting public safety or national security, the Act empowers the Nigeria Communications Commission to order any telecommunications operator to intercept private communications and disclose such data to an authorized officer of the state,[131] without a court warrant.
As indicated above, the Act does not provide for clear and objective criteria to be applied by the Commission when determining whether the impairments to the right to privacy in those circumstances would be necessary and proportionate. Even for legitimate purposes, such as the need to protect national security or public safety, restrictions such as communications surveillance may be imposed only if they are demonstrably necessary, and they are the only less restrictive means of addressing the threat. A further challenge is that all the members of the Nigeria Communications Commission ~~is not an independent authority because all~~

[127] Section 3 of the Act
[128] Section 3(2)(c) of the Act
[129] Section 147 of the Act
[130] See section 3 of the Act.
[131] Section 148(1)(c) of the Act

~~its members~~ are "appointed by the President from the 6 geo-political zones of Nigeria subject to confirmation by the Senate".[132] Some of the key sources during this research, said that the members of the Commission are in fact political appointees and their independence is questionable. Decisions to authorize communications surveillance must be made by independent bodies in order to ensure impartiality and objectivity and protect the right to privacy from being subjected to restrictions that are unlawful, unnecessary and/or disproportionate.

Although the Lawful Interception of Communication Regulations 2019 require the Attorney General to compile an annual report of all the concluded communications surveillance cases, there is no legal obligation to publish the report or some of the essential details in that report. In addition, there is no provision of law which imposes the duty on the State to ensure post-surveillance notification to targets. Without knowledge that their right to privacy has been subjected to limitations, it may be impossible for a person to exercise any right to legal recourse. The absence of a mandatory obligation to publish the annual communications surveillance report and the absence of a legal duty to ensure post surveillance notification violates the principle of transparency and undermines individuals' ability to seek an effect remedy and accountability from government for any arbitrary, unnecessary and or disproportionate violations of their right to privacy.

3.3 Key issues relating to restrictions on access to internet

On 4 June 2021, the Nigerian government indefinitely suspended access to Twitter in the country. The government alleged that Twitter was being used to undermine the "corporate existence of Nigeria,"[133] implying that the social media account was being used to promote the disintegration of the federation. However, there is no law which authorizes the suspension of access to internet or social media. The government has not cited any specific law to support its decision to suspend the use of Twitter in Nigeria. The bald claim that Twitter was being used to promote "the disintegration of the Federation", which is vague in itself, was not matched by the government with any evidence which prove the occurrence of any activities targeted at "disintegrating the Federation". Nor of course could any evidence be shown that a shutdown of Twitter was a necessary or proportionate actions in the absence of any such information.

Subsequently, the Nigerian government threatened to arrest and prosecute anyone violating the Twitter ban. This directive was challenged by the Socio-Economic Rights and Accountability Project (SERAP) before the Court of Justice of the Economic Community of West African States (ECOWAS) in

[132] See section 8(1) of the Act

[133] Federal Ministry of Information and Culture. 2021. *Social networking group* (Twitter). 4 June. Available from: https://twitter.com/FMICNigeria/status/1400843062641717249 [18 July 2021]

Registered Trustees of The Socio-Economic Rights & Accountability Project (SERAP) v Federal Republic of Nigeria. The court, on 22 June 2021, gave a preliminary injunction ordering the Nigeria government and its agents "to refrain from imposing sanctions on any media house or harassing, intimidating, arresting and prosecuting the Applicants or anyone for the use of twitter and other social media platforms," pending the determination of the substantive suit filed.[134] As of 29 August 2021, the Nigerian government had not complied with the court order, making the continued suspension of Twitter to be an unlawful restriction on the freedom of online expression.

3.4 Recommendations

I. All legislation regulating communications surveillance should be substantially amended by Parliament to set out objective criteria to be applied on a case-by-case basis by a court of law in order to determine the necessity of surveillance in each application for a warrant of surveillance. In this sense, the Communications Act, the Terrorism (Prevention) Act and the Cybercrimes Act should be reviewed to incorporate strict criteria to ensure that they set out restrictions such as communications surveillance may be imposed only if they are demonstrably necessary, and they are the only less restrictive means of addressing any specific threat.

II. Parliament should amend the Communications Act to ensure that decisions to authorize communications surveillance are made by an independent body (such as a court of law) in order to ensure impartiality and objectivity and protect the right to privacy from being subjected to restrictions that are unlawful, unnecessary and or disproportionate.

III. Parliament should amend the Cybercrimes Act to remove the power of State security agencies to access, monitor, transfer, and process data from any computer system or network that has been designated as critical information structure, without a court warrant. Such powers constitute restrictions to the right to privacy and must be exercised subject to a warrant issued by an independent body in order to ensure that restrictions may only be permitted or imposed if they necessary and proportionate to a legitimate public purpose under article 19(3) ICCPR.

IV. All surveillance laws should be amended to provide for a mandatory obligation of the State to ensure post-surveillance notification and to publish the annual communications surveillance report, as means of

[134] See *Registered Trustees of The Socio-Economic Rights & Accountability Project (SERAP) v Federal Republic of Nigeria ECW/CCJ/APP/23/21*

providing targets of surveillance with information that is necessary for them to exercise their right to and effective remedy and hold the state accountable for any invasion of privacy that may be unnecessary and or disproportionate to a legitimate purpose or otherwise unlawful.

V. The state should ratify the Malabo Convention and comply with the obligations of the Convention, particularly the duty to establish an independent body which monitors and oversees that the collection and processing of personal data is done lawfully and only when necessary and to the extent that it is proportionate.

VI. The Government must end the suspension of twitter in compliance with the decision of the Court of Justice of the Economic Community of West African States (ECOWAS) in the case of *Registered Trustees of The Socio-Economic Rights & Accountability Project (SERAP) v Federal Republic of Nigeria.*

VII. If the government decides to enact legislation regulating access to the internet including the use of social media platforms, such legislation must require government to obtain a warrant from an independent body (such as a court of law) before imposing restrictions. Such legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the state to ensure that restrictions on access to internet are permitted only when they are necessary and proportionate to a legitimate purpose.

4. South Africa

4.1 Main Applicable Laws

South Africa has ratified **the ICCPR** in 1998, and **the African Charter** but neither signed nor ratified the **Malabo Convention.**[135] Freedom of expression, the right of access to information and the right to privacy are guaranteed in the Constitution.[136] These rights are subject to limitation and the conditions to be met by the limitations are set out in section 36(1) of the Constitution as follows:

> *The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including - (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose.*

The **Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA)[137]** is directed at surveillance of communications and requires mandatory SIM card registration by the users. RICA requires that surveillance be authorized by a serving judge who is designated by the President to perform this role.[138] However, in exceptional circumstances of emergency, the police are permitted to intercept private communications without a judicial warrant, but in such cases must notify the designated judge as soon as is practically possible, providing an affidavit with results from the intercepted information and the contents.[139] The judge may ratify or order the surveillance to be discontinued or may make any other appropriate decision after considering whether the surveillance is lawful, necessary and proportionate.[140]

The **National Strategic Intelligence Act[141]** (NSIA) empowers the State security agencies, under the supervision of the Director General (appointed by the President) "to gather, correlate, evaluate and analyse domestic

---

[135] Greenleaf, G and Cottier, B 2020 *Comparing African data privacy laws: International, African and regional commitments* Available at: http://www5.austlii.edu.au/au/journals/UNSWLRS/2020/32.pdf [31 July 2021]
[136] See sections 16, 14 and 32 of the Constitution.
[137] Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002
[138] See Section 16(1) of the Act.
[139] See Section 7(4) of RICA.
[140] In terms of section 36(1) of the Constitution.
[141] National Strategic Intelligence Act 39 of 1994

intelligence, in order to identify any threat or potential threat to the security of the Republic or its people".[142] The Act limits intelligence gathering to only information relating to threats against national security. The Act is silent on whether a warrant is required from a court of law, in cases where intelligence gathering requires communications surveillance. Relying on this legislation, the State Security Agency (SSA) has been conducting bulk surveillance.[143]

The **Criminal Procedure Act[144]** permits the police to conduct surveillance of a criminal suspect, subject to obtaining a court warrant. Under this Act, the police can track and collect the metadata of the communications of a criminal suspect.

