

State of Internet Freedom in Africa 2018

Privacy and Data Protection in the Digital Era: Challenges and Trends in Africa

September 2018



Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the state of privacy and personal data protection in select African countries, tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. The study covers Burundi, the DRC, Ethiopia, Ghana, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda, Zambia, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

Research steering committee

Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

Country researchers

Burundi - Jean Paul Nkurunziza, Alain Ndikumana

DR Congo - Arsène Baguma Tungali and Blaise Ndola

Ethiopia – Berhan Taye and Roman Teshome

Ghana – Dora Mawutor

Kenya - Kenya ICT Action Network (KICTANet)

Malawi – Jimmy Kainja

Nigeria – Adaora Okoli

Rwanda – Robert Mbaraga

Senegal – Ababacar Diop

Tanzania – Asha Abinallah

Uganda – Daniel Mwesigwa and Edrine Wanyama

Zambia – Richard Mulonga

Zimbabwe – Natasha Msonza

Design

Ish Designs

muwonge_issa@yahoo.com

State of Internet Freedom in Africa 2018

Published by CIPESA, www.cipesa.org

September 2018



Creative Commons Attribution 4.0 Licence
<creativecommons.org/licenses/by-nc-nd/4.0/>
Some rights reserved.

Table of Contents

1. Introduction and Background	5
1.1 Introduction	5
1.2 Study Rationale	6
1.3 Aim of the Study	8
2 Study Methodology	9
3 Country Contexts	10
3.1 Political Economy	10
3.2 ICT Status	11
3.3 Political Environment	12
4 Laws and Policies Affecting Privacy and Personal Data Protection	18
4.1 International Framework for the Protection of Privacy	18
4.2 African Instruments on Privacy and Personal Data Protection	19
4.3 National Constitutional Frameworks for the Protection of Privacy	21
4.4 Legal Frameworks for Privacy and Data Protection Laws and Policies	23
4.5 Recognition of Personal Data in Statutes	24
4.6 Limitations on the Right to Privacy	25
5 Results: Status, Trends and Challenges	27
5.1 Limited Understanding of Privacy	27
5.2 Weak Policy and Legal Frameworks	28
5.2.1 <i>Absence of Comprehensive Data Protection Frameworks</i>	28
5.2.2 <i>Abuse of Laws to Undermine Privacy</i>	29
5.2.3 <i>Legal Provisions Compelling Telecom Companies to Cooperate on Surveillance</i>	30
5.2.4 <i>Unreasonable Search and Seizure Provisions</i>	32
5.3 Data Collection Programmes by Governments	33
5.3.1 <i>Mandatory Data Collection</i>	33
5.3.2 <i>Scaling up Digitisation Programmes</i>	36
5.4 Enhanced State Surveillance Capacity	39
5.4.1 <i>Permitted Interception and Surveillance</i>	39
5.4.2 <i>State Acquisition and Deployment of Surveillance Technologies</i>	41
5.4.3 <i>Increased Information Requests from Governments</i>	42

5.5 Privacy Breaches by Business Entities	44
5.5.1 <i>Legal Responsibility of Business Entities</i>	45
5.5.2 <i>Mishandling of Customer Data</i>	46
5.5.3 <i>Targeted and Indiscriminate Communication</i>	47
5.6 Dispute Resolution and Remedies	48
5.6.1 <i>Existing Frameworks for Remedies</i>	48
5.6.2 <i>Notable Judicial Decisions</i>	49
6 Conclusion and Recommendations	50
6.1 Conclusion	50
6.2 Recommendations	52
6.2.1 <i>Government</i>	52
6.2.2 <i>Companies/Business</i>	53
6.2.3 <i>Academia</i>	53
6.2.4 <i>Media</i>	54
6.2.5 <i>Technical Community</i>	54
6.2.5 <i>Civil Society</i>	54

1. Introduction and Background

1.1 Introduction

One of the earliest definitions of the right to privacy is from 1890, when Samuel Warren and Louis Brandeis defined it as the “right to be let alone”.¹ At the time, the United States was witnessing technological inventions and business methods that were making individuals’ personal lives more accessible to others irrespective of acquaintance, social or economic class, or the customary constraints of propriety.² These included the telephone, telephone exchanges, portable cameras, instantaneous photographs, sound recording devices, and newspapers. There was therefore need to outline principles to protect the individuals from invasion of their privacy.

The concerns expressed by Warren and Brandeis in 1890 are true today perhaps more than before, as the right to privacy is hugely affected by technological developments and by economic, political and social changes. Moreover, privacy concerns continue to feature prominently in democratic processes including elections, commercial transactions, citizen-to-government interactions, and generally in the use of social media.³

National and international efforts to protect personal data from misuse or unlawful access have sought to provide protection against questionable business practices, unlawful surveillance, and digitally mediated attacks perpetuated by adversaries such as hackers and fraudsters. The 1948 Universal Declaration of Human Rights (UDHR) and the 1966 International Covenant on Civil and Political Rights (ICCPR) articulate the right to privacy. The right has also been incorporated in more than 130 national constitutions worldwide.⁴

The right to privacy is central to the protection of human dignity, forms the basis of any democratic society, and supports other rights, such as freedom of expression, information and association.⁵ It is essential therefore for states to have policy, administrative and legal frameworks that robustly protect the individual from invasion of their privacy and abuse of their personal data. However, in Africa the weak or missing legal protections for personal data, abuse of existing laws by state agencies in service of often partisan interests, and poor digital security practices by citizens, are tremendously undermining citizens’ privacy and personal data.

¹ Warren, S. D. and Brandeis, L.D., *The Right to Privacy* (1980), Harvard Law Review, <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>

² Dorothy Glancy, *The invention of the Right to Privacy*, Arizona Law Review Vol. 21, 1971, <http://law.scu.edu/wp-content/uploads/Privacy.pdf>

³ Hunton & Williams, “Getting the Deal Through: Data Protection & Privacy,” <https://gettingthedealthrough.com/area/52/article/29146/data-protection-privacy-2018-introduction/>.

⁴ *Ibid.*

⁵ Privacy International, “What is Privacy,” <https://privacyinternational.org/explainer/56/what-privacy>

1.2 Study Rationale

The use of Information and Communications Technology (ICT) in Africa is fast growing among individuals, enterprises and governments departments. However, there are several challenges associated with ICT use in Africa. Those related to privacy and data protection, which are the focus of this report, are, however, only a manifestation of the poor state of internet freedom in many African countries, as they generally tend to undermine freedom of expression and the free flow of information online.

At the end of 2017, Sub-Saharan Africa had over 444 million mobile subscribers with an equivalent penetration rate of 44%, which is still well below the global average of 66%. Moreover, an annual growth rate of 4.4% is expected between 2017 and 2020, a subscriber growth rate that will be more than double the global growth rate over the same period.⁶

The mobile money industry in Africa is also growing exponentially. According to the GSMA, the mobile money industry registered 690 million accounts worldwide in 2017, and processed a billion dollars a day, generating direct revenues of over USD 2.4 billion. Of these accounts, 338 million were in Sub-Saharan Africa and processed \$19.9 billion in 1.2 billion transactions in 2017.⁷ Eastern Africa accounted for 56.4% (191 million) of the total Sub-Saharan accounts, processing USD 13.2 billion in 870.3 million transactions in 2017. According to the report, the registered accounts in Western Africa, Central Africa and Southern Africa accounts stood at 104.5 million, 32.9 million and 10 million respectively; transacting USD 5.3 billion, USD 1.3 billion and USD 123 million respectively during the same period.

Consequently, the growth in mobile subscriptions, increased use of smartphones, mandatory SIM card registration in the majority of African countries, enhanced collection of biometric data, access to new fintech products and digitisation of more sectors of the economy and public services have resulted in increased collection, processing and sharing of personal data making it increasingly prone to abuse by both state and non-state actors.

Furthermore, the digital environment has provided opportunity for anonymous communication which enables freedom of expression but can also be detrimental in avoidance of responsibility or facilitating illegal or criminal activities. Developments in technology have granted most end users the ability to create, upload and distribute content online with little effort and cost, in the absence of editing, censorship or ethical codes for the press.

Many internet users are not aware of the implications of their use of the web and how their rights are compromised or how their data is automatically gathered or processed without their knowledge, and sold or linked with other sources to produce a complex record of several aspects of their lives without clear legal control and regulatory mechanisms. Yet, in a bid to assure users of the security of information identifying them, industry players that benefit from the users' mistaken feeling of anonymity have cultivated the notion of highly complex "anonymised" data.⁸

⁶ GSMA, *The Mobile economy in Sub-Saharan Africa 2018*, <https://www.gsmaintelligence.com/research/2018/07/the-mobile-economy-sub-saharan-africa-2018/683/>

⁷ 2017 State of the Industry Report on Mobile Money, GSMA https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/GSMA_2017_State_of_the_Industry_Report_on_Mobile_Money_Full_Report.pdf

⁸ Report of the Special Rapporteur on the right to privacy, 22nd Session, 19 October 2017, https://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx; Expert workshop Concept Note, <https://www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf>

Indiscriminate and excessive data collection by government and private actors can also have a chilling effect on freedom of expression, which could limit civil engagement and undermine democracy.⁹ When users are aware of large scale data collection or surveillance, they may self-censor their behaviour due to fear of unexpected consequences.¹⁰ The misuse of personal data by security and intelligence agencies amidst inadequate judicial and parliamentary oversight over surveillance activity is one such example. Events like the Cambridge Analytica case in which Facebook user details were used to influence elections including, purportedly, in Nigeria and Kenya,¹¹ and use of big data in refugee and migration work without ethical and privacy considerations,¹² point to non-state actors' utilisation of citizen data for controversial purposes.

Indubitably therefore, the state of personal data protection tends to mirror - and to affect - the state of internet freedom in a country. Indeed, in various African countries, there are various worrying developments on the internet freedom front. There has been an increase in digital rights violations such as arrests and intimidation of online users, internet blockages and social media shutdowns¹³, and a proliferation of laws and regulations that undermine internet access and affordability, and weaken ICT's potential to improve livelihoods, catalyse free expression and civic participation.