The South African Parliament has recently passed the **Cybercrimes Act**,[145] and the President has since signed it into law. Article 29 of the Act gives the police the powers to search and seize articles (including computers or other devices), subject to obtaining a warrant from a court of law "if there are reasonable grounds for believing that an article (i) is within their [police's geographic] area of jurisdiction;[IS THIS "AND" OR "OR"????? (ii) is being used or is involved or has been used or was involved in the commission of an offence—(aa) within their area of jurisdiction; or (bb) within the Republic"

The **Protection of Personal Information Act, 2013** (POPIA Act), which came into effect in July 2021 is aimed at securing the protection of personal information by providing for the establishment of mechanisms that facilitate the lawful processing of personal information. One of these is that the Act creates the Information Regulator as an independent authority, appointed by the President[146] with the mandate to oversee and ensure that the collection and processing of personal information is done lawfully and in compliance with the requirements of the POPIA Act.[147] In terms of section 41(d) of the Act, the Information Regulator has the powers to receive and investigate complaints of violation of privacy of personal information. Pursuant to the investigation and where violations have been established, the Information Regulator may serve the responsible party with a notice to take specific steps to address the violations and or to stop the collection and processing of personal information.[148] The notices issued by the Information Regulator are binding.[149]

---

[142] Ibid, section 2(1)(a)(i).

[143] This was confirmed in the case of *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others 2021 (3) SA 246 (CC)* para 124

[144] See section 205 of the Criminal Procedure Act 51 of 1977

[145] Cybercrimes Act 19 of 2020

[146] And ratified by the Parliament (National Assembly House). See section 41(2) (b) of the Protection of Personal Information Act, 2013.

[147] Ibid, section 40.

[148] Ibid, section 95(1).

[149] Ibid.

4.2 Key issues relating to interception of communications and surveillance

In South Africa there have been reports of systematic abuse of the communications surveillance powers by the State Security Agency (SSA) during the government of former President Jacob Zuma between 2007 and 2017. In 2018, a high-level panel of experts (High Level Panel on the State Security Agency) was appointed by the current President Cyril Ramaphosa to investigate these reports. In its report, the panel confirmed these reports and concluded that there had been "a serious politicisation and factionalisation of the intelligence community." [150] Some of the members of the SSA were found to have unlawfully targeted certain persons for surveillance merely because of their divergent political views.[151] This was found to be in contravention of the Act which limits surveillance powers to be applied only pursuant to the protection of national security.[152] Under both the South African and international human rights law, targeting persons for surveillance because of their political views or beliefs is a violation of the principles of lawfulness and non-discrimination, explained in the above chapter of this report. Among other recommendations, the High Level Panel on the State Security Agency recommended that the perpetrators of illegal surveillance be held criminally accountable. The government is yet to implement this recommendation.

The findings of the high level panel were also echoed recently during a hearing before the Commission established to investigate allegations of State capture. It was reported that under the previous government of former President Jacob Zuma, a special division had been established within the State Security Agency (SSA) to conduct communications surveillance targeted at persons in the judiciary, media, trade unions, civil society, the governing party (ANC) and government officials perceived as opponents to the then President.[153] The surveillance was allegedly conducted without any warrant and it was reportedly done to collect personal information which would be used for smear campaigns against such persons. A high profile witness before the Commission testified that about 24 million South African Rand had siphoned out of the SSA agency's budget to manipulate judges including through targeting them with communications surveillance.[154] The surveillance was targeted mostly at judges who appeared to be handing down judgments that were not in

[150] The Report is available at https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf
[151] Ibid.
[152] Section 2(1)(a)(i) of the National Strategic Intelligence Act 39 of 1994.
[153]See https://www.dailymaverick.co.za/article/2021-01-30-zumas-spy-state-a-decade-of-unfettered-surveillance-secrets-lies-and-lootings-propped-up-by-a-private-army-of-spies/
[154] See https://www.theafricareport.com/62340/south-africa-zuma-spy-allegations-could-splash-ramaphosa-too/

favour of the then President.[155] During the hearings before this Commission, it was also alleged that millions of South African rand were used to bankroll illegal surveillance targeting the then President's political rivals in the ANC ahead of the governing party's 54th elective conference in December 2017.

4.3 Key issues relating to restrictions on access to internet

South Africa has not experienced any internet shutdowns or related restrictions . However, a key source from the telecommunications sector indicated during this study that the standard license agreement between government and internet service providers (ISPs) obliges ISPs to switch off internet if requested by the government to do so without a court order. There is no legislation which sets out procedures for suspending access to internet in South Africa. As was confirmed by one of the sources (who works for a local ISP) during the research, while an ISP can approach the court to challenge the directive to switch off internet on the basis of their duty to respect the constitutional right of freedom of expression, some companies are hesitant to contemplate such a move for fear of political reprisals. This leaves the right of access to internet and freedom of expression vulnerable to arbitrary interference.

4.4 Recommendations

I. Allegations of unlawful and discriminatory, communications surveillance, made during the hearings before the State Capture Commission in 2021 must be thoroughly, promptly and impartially investigated and the perpetrators must be held accountable.

II. The findings of the 2018 High Level Panel on the State Security Agency, relating to the unlawful and discriminatory surveillance by the members of the State Security Agency must be implemented urgently, including the recommendation by the High Level Panel to hold accountable those implicated in illegal communications surveillance.

III. Legislation should be enacted which provides for clear and objective criteria based on lawfulness, necessity and proportionality, to be applied by courts when adjudicating on request to restrict access to internet.

IV. Licensing agreements between government and internet service providers (ISPs) must be amended to ensure that ISPs will only switch off internet if requested by the government to do so and where

[155] Ibid

the request from government is accompanied by a court order or court warrant and the basis of criteria consistent with international human rights law and standards.

5. Tanzania

5.1 Main Applicable Laws

The United Republic of Tanzania (Tanzania) acceded to the **ICCPR** in 1976, and ratified **the African Charter** in 1984. It has neither signed nor ratified the Malabo Convention.

The Tanzanian **Constitution** protects the right to privacy,[156] including as it relates to communication. It also protects the freedom of expression, which notably extends to the right to seek, receive and, or disseminate information; and protection from interference with the confidentiality of one's private communication.[157] However, these rights are qualified by an extensive limitation clause which authorizes limitations for purposes (amongst others) of protecting national defence, public safety, public peace, public morality, public health, promoting national interest, promoting rural and urban planning and the rights of others.[158] There is no express constitutional requirement for the limitations to comply with the international human rights standards of lawfulness, non-discrimination, necessity and proportionality.

The **Tanzania Intelligence and Security Service Act**[159] establishes the Tanzania Intelligence & Security Service (TISS). Without a court warrant but with authorization of the Minister responsible for intelligence and security, this Act empowers the TISS to collect, analyse and retain information and intelligence which relates to activities that may on reasonable grounds be suspected to constitute threats to the national security.[160]

The **Prevention of Terrorism Act**[161] regulates how terror offences are to be investigated and prosecuted. Subject to obtaining a court warrant, section 31(1) of the Act empowers the police to intercept private communications "for the purpose of obtaining evidence of the commission of an offence [of terrorism] under this Act".
The warrant is to be obtained through an *exparte* application which must be authorised by the Attorney-General.[162] The Act also gives the Minister for Home Affairs the power to direct telecommunications and internet service providers to intercept communications without a court warrant,

[156] Section 16 of the Constitution
[157] Section 18 of the Constitution
[158] Section 30 of the Constitution
[159] Tanzania Intelligence and Security Service Act 15 of 1996
[160] See Section 5(1) and Section 14 of the Act
[161] Prevention of Terrorism Act 21 of 2002
[162] Section 31(2) of the Act

whenever this is necessary for the prevention or detection of terrorist crimes.[163]

The **Tanzania Communications Regulatory Authority Act**[164] establishes the Tanzania Communications Regulatory Authority (TCRA) which regulates the operations of communications operators in the country. The **Electronic and Postal Communications Act**[165] regulates the licensing of all electronic and postal communications service providers in Tanzania. In terms of section 59(1) of this Act, the President may, on the occurrence of any event which gives rise to a public emergency, or in the interest of national or public security, authorize the Tanzania Communications Regulatory Authority (TCRA) to order that any postal article, or class of postal articles, from any person or class of persons, or relating to any specific subject be intercepted, without a court warrant.[166] The President may delegate these powers to any other public officer.[167]

The **Cyber Crimes Act**[168] empowers a police officer at the rank of station chief to authorize any law enforcement officer to enter any premises and seize any computer or electronic gadget reasonably suspected to contain data or information needed for criminal investigation, subject to a warrant from a court of law.[169] The Act creates a number of criminal offences including the publication of false information.[170] Where the police reasonably suspect that a person has committed a crime using a telecommunications network, the Act empowers them to seek a court order demanding that the telecommunications operator reveal the identity or information which reveals the identity of the suspect.[171] The court order must be sought through an exparte application. In April 2016, the constitutionality of these powers was challenged [172] on the basis that they allow the State authorities to force service providers to disclose personal data of their users (customers) by virtue of court orders obtained through *ex parte* application, and thus, in violation of the right of their customers and the service providers to be heard. The applicant in this matter had received three notices from police demanding the disclosure of the personal details of anonymous users of its network who had published information exposing corruption at one of the country's leading banking institutions. The police claimed that the information was false and thus these users had committed a crime under the Cyber Crimes Act. The constitutional

[163] Section 30(1) of the Act
[164] the Tanzania Communications Regulatory Authority Act 12 of 2003
[165] Electronic and Postal Communications Act 3 of 2010
[166] Section 56(1)(c) of the Act
[167]See section 59(2) of the Act.
[168] Cyber Crimes Act 14 of 2015
[169] The Act requires a search warrant to be obtained from a court of law (in terms of the Criminal Procedure Act) except in the case of emergencies. See Sections 40 and 41 of the Criminal Procedure Act.
[170] Section 4 – 29 of the Act
[171] See sections 32 and 38 of the Cyber Crimes Act
[172] Jamii Media Company Ltd v. The Attorney General (2017) TLS LR 447

challenge failed when the Court held that the impugned provisions of the Act were not arbitrary and had been lawfully enacted by parliament.[173]

5.2 Key issues relating to interception of communications and surveillance

A major challenge is that various pieces of legislation permit the interception of private communications by State agencies, without a warrant of court. This leaves the rights to privacy and freedom of expression vulnerable to limitations which are not imposed for a legitimate, or are unnecessary and disproportionate to that purpose. For example, under the Tanzania Intelligence and Security Service Act, the Tanzania Intelligence & Security Service (TISS) is authorized to gather personal data including through intercepting private communications without a court warrant, as long as there is reasonable grounds to suspect that a person targeted for such surveillance is engaged or about to engage in activities which constitute threats to the national security.[174] Similarly, section 59(1) and (2) of the Electronic and Postal Communications Act empower the President or any public official delegated by the President to order the interception of private communications in order to protect national or public security, where there is reasonable suspicion that the targeted communications relate to a threat against national or public security. The Cyber Crimes Act empowers a police officer at the rank of station chief to authorize any law enforcement officer to enter any premises and seize any computer or electronic device reasonably suspected to contain data or information needed for criminal investigation, without a warrant from a court of law.[175] Although the right to privacy can legitimately be limited in order to protect national security, the limitations must be lawful, imposed only when they are strictly necessary and they must be the least restrictive means of preventing or addressing the threat. In order to ensure that limitations adhere to these legal standards, it is important that decisions to impose them must be made on a case by case basis with the approval of an independent body (such as a court of law) after an objective consideration of whether the limitations would be lawful, necessary and proportionate in the given circumstances. In case of urgent circumstances, the law may permit interception of private communications without a warrant of court, but a court of law must be notified immediately of the decision to impose these restrictions on one's right to privacy and the court must make a competent order as to whether that decision must be varied or not.

An additional defect is that the law permits State agencies to compel telecommunications operators to disclose personal data of their clients,

[173] Jamii Media Company Ltd v. The Attorney General (2017) TLS LR 447 at para 25
[174] Section 14 of the Act
[175] Section 31 of the Act

without being given the opportunity to defend the rights of their clients, or, critically to allow the targets of such disclosure the opportunity to do so. The Cyber Crimes Act[176] empowers the police to obtain an ex parte court order compelling a telecommunications operator to reveal the identity or information which reveals the identity of a criminal suspect.[177] An exparte application procedure in these circumstances undermines the telecommunications operators' duty to protect the privacy of their clients. Subsequently, their clients' right to privacy is subjected to limitations without respecting their right to be heard which could be exercised through court submissions by the telecommunications operators. This leaves the right to privacy vulnerable to arbitrary and therefore unlawful interference.

There is no provision in Tanzanian law for mandatory post-surveillance notification to targets. Post-surveillance notification is the principle that those who would have been subjected to surveillance must be informed after the fact, in order to ensure transparency, the right to an effective remedy and accountability in the application of these restrictions. Without such information, it will be impossible for an aggrieved targeted person to exercise any right to legal recourse. Thus, the absence of a mandatory obligation for post surveillance notification undermines individuals' ability to access an effective remedy and demand accountability from government for arbitrary, unnecessary and or disproportionate conduct constituting a violation of their rights to privacy and freedom of expression.