In March 2018, the Uganda Communications Commission ordered the registration of online content providers and released tough restrictions on registration of SIM cards. The Kenya government, in May 2018 enacted a cybercrimes law, which human rights defenders contend contravenes rights to freedom of expression and privacy. Shortly thereafter, in July 2018, social media and mobile money transaction taxes were introduced in Uganda, with users required to pay before accessing Over The Top (OTT) platforms which were blocked. In Tanzania, online content hosts and producers must pay over USD 900 to register with the state in order to maintain their platforms, according to new regulations. The DR Congo, which has ordered various internet disruptions in the last two years, also issued regulations in 2018 that require online content producers to register, while Zambia's cabinet in August 2018 endorsed the introduction of a daily tax on OTT calls¹⁴, as did Benin in July 2018.¹⁵ Burundi has this year passed a new law that expands the scope for surveillance and monitoring of communications, and tightened control over online publishers.

While some African countries have enacted data protection laws, many ICT users are unaware of their related privacy rights.¹⁶ Presently, 22 African countries have privacy and data protection laws, namely Angola (2016), Benin (2009), Botswana (2018), Burkina Faso (2004), Chad (2015), Cape Verde (2001), Côte d'Ivoire (2013), Equatorial Guinea (2016), Gabon (2011), Ghana (2012), Lesotho (2012), Madagascar (2014)¹⁷, Mali (2013), Mauritius (2017), Mauritania (2017), Morocco (2009), Senegal (2008), Seychelles (2002),¹⁸ South Africa (2013), Tunisia (2004), Zambia, and Zimbabwe (2003). Others, including Algeria, Democratic Republic of the Congo, Ethiopia, Kenya, Malawi, Mauritania, Niger, Nigeria, Rwanda, Sierra Leone, Swaziland, Tanzania and Uganda, have draft legislation.¹⁹

⁹ Cohen, J.E. (2013) What is Privacy for? Harvard Law Review 126.

¹⁰ The right to privacy in the digital age, https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf

¹¹ Claims about Cambridge Analytica's role in Africa should be taken with a pinch of salt, <https://bit.ly/2zssn2P>

¹² How big data can help migrants, <https://www.weforum.org/agenda/2015/10/how-big-data-can-help-migrants/>

¹³ CIPESA, A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa, https://cipesa.org/?wpfb_dl=252

¹⁴ CIPESA, Zambia Introduces Daily Tax on Internet Voice Calls, <https://cipesa.org/2018/08/zambia-introduces-daily-tax-on-internet-voice-calls/>

¹⁵ <https://internetwithoutborders.org/campaign-to-cancel-facebook-tax-benin/>

¹⁶ Are Organisations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?, https://researchspace.csir.co.za/dspace/bitstream/handle/10204/9267/Baloyi_19059_2017.pdf?sequence=1

¹⁷ LOI N° 2014 – 038 Sur la protection des données à caractère personnel

<https://www.afapdp.org/wp-content/uploads/2015/01/Madagascar-L-2014-038-du-09-01-15-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel.pdf>

¹⁸ Data Protection Act, 2002, <https://seylil.org/sc/legislation/act/2002/9>

¹⁹ What African Countries Can Learn from European Privacy Laws and Policies,

<https://cipesa.org/2017/07/what-african-countries-can-learn-from-european-privacy-laws-and-policies/>; See also a full list of countries with Data Protection Legislation and Bills at UNCTAD, "Data Protection & Privacy Laws" <http://unctad.org/en/Docs/Cyberlaw/DP.xlsx>; Emerging Data Protection regulations in Africa <http://www.elexica.com/~media/Files/Training/2015/05%20May/Emerging%20data%20protection%20regulations%20in%20Africa.pdf>

As the discussion on data protection and privacy takes on a new form with the introduction of the EU General Data Protection Regulation (GDPR) whose global impact cannot be ignored, it is necessary to analyse the data protection and privacy policies and practices in Africa. Moreover, it is crucial to situate the data protection debate on the continent in the wider context of internet freedom, by establishing how weak or non-existent data protection policies and practices lead to wider abuses of individuals' and entities' digital rights.

1.3 Aim of the Study

This research documents the state of privacy and personal data protection in select African countries, tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations by governments and businesses, and users' understanding of protecting their privacy online. The study covers Burundi, the DRC, Ethiopia, Ghana, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda, Zambia, and Zimbabwe.

The study identifies measures that can positively influence the right to privacy laws and practices in Africa. Accordingly, it will inform policy makers, academia, technologists, civil society, digital rights researchers, and the media, on the current legal, institutional and practice landscape and the opportunities for improvement to data protection and privacy laws and regulations with a view to advancing internet freedom in the region.

2 Study Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Reports of previous studies, media reports, academic works, government documents, and other literature, were reviewed. The literature review generated an understanding of the current debates and issues on privacy and data protection in the focus countries.

The legal and policy analysis included a review of laws and policies that influence privacy and personal data protection to establish how well, or not, they support the enjoyment of the right to privacy. The state of implementation of these laws and policies, their interpretation or misinterpretation, as well as abuse by state and non-state actors, were also studied. Such laws and policies include those that govern the telecoms sector, the media, social media use, access to information, interception of communications, security and intelligence agencies, and security enforcement in general. The study also reviewed provisions of relevant international instruments each focus country is party to, while also referring to relevant provisions in national constitutions, laws and policies relevant to privacy and data protection.

The Key Informant Interviews (KIIs) were conducted with purposively selected respondents from each of the countries studied. These included staff of private companies (such as banks, telecoms firms, Internet Service Providers), government ministries (such as those responsible for ICT, security), semi-autonomous bodies (such as electoral commissions, data protection agencies), telecoms regulators, media houses, social media users, human rights defenders and activists, consumers' associations, academics and lawyers.

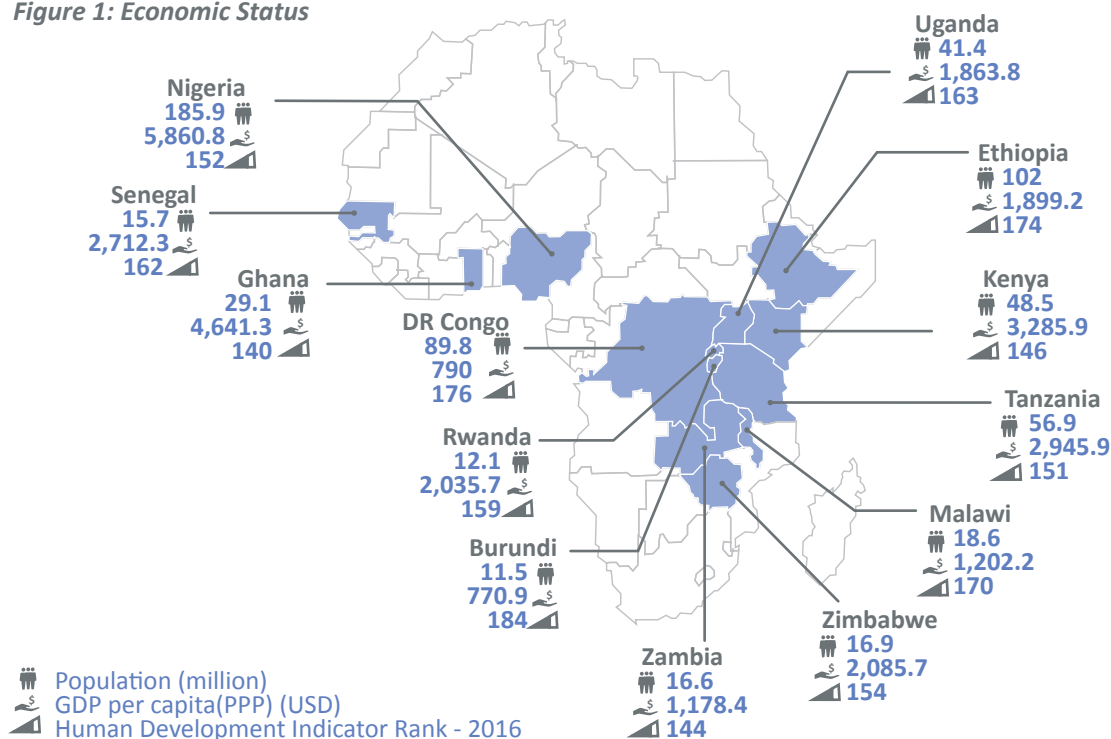
3 Country Contexts

This section provides an overview of the economic status, state of ICT connectivity including internet and mobile phone and mobile money usage. It also reviews the governance context, including the factors affecting, free expression, the rights to information, and privacy online and offline.

3.1 Political Economy

Aspects of the political economy status of the countries studied are shown in the Table 1 below. Among the countries reviewed, Nigeria has the highest population with 185.9 million people, followed by Ethiopia with 102 million. The smallest countries by population are Burundi and Rwanda with populations of 11.5 million and 11.9 million respectively. With regards to economic status, World Bank figures show that as of 2017, Nigeria had the highest GDP per capita (PPP) at USD 5,860 followed by Ghana (USD 4,641), Kenya (USD 3,285) and Tanzania (USD 2,945). DR Congo and Burundi recorded the lowest GDP per capita at USD 790 and USD 770 respectively.

Figure 1: Economic Status



²⁰ World Bank, GDP per capita, PPP (current international \$), <https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD>








²¹ UNDP, International Human Development Indicators, <http://hdr.undp.org/sites/default/files/rankings.pdf>

The Human Development Index (HDI) is a summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and having a decent standard of living. Out of the 188 countries ranked in the 2016 Index, Ghana ranked highest among the countries in the present research at 140, while Burundi was ranked lowest at 184.

3.2 ICT Status

Table 2 below provides the status of ICT in the countries under study. Most of the countries have four telecommunication service providers. Tanzania recorded the highest number of operators at seven, Ethiopia the least - just one.