There is no provision in the law for the establishment of an independent body with the competency to supervise and ensure that the imposition of restrictions on freedom of expression, access to information and right to privacy is done lawfully and only when such restrictions are necessary and proportionate. The Tanzania Communications Regulatory Authority (TCRA) established in terms of the Tanzania Communications Regulatory Authority Act is mandated to protect the rights of consumers, including their right to privacy and freedom of expression, but it is not an independent body. Its governing board is appointed by the President and the Minister.[178] As confirmed by key sources interviewed during this study, the regulatory authority is made up of political appointees who are subject to influence by the executive in carrying out their functions and this is why the authority has not been able to protect the rights of individuals against arbitrary restrictions. An additional challenge is that the Tanzania Communications Regulatory Authority is not independent because its operations and decisions can be overridden by the Minister. For example, in terms of section 59(1) and (2) of the Electronic and Postal Communications Act, the President or any public official delegated by the President may order the Tanzania Communications Regulatory Authority to intercept private communications in order to protect national or public security, and there is

[176] See sections 32 and 38 of the Cyber Crimes Act
[177] See sections 32 and 38 of the Cyber Crimes Act
[178] See section 7(2) and (3) of the Act

no provision in the law which requires the President or delegated authority to ensure that the orders for interception of communications must meet the requirements of necessity and proportionality. There is also no provision in the law which obliges the Tanzania Communications Regulatory Authority to ensure that the orders to intercept communications meet the standards of lawfulness, non-discrimination, necessity and proportionality before they can be enforced.

5.3 Key issues relating to restrictions on access to internet

The Tanzanian government stifles online freedom of expression through overbroad provisions of law which prohibit the online publication of certain content. For example, the Online Content Regulations of 2020[179] prohibits the publication of any content "against the State and public order including information or rumours for the purpose of ridicule, abuse or harming the reputation, prestige or status of Tanzania." This standard of "against the State" or "harming reputation, prestige or status" is vague and overbroad, in contravention of the principle of legality. There is simply no way an individual could understand how to regulate their conduct to conform with its provisions. In any event, a person should not have to regulate their behaviour because nearly everything that could come under these terms constitute expression that is protected under international human rights law. In terms of ICCPR and the ACHPR, these are not permitted (legitimate) grounds or purposes for the limitation of freedom of expression. Publishing information which may be perceived by the authorities as casting a country in bad light is not a legitimate purposes for which freedom of expression can be limited.

The government, in practice, also acts to stifle access to internet through the imposition of exorbitant, onerous registration and licensing requirements for internet users. The Electronic and Postal Communications Act's Online Content Regulations of 2020 prohibit any person from providing online content services without obtaining a licence from the TCRA.[180] Any person who violates this licensing requirement commits an offence and shall, upon conviction, be liable to a fine of not less than five million shillings (USD 2 156) or to imprisonment for a term of twelve months or both.[181] The registration requirement does not seem to serve any legitimate purpose consistent with article 19(3) ICCPR and thus appears to be an unlawful restriction against freedom of online expression. Furthermore, the sanctions against violating the registration requirement are disproportionate when compared to sanctions imposed against more serious crimes.[182]

[179] See Section 3(a) of the Act
[180] Section 4(1) of the Act
[181] Section 4 of the Act
[182] Serious crimes stipulated in the Penal Code such as public violence in duel or death threats attract six months to 12 months in prison. See Section 88 and 89 of the Penal code.

In addition, the cost of obtaining a license is particularly exorbitant when considered in the light of the average income earnings of Tanzanians. For news and current affairs content, the total cost for a first licence will be as high as USD905, and an additional USD431 must be paid for renewal every three years. For entertainment, education, and religious content, the initial cost is USD 475 and an additional USD215.50 must be paid for renewal every three years.[183] Those who want to stream content on the internet must obtain a simulcasting licence at the initial cost of USD 194, and an additional USD86 must be paid for renewal every three years. These fees are imposed as additional costs to the already high cost of data. In 2019, for example, 1GB of data cost the average person living in Tanzania 5.7% of their monthly income.[184] More than two-thirds of the population in Tanzania live below the internationally recognized income poverty line of USD 1.25 per day.[185] Thus, very few Tanzanians can afford these fees and therefore, they constitute an arbitrary impairment to the exercise of free online expression and the right of access to information. The Human Rights Committee has emphasized the importance of States ensuring access of individuals to communication technologies in order to comply with their obligations under article 19 of the ICCPR.[186]

Restrictions on access to certain social media platforms have also been imposed without a clear enabling law and any evidence to justify such restrictions. For example, in the lead up to the 2020 general elections, Twitter and WhatsApp were throttled and completely blocked on some days.[187] Such restrictions can only be imposed in terms of a published law and when they are necessary and to the extent that they are proportionate. The Tanzania Telecommunications Regulatory Authority asserted[188] that government undertook these measures to protect public order ahead of the elections but has not provided any legal basis for undertaking these measures and has not provided any evidence to justify its claims.

5.4 Recommendations

I. As a general rule, all legislation that provides for possibility of interception and storage of private communications by State agencies must be subject to a warrant by and independent judicial authority.

---

[183]Second Schedule, Online Content Service Fees available at https://businesslicences.go.ug/kcfinder/upload/files/UCC%20fees%20structure.pdf

[184] Canares, M. and Thakur, D. 2019. *Who wins? Who loses? Understanding women's experiences of social media taxation in East and Southern Africa*. Washington DC, Alliance for Affordable Internet. p 3

[185] See https://um.dk/en/danida-en/strategies%20and%20priorities/country-policies/tanzania/current-and-future-challenges-and-opportunities-in-tanzania/

[186] United Nations Human Rights Committee General Comment 34, Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, July 2011, para 15

[187] Freedom House. Freedom in the World: Tanzania. 2021. Available at https://freedomhouse.org/country/tanzania/freedom-world/2021 [27 June 2011]

[188] See https://www.dw.com/en/tanzania-restricts-social-media-during-election/a-55433057

Legislation must set out clear and objective criteria to be applied by public officials and the courts based on the obligation of the State to ensure that restrictions on the right to privacy are permitted only when they are provided in law, necessary and to the extent that they are proportionate to a legitimate purpose recognized in ICCPR article 19(3). In this sense, the Tanzania Intelligence and Security Service Act, and the Electronic and Postal Communications Act must be amended to remove the powers of State agencies to conduct communications surveillance without court warrant.

II. The Cyber Crimes Act must be amended to ensure that applications for court orders by State agencies which seek to compel telecommunications operators to disclose personal data of their clients, are made and adjudicated after hearing submissions from the relevant telecommunications operator and the customer, and after considering whether the disclosure of such information serves any legitimate purpose, is strictly necessary and proportionate. However, in exceptional circumstances where an ordinary court application would defeat the course of justice, the application can be determined exparte or after hearing submissions from the telecommunications operator and after considering whether the disclosure of such information would serve any legitimate purpose, is strictly necessary and proportionate.

III. Legislation should be enacted to provide for the establishment of an independent body that oversees that the imposition of restrictions on freedom of expression, access to information and right to privacy is done in accordance with criteria that spelled out clearly in accordance with the principle of legality and only when such restrictions are necessary and proportionate to a legitimate purpose provided under ICCPR article 19(3). In this regard, the government should move expeditiously to become a party to r the Malabo Convention which specifically calls on States parties to establish an independent oversight body for these purposes.

IV. All surveillance laws should be thoroughly reviewed be amended to provide for a mandatory obligation of the state to ensure post-surveillance notification, as means of providing targets of surveillance with information that is necessary for them to exercise their right to legal recourse and hold the State accountable for any arbitrary and unlawful interference on of privacy in terms of article 17 ICCPR.

V. The Online Content Regulations of 2020 should be amended to remove the mandatory requirement for internet users to register for licenses to publish content.

VI. Government authorities must desist from imposing online and other restrictions that are not based on any law. The illegal blocking of social media in the period towards the 2020 elections must be thoroughly and impartially investigated and those responsible must be held accountable.

VII. Legislation regulating access to internet, including access to and the use of social media platforms, must be amended to require government to obtain a warrant from a judicial authority before imposing restrictions. Such legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the State to ensure that restrictions on access to internet are permitted only when they are clearly spelled out in law, necessary and proportionate to a legitimate purpose under ICCPR article 19 (3).

6. Uganda

6.1 Main Applicable Laws

Uganda ratified **the African Charter** in 1986, and acceded to **the ICCPR** in 1995. It has not ratified the Malabo Convention.

The Ugandan **Constitution** protects the right to privacy,[189] which includes the right not to have one's correspondence and communication interfered with. It also protects the freedom of expression.[190]

The **Regulation of Interception of Communication Act**[191] establishes a Monitoring Centre under the control of the Minister responsible for security.[192] The Monitoring Centre is the sole facility legally designated to conduct legally authorized interception of communications in Uganda.[193] The Act authorizes the Chief of Defence Forces, the Director General of the External Security Organisation, the Director General of the Internal Security Organisation, or the Inspector General of Police (or their nominees) to intercept private communications for purposes of gathering information for the protection of national security, national defence and public safety, subject to obtaining a warrant from a court of law. [194] The warrant will be valid for three months, subject to review on good cause shown.[195] However, the Act does not expressly require the authorities to ensure that the interception of communications complies with the standards of lawfulness, non-discrimination, necessity and proportionality as is required under international human rights law.

The **Anti-Terrorism Act**[196] regulates the investigation and prosecution of persons suspected of terrorist offences. Part VII of the Act provides powers to intercept private communications for purposes of collecting information to "safeguard the public interest, prevent the violation of the fundamental and other human rights and freedoms of any person, prevent or detect the commission of any offence under this Act; or safeguard the national economy from terrorism".[197] A State security officer, duly authorized by the Minister of Internal Affairs can intercept private communications and conduct surveillance for a period of 90 days without a warrant from the court.[198]

---

[189] Section 27 of the Constitution
[190] Section 29 of the Constitution
[191] Regulation of Interception of Communication Act 2010
[192] Section 3 of the Act
[193] Section 3(5) of the Act
[194] Section 4(1) of the Act
[195] Section 2(1) of the Act
[196] Anti-Terrorism Act of 2002, as amended
[197] Section 19(4) of the Act
[198] Ibid

The **Data Protection and Privacy Act**[199] regulates the collection, processing and management of personal data. It is an offence, under the Act, for a third party to disclose personal data without the consent of the owner of that data and or without a competent order.[200]

The **Computer Misuse Act** provides for a range of computer misuse offences, including the unauthorized interception of any function of a computer service.[201] It also provides for the investigation of computer misuse offences.[202] Under the Act, investigative officers may apply to a court of law for an order for the preservation of data[203] or for data to be disclosed.[204] However, there is no provision in the law which obliges the authorities to ensure that such orders meet the standards of lawfulness, non-discrimination, necessity and proportionality as required under international human rights law.

The **Ugandan Communications Act**[205] establishes the Uganda Communications Commission, whose mandate includes monitoring, inspecting, licencing, supervising, controlling and regulating communications services.[206] No person may establish a telecommunications station, provide telecommunications services or construct, maintain or operate telecommunications apparatus without a licence issued by the Commission.[207] All licensees have a duty to ensure that the content that they broadcast is not "contrary to public morality."[208]

6.2 Key issues relating to interception of communications and surveillance

None of the key legislation[209] regulating the interception of private communications provides for clear and objective criteria to be applied by the courts when adjudicating over applications for warrant of surveillance, in contravention of the principle of legality. They simply require the State security agencies to apply for a warrant from a court of law. For example, the Regulation of Interception of Communication Act, authorizes the Chief of Defence Forces, the Director General of the External Security Organisation, the Director General of the Internal Security Organisation, or

[199] The Data Protection and Privacy Act of 2019
[200] Section 35 – 38 of the Act
[201] Section 15 of the Act
[202] Part III: Investigations and Procedures
[203] Section 9 of the Act
[204] Section 11 of the Act
[205] The Ugandan Communications Act of 2013
[206] Section 5(b) of the Act
[207] Section 22 of the Act
[208] Section 29 of the Act
[209] Namely Lawful Interception of Communications Regulations, the Terrorism (Prevention) Act and the Cybercrimes (Prohibition, Prevention, Etc) Act.

the Inspector General of Police (or their nominees) to intercept private communications for purposes of gathering information necessary for the protection of national security, national defence and public safety, subject to obtaining a warrant from a court of law. Similarly, under the Computer Misuse Act, an investigative officer may apply to a court of law for an order for the preservation of data[210] or for personal data to be disclosed.[211]

These pieces of legislation do not set out factors to be considered by the court to ensure that surveillance or interception of private communications or disclosure of personal data in those circumstances is permitted only when it is necessary and to the extent that it is proportionate. Even in circumstances where information is needed to protect national security, restrictions such as communications surveillance or interception of communication may be imposed only if they are demonstrably necessary, and they are the only less restrictive means of addressing the threat. Legislation must provide for clear and objective criteria for the court to establish this before warrants can be issued, and the criteria must be based on the obligation of the State to ensure that restrictions on the right to privacy and freedom of expression are permitted only when they are lawful, necessary and to the extent that they are proportionate to a legitimate purpose under article 19(3) ICCPR. Alternatively, the courts may develop the criteria through case law. However, to the knowledge of the ICJ [and the sources consulted] no criteria or standard has been developed by the Ugandan courts on the determination of the application for surveillance warrants, especially given that most of them are made ex parte.

The Anti-Terrorism Act permits, as a general rule, the interference with one's right to privacy without a court warrant. Under this Act,[212] a State security officer duly authorized by the Minister of Internal Affairs can intercept private communications and conduct surveillance for a period of 90 days without a warrant from the court, for purposes of collecting information necessary to combat or avert terrorism. Although the right to privacy is subject to lawful limitation in order to protect national security and public safety, the limitations must be provided for clearly in law, imposed only when they are strictly necessary and they must be the least restrictive means of preventing or addressing the specific threat. In order to ensure that limitations adhere to these legal standards, it is important that decisions to impose them must be made on a case by case basis with the approval of a judicial or similarly independent body after an objective consideration of whether the limitations would be lawful, necessary and proportionate in the given circumstances.

There is no provision in Ugandan law for mandatory post-surveillance notification to targets. Post-surveillance notification is the principle that

[210] Section 9 of the Act
[211] Section 11 of the Act
[212] Section 19(4) of the Act

those who would have been subjected to surveillance must be informed after the fact, in order to ensure transparency and accountability in the application of these restrictions. Without such information, it may be impossible for an aggrieved targeted person to exercise any right to legal recourse. Thus, the absence of a mandatory obligation for post surveillance notification undermines individuals' ability to access an effective remedy demand accountability from government for arbitrary deprivations of their right to privacy.