Figure 2: ICT Status

	 No. of telcos	 Mobile penetration (%)	 Mobile Subscriptions (million)	 Internet penetration (%)	 Internet Subscriptions (million)	 Mobile Money Subscriptions (million)	 % of Users of Mobile Money & Mobile Subscribers
Burundi ²²	4	49.9	5.3	8.5	0.9	2.5	47.1
DRC	4	40	30	15.2	11.4	6.6	22
Ethiopia	1	34	34.7	15.4	16.1	2	5.8
Ghana	5	75.5	22	16.6	10.1	11.7	53.1
Kenya ²³	5	95.1	44.1	85	36.1	29.1	65.9
Malawi	4	36	7.1	9	1.6	3.9	54.9
Nigeria	4	84	165	53	103	2	1.2
Rwanda ²⁴	4	78.9	9.3	47.8	5.6	8.6	92.4
Senegal	3	106.5	14.3	59.8	0.9	7.2	50.3
Tanzania ²⁵	7	78	41.8	45	22.9	20.8	49.7
Uganda	4	66	24.9	48	18.8	23.3	35
Zambia	3	79.1	113	25.5	5.2	6	5.3
Zimbabwe ²⁶	4	102.7	6.9	50.8	14.1	4.7	68.1

²² <http://www.arct.gov.bi/index.php/publications/indicateurs/48-indicateur-du-secteur-tic-au-burundi>

²³ 3rd Quarter Sector Statistics Report, Communications Authority, <https://ca.go.ke/wp-content/uploads/2018/07/Sector-Statistics-Report-Q3-2017-18-2.pdf>

²⁴ Active mobile telephone subscriptions as of July 2018, http://www.rura.rw/uploads/media/Monthly_Mobile_Telephone_Statistics_report_as_of_July_2018_.pdf

²⁵ TCRA, Quarterly Communication Statistics, https://www.tcra.go.tz/images/documents/reports/TelCom_Statistics_June_2018.pdf

²⁶ <http://www.potraz.gov.zw/?download=973>

According to the International Telecommunication Union (ITU), mobile phone penetration in Africa stood at 78% in 2017.²⁷ The continent is expected to have 725 million smartphone users by 2020, up from 557 million at the end of 2015 according to the GSMA.²⁸

Regarding mobile penetration, Senegal had the highest penetration rate (106.5%), while Ethiopia had the lowest (34%). Internet penetration was higher than mobile penetration in all countries. Internet penetration in Kenya was closest to the mobile penetration, standing at 85%. Another significant variance was the wide difference in mobile penetration and internet penetration rates in Zimbabwe and Burundi - 102.7% and 50.8% for the former, and 49.9% and 8.5% respectively for the latter. This shows that despite many persons being able to access mobile telephony in the two countries, internet access is still much lower. The study reviewed the number of mobile money subscriptions in the focus countries, and as seen from Table 2, Rwanda had the highest number of mobile money subscribers per existing mobile subscriptions at 92.4%, followed by Zimbabwe at 68.1%. Nigeria had the lowest number of mobile money subscriptions at 1.2% of the existing mobile subscribers.

These statistics indicate that there are still challenges in accessing mobile phones, internet and mobile money services across all countries. However, access and usage continues to grow, as ICT tools and services become more affordable. In turn, increased use of these services is expanding the amount of data collected, the devices that can be surveilled, and number of persons who can be profiled. The impact of privacy policies and legal frameworks should hence be viewed with this in mind.

3.3 Political Environment

In recent years, there have been positive and negative political developments in the countries under review. All have had general elections, starting with Malawi in May 2014, Burundi in July 2015, Tanzania in October 2015, Uganda in February 2016 and Rwanda and Kenya in August 2017. In July 2018, Zimbabwe held a general election while Rwanda held parliamentary elections in September 2018.

Successive Ethiopian governments were renowned for their repressive rule, including stifling the political opposition and curtailing fundamental freedoms.²⁹ They were characterised by the abuse of courts and the law to routinely crack down on online and offline activities of critics and opponents; unwarranted and pervasive surveillance and restriction of online activities of Ethiopians, including through a monitoring system and the ZSmart customer management database in the government-owned Ethio Telecom network.³⁰

The country has since gone through notable political reforms since new Prime Minister Abiy Ahmed took over from Hailemariam Desalegn, who resigned in February 2018. The new leader has ended the border war with Eritrea and normalised relations with Ethiopia's long-time foe; lifted the state of emergency; ordered the release of thousands of prisoners; condemned the brutal treatment of prisoners, calling it "terrorism; and unblocked hundreds of websites and TV channels.³¹ The government also announced measures to liberalise the telecom sector; dropped charges

²⁷ ITU, ICT Facts and Figures 2017, <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>

²⁸ Number Of Unique Mobile Subscribers In Africa Surpasses Half A Billion, Finds New GSMA Study <https://www.gsma.com/newsroom/press-release/number-of-unique-mobile-subscribers-in-africa-surpasses-half-a-billion-finds-new-gsma-study/>

²⁹ Human Rights Watch, "They know everything we do": Telecom and Internet Surveillance in Ethiopia, 2014, <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>

³⁰ Freedom of the Net, Ethiopia 2017. <https://freedomhouse.org/report/freedom-net/2017/ethiopia>

³¹ BBC News, Abiy Ahmed: Ethiopia's prime minister, <https://www.bbc.com/news/world-africa-43567007>

against opposition leaders, bloggers, and activists; reconnected mobile and broadband internet services that had been cut off since 2016; and unblocked 246 websites, blogs, and news sites that had been inaccessible for over a decade.³² Whereas his efforts are welcome, many remain cautiously optimistic regarding the future of his rule.

In Zimbabwe, long time president Robert Mugabe was ousted from power in a November 2017 coup, which saw his ally for decades, Emmerson Mnangagwa of the dominant ZANU-PF party, take over as president with the support of the military. Following a July 2018 election, Mnangagwa was declared the winner although the opposition Movement for Democratic Change (MDC) Alliance disputed the poll results. Technology played a key role in the elections. The Zimbabwe Electoral Commission registered five million voters with a new a biometric system;³³ politicians bombarded voters with campaign messages via SMS and WhatsApp groups;³⁴ the government set up a short-lived Ministry of Cyber Security, Threat Detection and Mitigation³⁵ to deal with fake news and “abuse” of social media; and developed a Computer Crime and Cybercrime Bill.³⁶ Zimbabwe has several legal provisions that allow the government to conduct surveillance without sufficient oversight, and online journalists and ICT users continue to face regular harassment for their online activities.³⁷

In Kenya, calm returned following a political agreement dubbed the “Building Bridges Initiative” between President Uhuru Kenyatta and veteran opposition leader and former Prime Minister Raila Odinga. The March 2018 agreement aimed to unite Kenyans after divisive and disputed elections in 2017 that left the country highly polarised. In September 2017, following a petition by Odinga, Kenya’s Supreme Court nullified the results of the August presidential election, in what was a first in Africa, plunging the country into uncharted waters.³⁹ The use of technology in the election proved useful in bringing out election irregularities. However, Odinga boycotted the subsequent runoff, which heightened the political uncertainty even as the government continued its onslaught on the media, civil society, opposition and critics. The situation was further complicated by Odinga’s purported swearing-in as “the people’s president” in January 2018.⁴⁰

There is still concern over the Kenyan government’s unlawful and disproportionate surveillance capabilities, including access to and interception of content and data by national security agencies without warrant; monitoring of social media reportedly using Israeli “web intelligence” firm webintPro; ⁴¹ proposed implementation of the now suspended Device Management System;⁴² the reported presence of a “middle-box” on the Safaricom cellular network;⁴³ and continued intimidation and assault of bloggers and internet users.⁴⁴

In Uganda, which has been under the rule of President Yoweri Museveni’s National Resistance Movement (NRM) since 1986, there is concern over the government’s increasing surveillance capability over citizens’ communications in the absence of data protection legislation, coupled with its hostility towards the political opposition and online critics.⁴⁵ These include the alleged planting of FinFisher intrusion malware on hotel Wi-Fi to illegally spy on targeted persons;⁴⁶ and the overly broad surveillance powers granted to government agencies under the Regulation of Interception of Communication Act and the Anti-Terrorism Act to intercept individuals’ communications.

³² CIPESA, *The Reforms Ethiopia Needs to Advance Internet Freedom*, https://cipesa.org/?wpfb_dl=273

³³ <http://mobile.apanews.net/en/news/zimbabwe-74-of-eligible-voters-register-to-vote-in-2018-elections>

³⁴ <https://www.newsday.co.zw/2018/07/nuisance-campaign-messages>

³⁵ The Ministry was dissolved following a cabinet reshuffle by president Mnangagwa in December 2017. See: <https://www.enca.com/africa/list-mnangagwa-names-new-zimbabwean-cabinet>

³⁶ <https://www.techzim.co.zw/2016/08/heres-zimbabwes-draft-computer-crime-cybercrime-bill>

³⁷ *Freedom of the Net Zimbabwe 2017*. <https://freedomhouse.org/report/freedom-net/2017/zimbabwe>

³⁸ *Building Bridges Initiative*, <https://businessday.co.ke/wp-content/uploads/2018/03/Building-bridges-to-a-new-Kenyan-nation.pdf>

³⁹ *New York Times*, *Kenya Supreme Court Nullifies Presidential Election* <https://www.nytimes.com/2017/09/01/world/africa/kenya-election-kenyatta-odinga.html>

⁴⁰ Raila Odinga ‘sworn in’ as Kenya’s people’s president <https://www.aljazeera.com/news/2018/01/kenya-tv-networks-gagged-odinga-inauguration-180130081747894.html>

⁴¹ Privacy International, *Track, Capture Kill: Inside Communications Surveillance and Counterterrorism in Kenya*, https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

⁴² *Communications Authority stops phone spying system plan as ordered*, the Standard.

<https://www.standardmedia.co.ke/business/article/2001230387/communications-authority-stops-phone-spying-system-plan-as-ordered>

⁴³ CIPIT, *Safaricom and Internet traffic Tampering*, <https://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf>

⁴⁴ *Freedom House*, *Freedom of the Net Kenya 2017*, <https://freedomhouse.org/report/freedom-net/2017/kenya>

⁴⁵ *Uganda: The changing face of political opposition* <https://www.aljazeera.com/news/2018/08/uganda-changing-face-political-opposition-180821104936104.html>

⁴⁶ *Freedom of the Net, Uganda 2017*, <https://freedomhouse.org/report/freedom-net/2017/uganda>

In May 2018, the Uganda government passed a widely opposed amendment to the Excise Duty Act,⁴⁷ introducing an excise tax of UGX 200 (USD 0.05) per user per day for use of Over The Top services such as WhatsApp, Facebook and Twitter.⁴⁸ The law became effective on July 1, 2018. The tax rendered the internet less affordable for Ugandans, particularly low income earners.⁴⁹ Over and above that, Museveni has been outspoken about people using social media to spread what he terms gossip and lies, and as such the tax can be seen as a move to stem freedom of expression.⁵⁰ In August 2018, there were protests following the arrest and detention of four opposition Members of Parliament, including Robert Kyagulanyi, a.k.a. Bobi Wine, the self-styled "ghetto president".⁵¹ The MPs were part of a group of 33 charged with treason, a charge widely viewed as politically motivated and aimed at silencing prominent critics of the president. These developments raised tensions and sparked protests in parts of the country.