There is no provision in the law for the establishment of an independent body that oversees that the imposition of restrictions on freedom of expression, access to information and right to privacy is done lawfully and only when such restrictions are necessary and proportionate. The Ugandan Communications Act[213] establishes the Uganda Communications Commission whose mandate includes protecting the rights of consumers and enforcing compliance with applicable domestic, regional and international standards.[214] Although section 8 of the Act provides that the Commission is independent, the same Act empowers the Minister to issue "policy guidelines to the Commission regarding the performance of its functions [and] the Commission shall comply with the policy guidelines given by the Minister under this section."[215] In addition, all the members of the Commission are appointed by the Minister with approval of Cabinet.[216] Thus, the Commission is subordinated to the Minister's control and its members are political appointees. Therefore, this Commission is susceptible to executive interference which may undermine its independence, and as confirmed by the key informants interviewed during this study, it has not been able to safeguard the rights of individuals from arbitrary interference through unlawful communication surveillance or illegal suspension of access to internet by the executive. For instance, in 2021, at the behest of the government the Commission illegally ordered the suspension of internet in the period towards the general elections.[217]

6.3 Key issues relating to restrictions on access to internet

In recent years, the Ugandan government, acting through the Ugandan Communications Commission, has shut down internet and blocked social media sites twice. The first time was in 2016 when Facebook, Twitter and WhatsApp were shut down for several days before the general elections. Access to internet and social media was also blocked in the period towards the elections in 2021 and ahead of President Museveni's inauguration. On all these occasions, the government justified the restrictions by claiming

[213] See section 4 of the Act
[214] See section 5(1) of the Act
[215] See section 7 (1) and (2) of the Act
[216] See section 9(3) of the Act.
[217] *Uganda 2021 general elections: The internet shutdown and its ripple effects*. 2021. Available at https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects

that there were a "necessary security measure" against those "telling lies about the elections".[218]

There is no law regulating internet shutdowns in Uganda. When the government (through the Ugandan Communications Commission) ordered the suspension of access to internet in January 2021, it sought to rely on section 56 of the Ugandan Communications Act.[219] Yet, these provisions do not provide the Commission with such powers. Section 56 of the Act provides that an operator shall not deny access or service to a customer "except for non-payment of dues or for any other just cause." The government interpreted "any other just cause" to include the need to protect national security and mitigate against the spreading of false information about the elections. Wholesale suspension of access to internet will almost always be a disproportionate means of restriction on freedom of expression, irrespective of whether some kind of restriction could be justifiable. In addition, it must be provided for law and expressly regulated by law, to protect individuals against arbitrary interference with their rights. Furthermore, mitigation against the spreading of false information is not in itself a legitimate purpose for restricting the freedom of expression under regional and international law. There are other means of combatting the spreading of alleged falsehoods about an election which do not include restricting online freedom of expression. In fact, switching off the internet undermines electoral transparency and fuels speculation as well as the spreading of misinformation through other means of communication. Furthermore, a law which authorizes the imposition of restrictions on these rights must require government to obtain a warrant from an independent body (such as a court of law) before imposing such restrictions. Such legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the State to ensure that restrictions on access to internet are permitted only when they are provided by law, and necessary and proportionate to a legitimate purpose under ICCPR article 19(3). Section 56 of the Ugandan Communications Act does not provide for any of these safeguards.

The Ugandan government is also restricting online freedom of expression and access to the digital space through the exorbitant taxation of internet and social media users. In 2018, the government introduced the so-called Over-The-Top (OTT) daily tax, levied on social media services including messaging and voice calls via WhatsApp, Facebook, Skype and Viber. However, this has recently been replaced by a 12% excise duty tax levied

[218] Butagira, T. 2016. *Museveni explains social media, mobile money shutdown.* Available at https://allafrica.com/stories/201602181520.html

[219] In March 2021, the East African Lawyers Association filed a petition against the state in the East African Court of Justice due to the shutdowns in January 2021. Their statement of reference contains copies of suspension notices dated 12 and 13 January 2021, issued to service providers by the Ugandan Communications Commission for the suspension of the operation of social media, and the suspension of the operation of internet gateways, respectively. These notices rely solely upon Sections 5(1) and 56 of the Ugandan Communications Act.

effective 1 July 2021.[220] The new tax has severely increased the total cost of data. For example, the cost of a 60GB monthly bundle increased by an additional USD 1.50[221] in a context where 41% of the population[222] live in poverty. These high costs of data have made access to internet unaffordable for many. It is reported that about 5 million users were cut off from internet connection within the first year of the OTT tax, because they could not afford the costs.[223] The high taxation effectively impairs the ability of large segment of the population to enjoy access to information and the means of expression. Uganda has an obligation to facilitate the exercise of this right without discriminating against anyone on the basis of their economic or social status.

The Ugandan government is also restricting online freedom of expression and access to the digital space through the imposition of mandatory registration and licensing of internet users. In August 2019, the Ugandan Communications Commission issued a directive which requires all persons currently offering or planning to commence the provision of online data communication and broadcasting services including social media bloggers, to register with the Commission and pay a registration fee of USD20. The registration requirement, especially for social media bloggers does not serve any legitimate purpose and thus may effectively constitute an illegitimate and unnecessary restriction against the exercise of freedom of online expression.

6.4 Recommendations

I. Legislation which seeks to authorize communications interception and surveillance must make the imposition of such restrictions to be subject to a court warrant. Legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the state to ensure that restrictions on the right to privacy are permitted only when they are lawful, necessary and to the extent that they are proportionate. In this sense, The Anti-Terrorism Act must be amended to remove the powers of State agencies to conduct communications surveillance without a court warrant. Where, in exceptional and urgent circumstances, the law allows for surveillance and interception of private communications without a court warrant a court of law must be notified immediately of the decision to impose

[220] See https://businesslicences.go.ug/kcfinder/upload/files/UCC%20fees%20structure.pdf Also see Mwesigwa, D. 2021. *Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data.* Available at https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/
[221] Roke Telkom. 2021. Changes in Invoicing Data. (Twitter) 20 June. Available at
[222] See https://opportunity.org/our-impact/where-we-work/uganda-facts-about-poverty
[223] Mwesigwa, D. 2021. *Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data.* Available at https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/

these restrictions on one's right to privacy and the court must make a competent order as to whether that decision must be varied or not.

II. All legislation regulating communications interception and surveillance should be amended so as to set out clear, objective criteria, in conformity with the principle of legality, to be applied on a case by case basis by public officials and a court of law which must apply the principles , necessity and proportionality, and legitimacy of purpose of surveillance in each application for a warrant of surveillance. In this sense, the Regulation of Interception of Communication Act and the Computer Misuse Act should be reviewed and amended to incorporate these criteria.

III. The parliament should enact legislation to provide for the establishment of an independent body that oversees the operation of all telecommunication and similar legislation, including the Ugandan Communications Act, Computer Misuse Act and the Anti-Terrorism Act that contemplates the imposition of restrictions to freedom of expression, access to information and right to privacy. The body should be empowered to ensure that any restrictions are clearly provided for in law and to ensure any restriction are necessary and proportionate to a legitimate purpose. If the body is not a judicial one, its determinations should be subject to judicial review. The government should act to ensure that Uganda becomes party to Malabo Convention which specifically calls on States parties to establish an independent oversight body for these purposes.

IV. The Parliament should amend all laws providing for surveillance authority to provide for a mandatory obligation of the responsible authorities to conduct post-surveillance notification, as means of providing targets of surveillance with information that is necessary for them to exercise their right to legal recourse and hold the authorities accountable for any interference on privacy or freedom of expression and information that does not meet the principle of legality and is unnecessary and or disproportionate to a legitimate purpose.

V. The Parliament should amend Ugandan Communications Act so as to remove the mandatory requirement for social media users to register and be licensed before they can publish online content and to remove all the taxation requirements imposed on social media users.

VI. The government must desist from imposing online and other restrictions that are not based on law. The arbitrary suspension of access to social media in the period towards the 2021 elections must be thoroughly investigated, those whose rights were allegedly violated should have access to an effective remedy and reparation and those responsible must be held accountable.

VII. The Ugandan Communications Act must be amended to require government to obtain a warrant from an independent body (such as a court of law) before imposing restrictions on access to internet or social media. Such legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the state to ensure that restrictions on access to internet are permitted only when they are clearly provided for in law, and are necessary and proportionate to a legitimate purpose withing the meaning of ICPR article 19(3).

7. Zimbabwe

7.1 Main Applicable Laws

Zimbabwe ratified **the African Charter** in 1986, and acceded to **the ICCPR** in 1991. It has signed, but not ratified the Malabo Convention.

The Zimbabwean **Constitution** protects the right to privacy, which includes, among other things, "the right not to have the privacy of … communications infringed."[224] Section 61(1) of the Constitution protects the freedom of expression and the media by stating that:

> *Every person has the right to freedom of expression, which includes- (a) freedom to seek, receive and communicate ideas and other information; (b) freedom of artistic expression and scientific research and creativity; and (c) academic freedom."* However, freedom of expression excludes *"incitement to violence; advocacy of hatred or hate speech; malicious injury to a person's reputation or dignity; or malicious or unwarranted breach of a person's right to privacy*."[225] The Constitution also guarantees the right of access to information.[226]

The **Interception of Communications Act**[227] provides for the interception of communications in Zimbabwe where there are "reasonable grounds to believe that a serious offence has been, or is being, or will be committed by an organised criminal group".[228] The Act also permits the interception of private communications for purposes of gathering information concerning an actual threat to national security or public safety.[229] It establishes the "Monitoring Centre" as the sole facility that is permitted to facilitate authorized interception of private communications. Under the Act, only the Chief of Defence Intelligence, the Director-General of the President's department responsible for national security, the Commissioner of the Zimbabwe Republic Police, and the Commissioner-General of the Zimbabwe Revenue Authority may apply for a warrant to intercept private communications.[230] Applications for warrants are to be made to and are decided on by the Minister of Transport and Communications.[231] All telecommunications service providers must comply with the warrant issued by the Minister in terms of this Act.[232]

---

[224] Section 57 of the Constitution
[225] Section 61(5)(a-d) of the Constitution.
[226] Section 62 of the Constitution
[227] Interception of Communication Act 6 of 2007
[228] Section 6 of the Act
[229] Section 6 of the Act
[230] Section 5(1) of the Act
[231] Section 5(2) of the Act
[232] Section 9 and 12 of the Act

The **Postal and Telecommunications Act** establishes the Postal and Telecommunications Board which regulates the issuing of licenses, terms, and conditions of licences for a range of telecommunication services and systems including cellular and other telecommunication licenses.[233] The Act also establishes a range of communications offences including, prohibiting the sending of telephone messages that are "grossly offensive, indecent, obscene or threatening, false, causing annoyance, inconvenience or needless anxiety."[234] To support the implementation of this Act, the executive (Minister of communications) enacted the **Postal and Telecommunication (Subscriber Registration) Regulations**.[235] Among other obligations, these regulations require telecommunications service providers to ensure that each subscriber or customer's identity and other personal details are recorded and registered in their system before activating a SIM-card on their telecommunication network systems.[236] These Regulations also provide for the establishment of a central subscriber information database which contains all telecommunications subscriber information, and this database is to be managed by a government agency (the Postal and Telecommunication Regulatory Authority of Zimbabwe).[237]

The **Postal and Telecommunication (Telecommunications Traffic Monitoring System) Regulations,[238]** promulgated by the executive, provides for the monitoring of telecommunications traffic in Zimbabwe, to ensure accurate revenue collection by the government from the telecommunications service providers. The administration is performed through the installation of a 'civil tool' that monitors and creates a log sheet of all telecommunication transactions processed by each telecommunications service provider.[239] The Regulations do not provide details on the nature of information which is collected by this tool and whether there are any measures in place to protect the confidentiality of any personal information that may be gathered through it.

At the time of compiling this report, the Zimbabwean Parliament had passed the **Cyber Security and Data Protection Bill**, but the President was yet to sign it into law. If signed into law by the President, the Bill would provide for the investigation and collection of evidence for cybercrime and data breaches. It would empower a person in the position of a police officer to make an application to a magistrate for a warrant for the search and seizure of any premises reasonably believed to have a computer system which has data to be used as evidence of a cybercrime. The police officer would also have the power to access a computer system for the purpose of obtaining evidence in investigations, subject to obtaining

[233] Section 3 to 30 of the Act
[234] Section 288 of the Act
[235] Statutory Instrument 95 of 2014
[236] Section 3(1) of the Regulations
[237] Section 8(1) of the Regulations
[238] Statutory Instrument 95 of 2021
[239] Section 3 of the Regulations

a court warrant. In addition, the bill seeks to provide for criminal liability for the publication of false information by stating that:

> *Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.*[240]

In 2016, cabinet adopted the **National Policy for Information and Communication Technology.**[241] This policy sets out a plan to centralize government control over the provision of the infrastructure for broadband internet services, information and applications, purportedly to "avoid the duplication of investment by service providers in the country."[242]

7.2 Key issues relating to interception of communications and surveillance

The Interception of Communications Act permits the interception of private communications without a warrant issued by an independent authority. Under the Act, a warrant for the interception of private communications is sought from the Minister of Transport and Communication,[and there is no judicial approval needed].[243] A cabinet Minister is not an independent authority. This leaves the rights to privacy and freedom of expression and information vulnerable to arbitrary interference especially by the executive through interception and collection of information that is provided clearly in law and may be unnecessary and disproportionate to a legitimate purpose. As confirmed by sources interviewed during this study as well as other media[244] and civil society organizations working in the country, the government heavily relies on this provision in the Act to conduct communications surveillance of opposition and civil society activists and, thus, unlawfully limiting the right to privacy.

Neither the Interception of Communications Act nor any other law creates a mandatory obligation for the government to provide post-surveillance notification. Yet, the Interception of Communications Act provides that any person who is aggrieved by a decision to issue a warrant of interception may appeal to an Administrative Court[245] for legal recourse within one

[240] See section of Section 164C of the Bill
[241] National Policy for Information and Communication Technology (ICT), 2016
[242] Paragraph 7.1 of the policy.
[243] Section 5(1)(a) – (d) of the Act
[244] See IFEX report available at https://ifex.org/right-to-privacy-under-threat-in-zimbabwe/
[245] Established as part of the judiciary in terms of section 162(e) of the Constitution.

month of being notified or becoming aware of that decision.[246] This right to an effective remedy is meant to protect individuals against the arbitrary and unlawful interferences on the enjoyment of their human rights, including their rights to privacy and freedom of information and expression, and to hold the State and State authorities accountable for such violations. However, the absence of a mandatory obligation for post surveillance notification undermines ability of individuals to access to justice in this regard.