In Tanzania, the government has also come under growing criticism for muzzling free speech. The government continued to implement the restrictive Cybercrimes Act 2015 and the Media Services Act 2016; suspended critical newspapers such as Mawio and Mwanahalisi for two years,⁵² arrested a local rapper, Ney wa Mitego over a song critical of President John Pombe Magufuli;⁵³ prosecuted social media users for insulting the president;⁵⁴ and arrested and prosecuted the founders of JamiiForums.⁵⁵ In March 2018, Tanzania introduced a new regulation⁵⁶ which requires online content creators⁵⁷ to pay application fees of TZS 100,000 (USD 43.7), initial three year license fees of TZS 1,000,000 (USD 437) and renewal fees of a similar amount. The penalty for non-compliance fine of TZS 5,000,000 (USD 2,186). The regulations require persons to furnish ownership details in order to obtain an operating licence. In May 2018, human rights activists obtained an injunction halting the application of the regulations citing the law as an affront to free speech.⁵⁸ The injunction was overturned in May 2018,⁵⁹ and implementation of the regulations halted the operations of some bloggers, including popular online platform JamiiForums which ceased operations for some time in order to avoid the punitive actions under the law.⁶⁰ Tanzania subsequently published a list of 148 licensed online content services providers, who included Jamii Forums.⁶¹

Meanwhile, Rwanda's president Paul Kagame secured a third five-year term in August 2017 with 99% of the votes cast. Under a 2015 constitutional amendment which Kagame's critics opposed, but got approval from 98% of voters, the two-term limit for president was amended to enable Kagame to extend his 17 years' stay in office from 2017, for possibly another 10 years.⁶² The National Election Commission (NEC) disqualified three opposition candidates

⁴⁷ Excise Duty (Amendment) Bill 2018, <http://parliamentwatch.ug/wp-content/uploads/2018/05/L-03-04-18-The-Excise-Duty-Amendment-Bill-2018.pdf>

⁴⁸ Defined as "the transmission or receipt of voice or messages over the internet protocol network and includes access to virtual private networks but does not include educational or research sites prescribed by the Minister by notice in the Gazette."

⁴⁹ Alliance For Affordable Internet, Uganda: New social media tax will push basic connectivity further out of reach for millions, <https://cipesa.org/2018/06/uganda-new-social-media-tax-will-push-basic-connectivity-further-out-of-reach-for-millions/>

⁵⁰ BBC News, Anger at Uganda's tax on social media, <https://www.bbc.com/news/world-africa-44682345>

⁵¹ Uganda's Bobi Wine: Pop star MP charged with treason <https://www.bbc.com/news/world-africa-45282125>

⁵² Tanzanian newspaper suspended for 'insulting president' https://www.newvision.co.ug/new_vision/news/1461956/tanzanian-newspaper-suspended-insulting-president

⁵³ Tanzanian rapper held for 'insulting' President Magufuli in song <https://www.standardmedia.co.ke/article/2001234214/tanzanian-rapper-held-for-insulting-president-magufuli-in-song>

⁵⁴ Five charged with "insulting Magufuli" on social media <https://www.businessdailyafrica.com/news/Five-charged-with--insulting-Magufuli--on-social-media/539546-3381908-hcv6ffz/index.html>

⁵⁵ Tanzanian police charge Jamii Forums founder <https://www.bbc.com/news/world-africa-38341151>; Tanzanian Court Acquits Jamii Forums Founders on One of Three Charges <https://cipesa.org/2018/06/tanzanian-court-acquits-jamii-forums-founders-on-one-of-three-charges/>; Freedom House, Freedom of the world, Freedom House. <https://freedomhouse.org/report/freedom-world/2018/tanzania>

⁵⁶ the Electronic and Postal Communications (Online Content) Regulations 2018, https://www.tcra.go.tz/images/documents/regulations/SUPP_GN_NO_133_16_03_2018_EPOCA_ONLINE_CONTENT_REGULATIONS_2018.pdf

⁵⁷ The law applies to bloggers, internet cafes, online content hosts, online forums, online radio or television, social media and subscribers and users of the internet.

⁵⁸ Reuters, Tanzania bloggers win temporary court order against state crackdown, <https://www.reuters.com/article/us-tencent-holdings-gaming/tencent-to-put-new-checks-on-hit-game-amid-china-crackdown-on-gaming-idUSKCN1LM0K0>

⁵⁹ Tanzania government wins court case to impose online regulations <http://www.theeastafrican.co.ke/news/ea/Tanzania-government-wins-court-case-to-impose-online-regulations/4552908-4587076-i8espo/index.html>

⁶⁰ The Great Silencing, or why I stopped blogging <http://www.theeastafrican.co.ke/oped/comment/Why-I-stopped-blogging-Tanzania/434750-4748244-y548qyz/index.html>; Tanzania: Jamii Forum Founder Speaks Out On Decision to Close Site <https://allafrica.com/stories/201806120534.html>

⁶¹ https://www.tcra.go.tz/images/headlines/Licensed_Online_Content_Service_Providers__31st_July_2018.pdf

⁶² The changes made to Rwanda's constitution are peculiar – here's why, available here: <http://theconversation.com/the-changes-made-to-rwandas-constitution-are-peculiar-heres-why-53771>

including the only woman, outspoken opposition leader and Kagame critic, Diane Rwigara, despite her insistence that she met all the requirements to run.⁶³ The government orchestrated a campaign of media smears and intimidation against her, and later in September 2017, arrested and detained her along with her mother and sister on charges of forgery, tax evasion and inciting insurrection, charges the family believes are politically motivated.⁶⁴ In June 2018, the Rwanda Revenue Authority sold Rwigara's family assets for USD 2 million in order to recover USD 7 million in alleged tax arrears.⁶⁵ Other members of banned opposition groups have been reported to have faced arbitrary arrests, beatings, politicised prosecutions, and enforced disappearances.⁶⁶

In Malawi, there have been concerns over the implementation of the Consolidated ICT Regulatory Management System (CIRMS), also known as the “spy machine”, which was implemented in September 2017.⁶⁷ Civil society and telcos challenged its implementation in courts, all the way to the Supreme Court of Appeal, since it was first announced in 2011, reasoning that it could be used to monitor and surveil private electronic communications such as phone calls and text messages.⁶⁸ The government, in whose favour the apex court ruled in June 2017, claims the system aimed to enable MACRA to be updated on the quality of service of mobile phone operators, revenue assurance, fraud and spectrum management. Many Malawians do not feel comfortable criticising the government and thus engage in self-censorship. The government has specifically targeted online activities, including arresting three opposition members in February 2016 based on a private WhatsApp group chat and charging them with treason in October 2016, over an alleged scheme to unseat president Peter Mutharika.⁶⁹ The charges were dropped in March 2017 after failure by the state to bring them to court a year after the arrests.⁷⁰

Since a failed coup in 2015, Burundi has stepped up the persecution of those suspected of opposing president Pierre Nkurunziza. In September 2017, a United Nations Commission of Inquiry on Burundi confirmed the persistence of extrajudicial executions, arbitrary arrests and detentions, enforced disappearances, torture and cruel, inhuman or degrading treatment and sexual violence in Burundi committed by members of the National Intelligence Service, the police, the army and the youth league of the ruling party, commonly known as the Imbonerakure.⁷¹

Similarly, Nkurunziza has tightened control over independent media and critical online publishers.⁷² Frivolous sanctions have been slapped against media houses, access to some online publishers' websites restricted. For example, CCIB FM+, a media outlet, was suspended in September 2017 after it broadcast an editorial critical of the government's response to the shooting of 36 Burundian refugees by security forces in the DRC.⁷³ In April 2018, the Media Regulator CNC, suspended the online commentary column of the Iwacu newspaper for three months.⁷⁴ In May 2018, an obnoxious law was enacted that makes it easier for security agencies to seize computer data in real time and conduct surveillance and intercept citizens' communications with little judicial oversight.⁷⁵

The DRC, meanwhile, is preparing for general elections scheduled for December 23, 2018. The August 2018 announcement by president Joseph Kabila, in power since 2001 in that he would not vie for re-election, was welcomed by many.⁷⁶ Kabila's last term officially ended in December 2016. Kabila's government has a long history of stifling media freedom, freedom of expression and of assembly. In the past, the government has ordered Internet

⁶³ Three Rwandan Presidential Candidates Disqualified Amid Criticism <https://www.voanews.com/a/three-rwandan-presidential-candidates-disqualified/3933118.html>

⁶⁴ Rwandan court refuses bail for Diane Rwigara <https://www.nation.co.ke/news/africa/Court-refuses-bail-for-Diane-Rwigara/1066-4152944-okaco0/index.html>

⁶⁵ Diane Rwigara: Rwandan politician's assets auctioned <https://www.bbc.com/news/world-africa-44521197>

⁶⁶ Freedom of the World, Rwanda 2017. <https://freedomhouse.org/report/freedom-world/2018/rwanda>

⁶⁷ Freedom of the world, Malawi 2018 <https://freedomhouse.org/report/freedom-world/2018/malawi>

⁶⁸ 'Spy machine' roll out in September, says Malawi regulator, <https://www.nyasatimes.com/spy-machine-roll-september-says-malawi-regulator/>

⁶⁹ Freedom of the Net, Malawi 2016 <https://freedomhouse.org/report/freedom-net/2016/malawi>

⁷⁰ Treason charges dropped against Kabwila, two others <https://malawi24.com/2017/03/29/treason-charges-dropped-kabwila-two-others/>

⁷¹ Report of the Commission of Inquiry on Burundi, Human Rights Council https://reliefweb.int/sites/reliefweb.int/files/resources/G1723746_0.pdf

⁷² A New Interception Law and Blocked Websites: The Deteriorating State of Internet Freedom in Burundi

<https://cipesa.org/2018/07/a-new-interception-law-and-blocked-websites-the-deteriorating-state-of-internet-freedom-in-burundi/>

⁷³ Burundi radio station suspended for criticising killings

<https://www.nation.co.ke/news/africa/Burundi-radio-station-suspended-criticising-killings/1066-4118228-dxgn1o/index.html>

⁷⁴ CNC suspends commentary column of Iwacu newspaper <http://www.iwacu-burundi.org/englishnews/cnc-suspends-commentary-column-of-iwacu-newspaper-2/>

⁷⁵ Law No 1/09 of May 11 2018 <http://www.assemblee.bi/IMG/pdf/9%20du%2011%20mai%202018.pdf>

⁷⁶ DR Congo's Kabila will not stand for re-election: spokesman <https://www.aljazeera.com/news/2018/08/drc-kabila-stand-election-spokesman-180808130105604.html>

shutdowns or restrictions of access to certain online applications and services, citing the need to protect public order and national security. These network disruptions were ordered at election times or during demonstrations to protest Kabila's continued stay in power despite the end of his constitutional term. The government closed radio and television stations critical of government such as Nyota TV and Radio Télévision Mapendo in January 2016,⁷⁷ while Radio Television Lubumbashi Jua (RTLJ), Radio Télévision Graben Beni, Radio Liberté Beni, Radio Télévision Rwanzururu, Radio Ngoma, Radio Furu and Radio Equateur were shut down in November 2014.⁷⁸

In Nigeria, there is elevated political tension as the country gears up for a general election in February 2019, in which the incumbent, president Muhammadu Buhari, will seek a second term.⁷⁹ There had been concerns regarding his health following a long absence from office in early 2017 for unspecified medical checks, leading to street protests calling for a change of government.⁸⁰ A number of the political parties are witnessing maneuvering as top politicians defect mostly from the ruling All Progressives Congress (APC) to the former ruling party, the People's Democratic Party (PDP). There is concern that discussions about the economy have taken a back seat as politics takes the centre stage. Many are keen to see how well prepared the National Electoral Commission will be for the general election. President Buhari's government is still struggling to deal with formidable challenges such as public mistrust of the government; addressing corruption; energy sector reforms; tackling poverty and ineffective service delivery; and insecurity including terrorist attacks especially from the insurgent Boko Haram; and kidnapping.⁸¹

Ghana's strong democratic credentials continue to ensure political stability. The west African country held its seventh successive peaceful general elections in 2016 that brought the then major opposition party, the New Patriotic Party, to power. The current president, Nana Akufo-Addo, a human rights lawyer, won the presidential election with 53.8% of the vote, defeating incumbent John Mahama after a hotly-contested race.⁸² In Ghana, human rights and the rule of law are largely respected with the judiciary generally regarded as independent, and enjoying public trust. The media enjoys a relatively high degree of freedom, as private press and broadcasters operate without significant restrictions.⁸³ However, government agencies have been reported to sometimes harass and arrest journalists, especially those reporting on politically sensitive issues, and political corruption continues to undermine government performance.⁸⁴

Likewise, Senegal has had a vibrant democracy with a tradition of stable governments and civilian rule, and is the only country in West Africa that has never undergone a coup. Current president Macky Sall won the run-off in the January 2012 elections, defeating former ally, president Abdoulaye Wade, who was running for a controversial third term.⁸⁵ Sall has since reduced the presidential term from seven years to five, setting an example in the continent where term limits are frequently extended. Further, under his leadership, the separatist conflict in the southern Casamance region has reduced, while a ceasefire was declared by rebel leader Salif Sadio in 2014. The country's media is generally diverse and unrestricted. While the judiciary is independent, it is inadequately resourced and subject to external influences.⁸⁶ Further, corrupt practices such as bribery and impunity of government officials remains a problem, despite government commitment to be transparent and to promote good governance.⁸⁷

⁷⁷ Reporters Without Borders, Government closes two opposition TV stations in Lubumbashi <https://rsf.org/en/news/government-closes-two-opposition-tv-stations-lubumbashi>

⁷⁸ CPI, Authorities order radio stations to be closed in the DRC <https://cpj.org/2014/11/authorities-order-radio-stations-to-be-closed-in-t.php>

⁷⁹ Nigeria: Economic Reforms Suffer As Politics Take Centre Stage <https://allafrica.com/stories/201808060053.html>

⁸⁰ Nigeria's president 'hale and hearty', says deputy amid health doubts

<https://www.reuters.com/article/us-nigeria-president/nigerias-president-hale-and-hearty-says-deputy-amid-health-doubts-idUSKBN15L23L>

⁸¹ U.S. Relations With Nigeria <https://www.state.gov/r/pa/ei/bgn/2836.htm>; Nigeria Economic Outlook 2018

<https://www.gibs.co.za/news-events/news/Pages/Nigeria-Economic-Outlook-2018.aspx>

⁸² Ghana country profile <https://www.bbc.com/news/world-africa-13433790>

⁸³ The World Bank In Ghana <http://www.worldbank.org/en/country/ghana/overview>

⁸⁴ Freedom in the World 2018 Ghana <https://freedomhouse.org/report/freedom-world/2018/ghana>

⁸⁵ Macky Sall Senegal election win 'example for Africa' <https://www.bbc.com/news/world-africa-17514525>

⁸⁶ Senegal <https://www.heritage.org/index/country/senegal>

⁸⁷ Department of State: 2014 Investment Climate Statement <https://www.state.gov/documents/organization/228812.pdf>

Zambia has also been politically stable although government is increasingly hostile to the media and the political opposition. In April 2017, opposition leader Hakainde Hichilema was arrested, charged with treason and detained for four months after his convoy failed to move aside for president Edgar Lungu's motorcade.⁸⁸ Following his arrest, the government imposed a 90-day state of emergency, which was extended for a similar period to "restore public order" following rising tensions.⁸⁹ Lungu narrowly won the August 2016 presidential poll, which was characterised by election-related violence, government restrictions on opposition-aligned media, misuse of public resources by the ruling Patriotic Front (PF) party, and the use of the Public Order Act to restrict opposition rallies. Government accountability is weak, official corruption is widespread, and impunity is common.⁹⁰

Media and internet freedom in the country are weak with clampdowns on online critics on the rise. During the August 2016 election period, the government was suspected of causing internet disruptions in opposition strongholds.⁹¹ In April 2017, opposition leader Chilufya Tayali was arrested and charged for libel over a post on Facebook critical of the police following Hichilema's arrest.⁹² In January 2018, a medical doctor was sentenced to three years imprisonment for defaming the president on Facebook.⁹³ In December 2017, the government announced that it would develop new laws to curb social media "abuse",⁹⁴ having warned the public against misusing social media.⁹⁵ However, the government cited proliferation of cybercrimes, pornography, identity theft, hate speech, insults, and fraud as justifications for the prospective new laws, which as of August 2018 were yet to be drafted.⁹⁶ In April 2018, government announced that it would introduce a 30 Ngwee (USD 0.03) a day tariff on internet phone to be charged through mobile network operators and internet service providers. The government expects to collect K300 million (USD 25.8 million) annually from the tax.

It has been a beehive of political activities across the continent, and with more elections expected in the coming months, the situation is expected to continue. Unfortunately, little movement has been experienced on the side of respect for human rights, as governments have become more retrogressive in an effort to entrench themselves in power. There has been more arrests and intimidation of critical voices across the board, and with the internet offering a safe space for opposition and critical organising, governments in the region have turned considerable attention to patrolling and controlling that space.

⁸⁸ Zambia opposition leader Hakainde Hichilema released <https://www.bbc.com/news/world-africa-40945825>

⁸⁹ Zambia extends state of emergency by three months - presidency office <https://reut.rs/2NEgr6E>

⁹⁰ Freedom in the World 2018 - Zambia <https://freedomhouse.org/report/freedom-world/2018/zambia>

⁹¹ Zambian government suspected of causing internet shutdown following outage in opposition strongholds <https://bit.ly/2Q6laLt>

⁹² Zambian opposition leader arrested over 'libelous' Facebook post <https://bit.ly/2xyuctG>

⁹³ Mongu Doctor jailed for three years for insulting President Lungu on Facebook <https://bit.ly/2xMwSTJ>

⁹⁴ Mushimba explains 5 social media bills <https://bit.ly/2ld0b6V>

⁹⁵ Kampyongo warns of stern action against individuals abusing social media <https://bit.ly/2pxWjFd>

⁹⁶ Zambia planning social media clampdown <https://bit.ly/2MZ7EqR>

4 Laws and Policies Affecting Privacy and Personal Data Protection

This section provides an overview of international and regional human rights instruments as well as national laws and policies relevant to privacy and data protection. It highlights sections of these laws and how they define the right to privacy and limit the right, including the justifications provided. It reminds the countries studied of the obligations at the national, regional and international levels to ensure that privacy and data protection are respected across all domains. The section also makes strides in highlighting key principles to be imbedded in the legislative and policy frameworks on privacy and data protection.

4.1 International Framework for the Protection of Privacy

The right to privacy is enshrined in various international human rights instruments. These include the Universal Declaration of Human Rights (UDHR); International Covenant on Civil and Political Rights (ICCPR); UN Convention on the Rights of the Child (UNCRC); and the United Nations Convention on Migrant Workers (CMW). These instruments adopt the same language and definition of privacy.

Article 12 of the UDHR provides that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”⁹⁷ Article 17 of the ICCPR provides that: “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 reputation. Everyone has the right to the protection of the law against such interference or attacks.” The UNCRC recognises in Article 16 that children have a right to privacy, and that the law should protect them from “attacks against their way of life, their good name, their families and their homes.”⁹⁸ Article 14 of the CMW provides that “No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications”.⁹⁹ The explicit inclusion of the right to privacy as part of the body of international human rights instruments confirms the importance of the right to humanity in general.

Other key UN institutions have articulated the right to privacy, including the Human Rights Committee which in April 1988, in its General Comment No. 16, stated that the right to privacy under Article 17 of the ICCPR required states “to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.”

⁹⁷ UDHR, <http://www.un.org/en/universal-declaration-human-rights/>

⁹⁸ UNCRC, https://www.unicef.org/crc/files/Rights_overview.pdf

⁹⁹ UNCMW, <https://www.ohchr.org/en/professionalinterest/pages/cmw.aspx>

Further, given recent technological developments, in December 2013 the United Nations General Assembly adopted Resolution 68/167, affirming that the rights held by people offline must also be protected online.¹⁰⁰ The Resolution called upon all states to respect and protect the right to privacy in digital communications. It further called on all states to “review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasised the need for States to ensure the full and effective implementation of their obligations under international human rights law”.