There are no mechanisms provided under the law to ensure the protection of the confidentiality of personal information collected under the laws which regulate telecommunications operations in the country. For example, under the Postal and Telecommunication (Subscriber Registration) Regulations,[247]a central subscriber information database which contains all telecommunications subscriber information must be created and be managed by a government agency.[248] This database contains personal information of all subscribers and such information is placed under the control of the Postal and Telecommunications Regulation Authority of Zimbabwe (a government agency) without any mechanism in place to guarantee that its confidentiality is adequately secured. Furthermore, under the Postal and Telecommunication (Telecommunications Traffic Monitoring System) Regulations,[249] the government is empowered to install a 'civil tool' to monitor and create a log sheet of all telecommunication transactions processed by each telecommunications service provider.[250] The Regulations do not provide details on the nature of information which is collected by this tool and whether there are any measures in place to protect the confidentiality of any personal information that may be gathered through this tool. Without such measures or guarantees, the right to privacy and freedom of expression and information is vulnerable to arbitrary interference with drastic consequences on many other rights. Sources interviewed during this study indicated that the personal data collected under this legislation has been used by the State security agencies to locate and abduct political activists. Zimbabwe has a terrible history of political abductions, many of which constitute crimes under international law.[251] In the ~~previous~~ general election of 2018, the ruling party ZANU PF is said to have relied on this database to send out unsolicited text messages as part of its campaign strategy.[252]

Neither the Interception of Communications Act nor any other law protects the confidentiality of communication meta data. Communications meta

[246] Section 18 of the Act
[247] Section 8(1) of the Act
[248] Section 8(1) of the Regulations
[249] Section 3 of the Act
[250] Section 3 of the Act
[251] See https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25944&LangID=E
[252] See https://zimbabwe.misa.org/2018/07/13/zimbabwes-urgent-need-data-privacy-laws/

data refers to all other information about a communication transaction other than the content of the actual communication transaction.[253] The Interception of Communications Act only prohibits the listening into and recording of details of the actual communication,[254] but does not prohibit access to meta data. Yet, metadata is often more telling than content data, in that it provides the whereabouts of the person under surveillance, who they communicate with, and when. Collection of meta data is therefore an a presumptively and unlawful interference with enjoyment of the right to privacy and freedom of expression and information and can jeopardize other human rights including the rights to liberty and security and freedom from ill-treatment. The absence of legal protections of the confidentiality of communications meta data leaves these rights vulnerable to arbitrary and unlawful interference.

7.3 Key issues relating to restrictions on access to internet

Zimbabwe does not have any legislation that specifically authorizes the imposition of restrictions on access to internet, including the suspension of internet and use of social media platforms. Yet the executive has in the past unilaterally imposed restrictions on access to the internet. In January 2019, the government (acting though the Minister of telecommunications) switched off internet across the whole country for five days[255] in the wake of mass demonstrations organized by civil society and the opposition against the government. In July 2020, the government is alleged to have obstructed internet connectivity ahead of similar mass protests.[256]

In an effort to explain the legal basis for the suspension of internet connectivity in January 2019, one of the telecommunications operators and internet service providers (Econet) issued a press statement stating that:

> *Further to a warrant issued by the Minister of State in the President's Office for National Security through the Director-General of the President's Department acting in terms of the Interception of Communications Act, internet services are currently suspended across all networks and internet service providers. We are obliged to act when directed to do so and the matter is beyond our control.*[257]

---

[253] See https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf
[254] Section 3 of the Interception of Communication Act
[255] See Provisional Order of Zimbabwe High Court. Available from: http://www.veritaszim.net/sites/veritas_d/files/Provisional%20Order%20for%20internet%20access%20%5Bboth%20pages%5D.pdf
[256] See https://netblocks.org/reports/zimbabwe-internet-disruption-limits-coverage-of-protests-7yNV70yq
[257] Veritas. 2019. *The Internet Shutdown: The High Court's Ruling of 21st January – Court Watch 1 / 2019*. Available from: https://kubatana.net/2019/01/31/internet-shutdown-high-courts-ruling-21st-january-court-watch-1-2019/

This implied that the government authorities had relied on section 6 of the Interception of Communications Act to compel internet service providers to suspend the provision of internet. Section 6 of the Act empowers the Minister to compel a telecommunications operator to intercept communications in the interest of national security, public safety and where there are reasonable grounds to believe that a serious offence has been, or is being, or will be committed by an organised criminal group." This provides for powers to intercept communications and it does not provide powers for the Minister or anyone else to suspend access to internet. This view was confirmed by the High Court in a legal challenge brought by the Zimbabwe Lawyers for Human Rights and MISA Zimbabwe.[258]

7.3 Recommendations

I. Legislation, including the Interception of Communications Act, which seeks to authorize communications interception and surveillance must make the imposition of such restrictions to be subject to a court warrant. Legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the State to ensure that restrictions on the right to privacy are permitted only when they comply with principles of non-discrimination, legality, necessity, proportionality, and legitimate purpose. The Interception of Communications Act must be amended to remove the powers of the Minister to issue warrants for the interception of communication. The officials requesting the warrant and the courts must respect the principles of non-discrimination, legality, necessity, proportionality and legitimate purpose.

II. All surveillance laws, including the Interception of Communications Act, must be amended to provide for a mandatory obligation of the State agencies to ensure post-surveillance notification, as means of providing targets of surveillance with information that is necessary for them to exercise their right to and effective remedy and hold the State and State officials accountable for any interferences on their right to privacy that is not provided for by law in specific and exact terms, unnecessary and or disproportionate to a legitimate purpose within the meaning of ICCPR article 19(3). This would make the right to legal recourse provided under section 18 of the Interception of Communications Act to be more effective.

III. Both the Postal and Telecommunication (Subscriber Registration) Regulations and the Postal and Telecommunication (Telecommunications Traffic Monitoring System) Regulations must be amended to provide for the creation of mechanisms for the protection

[258] *ZLHR and MISA Zimbabwe v Minister of State for National Security and Others* [2019] ZWHC 265

of the confidentiality of personal information collected under these and other laws which regulate telecommunications operations in the country. This can also be achieved by ensuring that this information is managed by a court or similar independent authority as opposed to an executive agency of government as is the current arrangement. These protection mechanisms can also be incorporated into the proposed Cyber Crimes Bill.[259]

IV. Government authorities must desist from imposing online and other restrictions that are not based on law, expressed clearly in consistent with the principle of legality. . The arbitrary suspension of access to internet in January 2019 and July 2020 must be thoroughly, impartially and effectively investigated and those responsible for this unlawful action must be held accountable.

V. Any law which seeks to authorize the suspension of access to internet or the imposition of any restrictions on internet must require authorities who wish to exercise such powers to obtain a warrant from a judicial authority before imposing the restrictions. Such legislation must set out clear and objective criteria to be applied by the courts based on the obligation of the State to ensure that restrictions on access to internet are permitted only when they are provided for by law consistent with the principle of legality, and are necessary and proportionate to legitimate purpose recognized under ICCPR article 19(3).

[259] Section 3 of the Bill.

International
Commission
of Jurists

P.O. Box 91
Rue des Bains 33
CH 1211 Geneva 8
Switzerland

t +41 22 979 38 00
f +41 22 979 38 01
www.icj.org