Likewise, the December 2014 UN Resolution 69/166 on Privacy in the Digital Age affirmed that the same rights that people have offline must also be protected online, including the right to privacy.¹⁰¹ It called upon all states “to respect and protect the right to privacy, including in the context of digital communication” and “to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.” In March 2017, the Human Rights Council reiterated previous UN Resolutions on the right to privacy in the digital age.¹⁰² The Council called upon business enterprises to “meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights” and to “work towards enabling technical solutions to secure and protect the confidentiality of digital communications.”

A December 2014 report of the Human Rights Council panel discussion on the right to privacy noted that there is a need “for better implementation at the national level of the international norms related to the right to privacy, through adequate national legislation and stronger safeguards and oversight.”¹⁰³ Of the countries in this study, only Senegal has signed or ratified the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.¹⁰⁴ The convention has been ratified or acceded to by 53 states. Two African countries, Senegal and Tunisia, have acceded to the Convention, while Burkina Faso and Morocco have been invited to either sign, ratify, or accede to the convention.¹⁰⁵ A number of these instruments while persuasive, are not binding or enforceable in the countries studied.

4.2 African Instruments on Privacy and Personal Data Protection

In Africa, regional economic communities have taken measures to protect privacy and personal data. The African Union (AU) has also taken steps to strengthen privacy and personal data protection, in a bid to support the establishment of specific legal regimes in African countries.

The East African Community (EAC) has not adopted a specific framework on data protection and privacy, but it was the first African regional economic community to develop a framework for cyber laws.¹⁰⁶ In 2008, it developed the Framework for Cyber laws to guide its Member States on regional and national processes in order to facilitate a harmonised legal regime on electronic commerce and to curb unlawful conduct.¹⁰⁷ The framework law calls upon member states to enact laws that protect personal data. As a result of this initiative at the time, Burundi and Kenya developed draft legislation on privacy and data protection in 2012, while Rwanda’s Telecommunications law was amended in the same year to include provisions on privacy and data protection.¹⁰⁸

¹⁰⁰ Resolution 68/167, UN General Assembly. <http://undocs.org/A/RES/68/167>

¹⁰¹ Resolution 69/166, UN General Assembly. http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y

¹⁰² Human Rights Council, *The Right to Privacy in the Digital Age*. <https://bit.ly/2xDfKAX>

¹⁰³ Summary of the Human Rights Council panel discussion on the right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39

¹⁰⁴ Text of the Convention, <https://rm.coe.int/1680078b37>

¹⁰⁵ Chart of signatures and ratifications of Treaty 108, <https://bit.ly/2JPrMPR>; Non-member Invitation, <https://bit.ly/2O7paOf>

¹⁰⁶ Harmonizing Cyberlaws and Regulations: The experience of the East African Community, UNCTAD. http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf

¹⁰⁷ Draft EAC legal framework for cyberlaws. <https://bit.ly/2IhhR1i>

¹⁰⁸ *Ibid*

In February 2010, the Economic Community of West African States (ECOWAS) adopted the Supplementary Act on Personal Data Protection Within ECOWAS.¹⁰⁹ The Act urges member states to establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the state. It also provides for definition of key terms; required formalities for executing data processing; the institutional framework for the protection of data (calling for each state to establish its own independent data protection authority); and the principles guiding the processing of personal data, including consent, legality, fairness, occurrence, purpose, transparency, confidentiality and security, and exceptions. rights of individuals whose personal data are the subject of processing, to information, access, objection, rectification and destruction; and the obligations of personal data controllers, including confidentiality, security, preservation and durability. Supplementary Acts such as this one are binding on member states and the institutions of the Community.¹¹⁰

Similarly, in November 2012, the SADC ministers responsible for ICT adopted a model law on data protection to assist member states to prevent the violations of privacy likely to arise from the collection, processing, transmission, storage and use of personal data, and to protect the related rights of the data subject.¹¹¹ The model law provides for key definitions; an independent data protection authority; general rules on the processing of data, including data quality to ensure lawful and fair data processing; and duties of data controllers and data processors, to promote data security, transparency and accountability. It also provides for rights of data subjects, including to access, rectification, deletion of data, temporary limitation of access to data and to representation in the case of minors; recourse to judicial authority; sanctions for violation of the law; limitation of the right to preserve state security, defence, public safety and criminal investigations; transborder flows; code of conduct; for controllers; and, rules governing whistleblowing. Southern African countries such as Angola, Lesotho and South Africa have enacted privacy laws.¹¹²

At the AU level, the Constitutive Act of the African Union¹¹³ commits the AU to promote and protect human and peoples' rights in accordance with the African Charter on Human and Peoples' Rights and other relevant human rights instruments; and recognises human rights as a core principle to guide its functions. However, the African Charter on Human and Peoples Rights, which was adopted in 1981 and came into force in 1986, does not explicitly recognise the right to privacy.¹¹⁴ This omission makes the continent's foremost human rights instrument inadequate to safeguard the right to privacy and as such, it falls short of international human rights standards with respect to this right.

Nonetheless, in June 2014 AU member states adopted the African Union Convention on Cybersecurity and Personal Data Protection (also referred to as the Malabo Convention), making it the first pan-African instrument on privacy and personal data protection.¹¹⁵ The convention addresses electronic transactions, personal data protection, cybersecurity and cybercrime, taking into account the requirements to respect the rights of citizens in various international human rights treaties and conventions, including the African Charter. In particular, Article 8 of the convention calls upon state parties to commit to establish a "legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data." The convention also outlines internationally recognised principles in personal data collection, storage and processing.

Unfortunately, since its adoption in June 2014, only 10 of the AU's 55 member states have signed the convention: Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia. So far, only Mauritius and Senegal have ratified it, meaning the convention is unenforceable since it requires a minimum of 15 ratifications in order to enter into force. Of the countries under this study, only Ghana, Senegal and Zambia have

¹⁰⁹ Text of Act, <https://ccdcoe.org/sites/default/files/documents/ECOWAS-100216-PersonalDataProtection.pdf>

¹¹⁰ Supplementary Acts/Protocols, ECOWAS. <http://www.ecowas.int/ecowas-law/find-legislation/>

¹¹¹ SADC Model Law on Data Protection, <https://bit.ly/2QWim4D>

¹¹² Privacy is Paramount: Personal Data Protection in Africa <https://bit.ly/2ldfBrI>

¹¹³ See Act, <http://www1.uneca.org/Portals/ngm/Documents/Conventions%20and%20Resolutions/constitution.pdf>

¹¹⁴ African Charter, <https://bit.ly/1KvVTQf>

¹¹⁵ AUCC, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

signed the convention.¹¹⁶ The slow pace of adoption has been attributed to privacy and data protection not being priorities for many African governments and because that the convention included too many aspects in the same instrument.¹¹⁷

In May 2018, the African Union Commission (AUC) launched the Personal Data Protection Guidelines for Africa, which were developed jointly with the Internet Society (ISOC).¹¹⁸ The guidelines emphasise the importance of ensuring trust in online services and set out 18 recommendations for governments and policymakers, data protection authorities (DPAs), data controllers and their partners, and citizens and civil society based on the multi-stakeholder model. The guidelines also provide essential principles relating to online personal data protection including: consent and legitimacy; fair and lawful processing; purpose and relevance of data; management of the data lifecycle (retention, accuracy, deletion); transparency of processing; and, confidentiality and security of personal data. It remains to be seen how they will be received and implemented by states.

Other relevant instruments that provide for the right to privacy include the African Charter on the Rights and Welfare of the Child (article 10); the African Union Principles on Freedom of Expression (the right of access to information) (article 4); the Declaration of Principles on Freedom of Expression in Africa (2002) (Part V);¹¹⁹ and, the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa 2016.¹²⁰

4.3 National Constitutional Frameworks for the Protection of Privacy

At the national constitutions of the countries under review have provisions on protecting the right to privacy (see Table 3 below). With the exception of Burundi, they all have constitutional provisions on the rights to freedom of expression and the right to information.

Figure 3: Constitutional Provisions on the Right to Privacy

Definition of Privacy and Data Protection in Constitution

No one may be the object of arbitrary intrusion into his or her private life, family, domicile or his or her correspondence, nor attacks against his or her honor or reputation.

Police searches or home visits by enforcement may not be ordered except in the forms and conditions provisioned by the law. Privacy in one's correspondence and communications is guaranteed, respecting the forms and conditions determined by the law.

Burundi

Article 43¹²¹

DR Congo

Article 31¹²²

All persons have the right to the respect of their private life and to the secrecy of their correspondence, of telecommunications and of any other form of communication.

This right may only be infringed in the cases specified by the law.

Ethiopia

Article 26¹²³

1. Everyone has the right to privacy. This right shall include the right not to be subjected to searches of his home, person or property, or the seizure of any property under his personal possession.

2. Everyone has the right to the inviolability of his notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices.

3. Public officials shall respect and protect these rights. No restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.

Ghana

Article 18¹²⁴

No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

¹¹⁶ Status list, https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf

¹¹⁷ Scarcity of data protection laws in Africa leaves NGOs exposed, <https://www.devex.com/news/scarcity-of-data-protection-laws-in-africa-leaves-ngos-exposed-93008>

¹¹⁸ The Guidelines https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

¹¹⁹ See: <http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html>

¹²⁰ See: <http://www.achpr.org/sessions/59th/resolutions/362/>

¹²¹ Constitution of Burundi, https://www.constituteproject.org/constitution/Burundi_2005.pdf

¹²² Constitution of the DRC 2005 (rev. 2011) https://www.constituteproject.org/constitution/Democratic_Republic_of_the_Congo_2011?lang=en

¹²³ Constitution of Ethiopia, <http://www.wipo.int/edocs/lexdocs/laws/en/et/et007en.pdf>

¹²⁴ Constitution of Ghana, https://www.constituteproject.org/constitution/Ghana_1996?lang=en

 <p>Kenya Article 31¹²⁵</p>	<p>Every person has the right to privacy, which includes the right not to have—</p> <ul style="list-style-type: none"> (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed.
 <p>Malawi Article 21¹²⁶</p>	<p>Every person shall have the right to personal privacy, which shall include the right not to be subject to -</p> <ul style="list-style-type: none"> (a) searches of his or her person, home or property; (b) the seizure of private possessions; or (c) interference with private communications, including mail and all forms of telecommunications.
 <p>Nigeria Article 37¹²⁷</p>	<p>The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.</p>
 <p>Rwanda Article 23¹²⁸</p>	<p>The privacy of a person, his or her family, home or correspondence shall not be subjected to interference in a manner inconsistent with the law; the person's honour and dignity shall be respected.</p> <p>A person's home is inviolable. No search or entry into a home shall be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by the law.</p> <p>Confidentiality of correspondence and communication shall not be waived except in circumstances and in accordance with procedures determined by the law.</p>
 <p>Senegal Article 13¹²⁹</p>	<p>The secrecy of correspondence and of postal, telegraphic, telephonic or electronic communications shall be inviolable. This inviolability shall be subject only to such restrictions as are made applicable by law.</p>
 <p>Tanzania Article 16¹³⁰</p>	<ul style="list-style-type: none"> (1) Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications. (2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.
 <p>Uganda Article 27¹³¹</p>	<ul style="list-style-type: none"> (1) No person shall be subjected to— (a) unlawful search of the person, home or other property of that person; or (b) unlawful entry by others of the premises of that person. (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.
 <p>Zambia Article 17</p>	<ul style="list-style-type: none"> 1. Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises. 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this Article to the extent that it is shown that the law in question makes provision— a) that is reasonably required in the interests of defence, public safety, public morality, public health, town and country planning, the development and utilisation of mineral resources, or in order to secure the development or utilisation of any property for a purpose beneficial to the community; b) that is reasonably required for the purpose of protecting the rights or freedoms of other persons; c) that authorises an officer or agent of the Government, a local government authority or a body corporate established by law for a public purpose to enter on the premises or anything thereon for the purpose of any tax, rate or due or in order to carry out work connected with any property that is lawfully on those premises and that belongs to that Government, authority, or body corporate, as the case may be; or d) that authorises, for the purpose of enforcing the judgement or order of a court in any civil proceedings, the search of any person or property by order of a court or entry upon any premises by such order;
 <p>Zimbabwe Article 57¹³²</p>	<p>Every person has the right to privacy, which includes the right not to have--</p> <ul style="list-style-type: none"> (a) their home, premises or property entered without their permission; (b) their person, home, premises or property searched; (c) their possessions seized; (d) the privacy of their communications infringed; or (e) their health condition disclosed.

¹²⁵ Constitution of Kenya, <http://www.kenyalaw.org/lex/actview.xql?actid=Const2010>

¹²⁶ Constitution of Malawi, <http://www.wipo.int/edocs/lexdocs/laws/en/mw/mw002en.pdf>

¹²⁷ Constitution of Nigeria, https://www.constituteproject.org/constitution/Nigeria_2011?lang=en

¹²⁸ Constitution of Rwanda, https://www.constituteproject.org/constitution/Rwanda_2015.pdf?lang=en

¹²⁹ Constitution of Senegal <http://www.wipo.int/edocs/lexdocs/laws/en/sn/sn006en.pdf>

¹³⁰ Constitution of Tanzania, <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan040857.pdf>

¹³¹ Constitution of Uganda, <https://ulii.org/ug/legislation/consolidated-act/0>

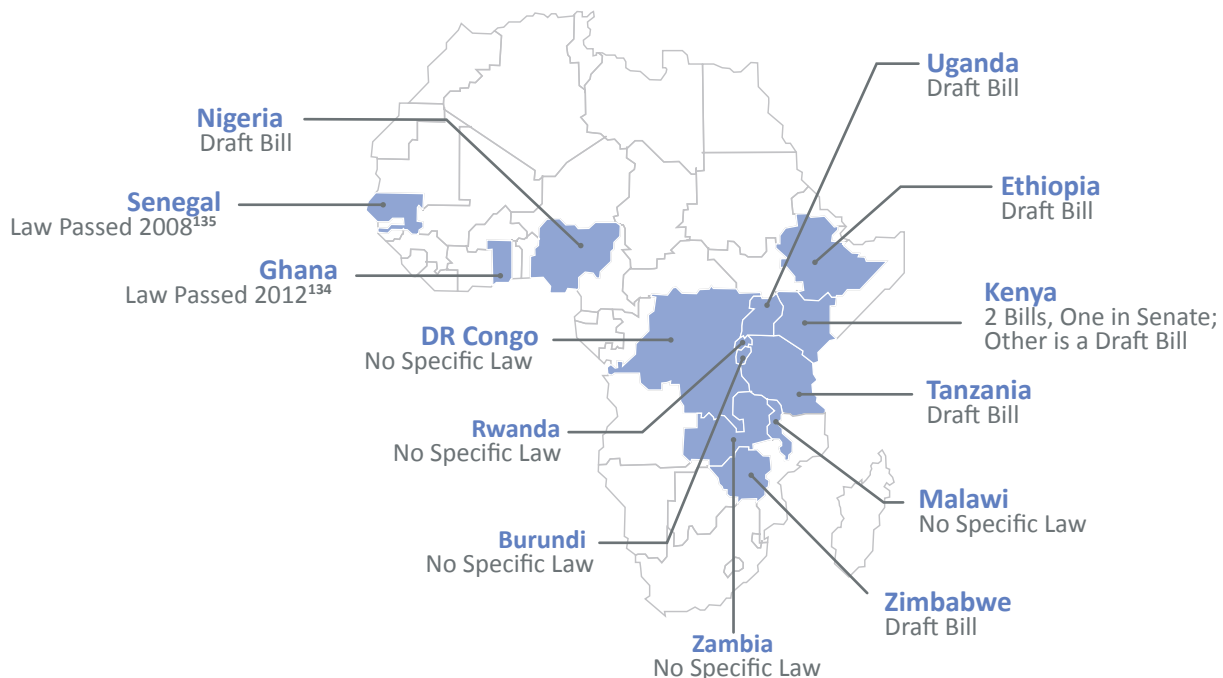
¹³² Constitution of Zimbabwe, https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf

A review of these provisions indicates a general protection of the right to privacy with specific context differences. The key aspect that is restricted across all the constitutions is arbitrary searches and seizures of home and property; and the infringement of privacy of communication or correspondence.

4.4 Legal Frameworks for Privacy and Data Protection Laws and Policies

There are 22 African countries that have enacted comprehensive personal data protection legislation, namely Angola, Benin, Botswana, Burkina Faso, Chad, Cape Verde, Côte d'Ivoire, Equatorial Guinea, Gabon, Ghana, Lesotho, Madagascar, Mali, Mauritius, Mauritania, Morocco, Senegal, Seychelles, South Africa, Tunisia, Zambia, and Zimbabwe.¹³³ Of the countries currently under review, only Ghana and Senegal have comprehensive privacy and data protection laws, while Zambia has provisions on privacy and data protection covered in other legislation. Most of the other countries have various aspects of the right to privacy covered in separate legislation. Others, such as Ethiopia, Kenya, Nigeria, Tanzania, Uganda, and Zimbabwe, have draft privacy and data protection legislation. Table 4 below, shows the status of privacy and data protection legislation.

Figure 4: Status of Privacy and Data Protection Laws



In each of the countries studied, there are various laws that provide for the protection of privacy and personal data. These include laws on access to information; anti-terrorism; interception of communications; intelligence and security services law; ICT and telecoms; Cyber Crime; electronic communication, and electronic transactions.

¹³³ Deloitte, *Privacy is Paramount Personal Data Protection in Africa*

https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

¹³⁴ Data Protection Act 2012 <https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf>

¹³⁵ Data Protection Act Law No. 2008-12 http://www.wipo.int/wipolex/en/text.jsp?file_id=181186

4.5 Recognition of Personal Data in Statutes

The term personal data is defined in various ways in existing legislation. The laws do not distinguish between the protections of privacy and data protection online and offline.

In section 96, Ghana's Data Protection Act, 2012 defines personal data as "data about an individual who can be identified, from the data, or from the data or other information in the possession of, or likely to come into the possession of the data controller." It also creates a category of personal data known as special personal data, which is personal data that includes information relating to race, colour, ethnic or tribal origin of the data subject; the political opinion of the data subject; and the person's religious beliefs or other beliefs of a similar nature; the physical, medical, mental health or mental condition or DNA of the data subject. It also includes data on the person's sexual orientation, among others.

Senegal's Personal Data Protection Act 2008, in its Article 4 defines personal data as "any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or one or more elements, specific to its physical, physiological, genetic, psychic, cultural, social or economic identity."

The Rwandan ICT law defines personal data as "any information relating to an identified or identifiable natural person by reference to any number of his/her identifications or to his or her physical, physiological, mental, economic, cultural or social identity".¹³⁶ Likewise, Malawi's Electronic Transactions Act, 2016 defines personal data as any information relating to an individual who may be directly identified; or if not directly identified, may be identifiable by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social, or economic identity.

The term "personal data" is not included in Zambia or Zimbabwe's legislation. Section 2 of Zimbabwe's Access to Information and Protection of Privacy Act (AIPPA) however, defines the term "personal information" as "recorded information about an identifiable person", which may include names; addresses; contact details; race; marital status; gender; sexual orientation, blood type; fingerprints; identifying numbers or symbols; health care history, financial, opinions about the individual, personal views or opinions, personal correspondence, home and family. Zambia's Electronic Communications Act No. 21 of 2009 has a similar provision.¹³⁷

Nigeria's National Information Technology Development Agency (NITDA) Data Protection Guidelines 2017 define personal data as "... any information relating to an identified or identifiable natural person ('data subject'); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others." In Burundi, Ethiopia, Kenya, Uganda, the definitions are varied and are contained in draft legislation that are awaiting adoption by their respective legislatures.

The various laws also provide for principles of data protection, which set the standard for privacy and data protection. For example, section 71 of Malawi's Electronic Transactions Act enshrines principles such as fairness, legality, legitimate purpose, data minimisation, accuracy, correction and retention limitation. Zimbabwe's AIPPA in Part V and VI provides for principles such as accuracy and completeness, correction, data security, retention limitation, consent, legitimate and lawful purpose. However, the provisions regulate data collection and processing by public bodies, as opposed to applying to all persons and entities collecting data. Similar principles are contained in draft legislation in Kenya and Ethiopia.

¹³⁶ Law N°24/2016 du 18/06/2016 governing Information and Communication Technologies, article 5 point 4a, Official Gazette n°26 of 27/06/2016, Herein after ICT Law, http://www.mitec.gov.rw/fileadmin/Documents/Policies_and_Regulations/ICT_laws/ICT_LAW.pdf

¹³⁷ Electronic Communications Act No. 21 of 2009

https://www.unodc.org/res/cld/document/zmb/2009/electronic_communications_and_transactions_act_html/Electronic_Communications_and_Transactions_Act.pdf

4.6 Limitations on the Right to Privacy

The right of privacy has limitations in all the countries studied under their constitutions and statutes. Under Article 17 of Zambia's constitution, the right to privacy may be limited in the interests of defence, public safety, public order, public morality, public health, and protecting the rights or freedoms of other persons. and public health. It may also be limited for reasons ranging from town planning to taxation and mineral resources management.

Ghana's constitution states that limitation to the right to privacy must be "in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others." In Kenya, restrictions to the right to privacy should follow with Article 24 of the constitution, which provides that such limitations must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.

Under its Article 26(3), Ethiopia's constitution states that the right can be restricted only in compelling circumstances and in accordance with specific laws whose purposes are the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others. In Article 45, Nigeria's constitution cites defence, public safety, public order, public morality or public health and for protecting the rights and freedoms of other person as main reasons for derogating from the right to privacy.

In Senegal, the Personal Data Protection Act 2008 in Article 33 stipulates that "the requirement of consent is waived where the processing is necessary: the fulfillment of a legal obligation to which the controller has subscribed; the performance of a public-interest mission or of the public authority, which is entrusted to the controller or to the third party to whom the data are communicated; safeguarding the interest or fundamental rights and freedoms of the data subject."

The DRC's Law on The Framework Law number 013/2002 of October 16th, 2002 on Telecommunications cites limitations to the right to privacy include in instances such as during a trial to prove the truth, to protect the public order, and national security. In Rwanda, the major limitation is "national security", which is described under Article 3 of the Prime Minister's Order No. 90/03 of 11/09/2014 determining the modalities for the enforcement of the law regulating interception of communication.¹³⁸ Article 3 of the law interceptions law n°60/2013 of 22/08/2013 regulating the interception of communications provides that "Interception of communications shall be considered lawful where it is done in the interest of national security and in accordance with this Law."

In Zimbabwe, the right is explicitly limited under the AIPPA and the Interception of Communications Act. Section 25 of Access to Information and Protection of Privacy Act (AIPPA) provides that information may be disclosed where: the disclosure is desirable or necessary for the purpose of subjecting the activities of the government or a public body to public scrutiny; the disclosure is likely to promote public health and safety or the protection of the environment; the personal information is relevant to a fair determination of the applicant's rights; and the disclosure will assist in researching or validating the claims, disputes or grievances of indigenous people [section 25(2)]. Section 6(1) of Zimbabwe's Interception of Communications Act¹³⁹ outlines circumstances under which privacy and data protection may be restricted by allowing for the issuance of warrants to intercept communications in specific circumstances.

¹³⁸ Prime Minister's Order N° 90/03 of 11/09/2014 determining modalities for the enforcement of the Law regulating interception of communication, Article 3, Official Gazette n° 46 of 17/11/2014, <https://bit.ly/2zuRRfjW>

¹³⁹ Interception of Communications Act <https://bit.ly/R5gPZO>

Under section 35 (2) of Kenya's Prevention of Terrorism Act,¹⁴⁰ the right to privacy is limited for purposes of ensuring investigation, detection and prevention of a terrorist act. Section 36A also limits the right for intercepting communication directly relevant in detecting, deterring and disrupting terrorism. Further, the National Intelligence Service Act in section 36 specifically limits the right to privacy in respect of a person who under investigation by the National Intelligence Service or suspected to have committed an offence.

From the foregoing, national security remains the most common justification and basis for the limitation of the right to privacy. Other reasons include the investigation and detection of crime, protection of national interests and the defence of human rights. Whereas these limitations are important for the protection of fundamental rights and freedoms, countries need to ensure that there are sufficient checks and balances to prevent the abuse of such provisions.

¹⁴⁰ Prevention of Terrorism Act. <http://www.kenyalaw.org/lex/actview.xql?actid=No.%2030%20of%202012>

5 Results: Status, Trends and Challenges

This chapter details the emerging trends and key challenges to privacy and personal data protection, citing various examples and incidents from various countries.

5.1 Limited Understanding of Privacy

The concept of privacy is not fully understood in the countries under review. Similarly, the level of public awareness about privacy and data protection is limited, with many citizens tending to be indifferent to privacy and data protection issues.

Further, there is no direct translation or equivalent term for the word “privacy” in many African languages. In Swahili, a widely spoken language in eastern Africa, the word with closest meaning is *siri* which means secret. In Chichewa, the major language in Malawi, the closest term is ‘chinsinsi’ which also means secret. Similarly, in Shona, a language spoken in Zimbabwe, the closest words are ‘chakavandika’ or ‘tsindidzo’ which though hardly used in normal conversations, mean secret. In Amharic, which is widely spoken in Ethiopia, the closest meaning to the term privacy is the phrase *Ye Gil Hiwote Ye'Mekeberna Yemetebeke Mebit'* which means 'the respect and protection of personal life.'

The lack of a direct translation for privacy presents a challenge to the understanding and promotion of privacy issues. African society values openness and shuns matters conducted in secret, save for where the situation demands. Hence, few people are keen to question the necessity, legitimacy or processes of collection and handling of personal data by government or business entities as, in their view, “they have nothing to hide”. As a result, governments have continued unhindered to introduce more data collection programs yet there is lack of safeguards for the protection of that data from abuse. These range from the facial recognition programme in Zimbabwe to mandatory SIM card registration in all countries studied.

Universally, governments claim the measures are necessary to fight crime, are entirely for the public good, and only criminals would have something to hide. In Burundi, the Ministerial Order Number 01 of 2014 was introduced to address the “urgent” need to ensure the security of the state and to fight crimes committed using mobile phones.¹⁴¹ Similarly, in Malawi mandatory SIM card registration was introduced to help fight electronic-based crimes such as fraud which the government said was on the rise.¹⁴²

Moreover, some internet users are not only unaware of the existence of, but also lack the capacity to use the privacy and data protection tools and controls that are available on social media platforms and other online services.¹⁴³ According to an Information Systems Audit and Control Association (ISACA) study, social media users prefer

¹⁴¹ *Circulaire relative à l'enregistrement des abonnés de la Téléphonie Mobile.* <http://www.arct.gov.bi/images/circulaires/circulaire2.pdf>

¹⁴² *Malawi government lifts suspension on SIM Card registration* <https://www.nyasatimes.com/malawi-govt-lift-suspension-sim-card-registration-dausi-tells-parliament/>

¹⁴³ *Lack of Privacy Awareness in Social Networks* <https://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Lack-of-Privacy-Awareness-in-Social-Networks.aspx>

convenience and do not have any reservations about providing personal information as part of their profiles. Also, they are not aware that when they naively and without precaution provide personally identifiable information (PII) for the benefit of their friends and circles, the same can be shared and accessed by third parties.

5.2 Weak Regulatory Frameworks

This section presents an analysis of the weaknesses of the existing policy and legal frameworks of the countries under review.

5.2.1 Absence of Comprehensive Data Protection Frameworks

The lack of a standalone policy or legislation on the right to privacy and data protection is a major weakness in most of the countries studied. The protection of the right was found to be fragmented and contained in various laws and policies. Some countries such as Kenya, Nigeria, and Uganda have data protection and privacy bills that have failed to progress through their parliaments for years. Kenya's first Data Protection Bill was developed in 2012.¹⁴⁴ To-date, it is yet to be adopted. Instead, the country abandoned the initial bill and in 2018 developed two new privacy bills, adding to uncertainty and delays in the law's enactment. Ethiopia's draft Data Protection Proclamation was first published in 2009 but is yet to be adopted. Nigeria, the country with the largest number of internet users in Africa, is yet to adopt the Data Protection Bill introduced in 2010.¹⁴⁵ Meanwhile, Nigeria's Digital Rights and Freedom Bill is currently awaiting transmission from the Senate to the president for assent, while the Data Protection Bill passed by the House of Representatives is now being considered by the Senate.

Uganda's Data Protection and Privacy Bill was first published in 2014 but it was only in February 2018 that parliament called for submissions from the public.¹⁴⁶ In Tanzania, the process of drafting the Personal Data Protection law started in 2009.¹⁴⁷ While the drafting process was said to be in the final stage in December 2017, following which it would be submitted for cabinet approval, this is yet to happen.¹⁴⁸ Burundi has similarly been working on a draft law on personal data protection since 2017, but it is yet to be discussed by cabinet.

Privacy groups have observed that many African governments have vested interests in not introducing data protection laws since they use citizens' data for their own ends such as for political campaigns, as in Kenya, or for suppressing political dissent.¹⁴⁹ In Zimbabwe, delays in passing the Computer Crime and Cyber Security bill, currently in its third draft since 2016, has despite promises, been attributed to the lack of political will.¹⁵⁰ In Zambia, efforts by civil society to engage on developing the Cybercrimes and Cybersecurity Bill 2017 were thwarted as the government continued to develop the legislation in a closed and non-participatory manner.¹⁵¹ In March 2018, Malawi announced plans to develop a Data Protection Act.¹⁵²

¹⁴⁴ Data Protection Bill, 2012. http://www.constitutionnet.org/sites/default/files/the_data_protection_bill_2012_revised_10th_jan2012.pdf

¹⁴⁵ In Africa, scant data protection leaves internet users exposed <https://reut.rs/2GBa6Bu>

¹⁴⁶ CIPESA Submits Comments On The Uganda Data Protection and Privacy Bill, 2015 <https://cipesa.org/2018/02/cipesa-submits-comments-on-the-uganda-data-protection-and-privacy-bill-2015/>

¹⁴⁷ Tanzania: Personal Data Protection Law On Horizon <https://allafrica.com/stories/201712210571.html>

¹⁴⁸ Ibid

¹⁴⁹ In Africa, scant data protection leaves internet users exposed <https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ>

¹⁵⁰ Techzim, President Mnangagwa Promises A New Cyber Security Bill, We've Heard This Before <https://www.techzim.co.zw/2018/09/presidentmnangagwa-promises-a-new-cyber-security-bill-weve-heard-this-before/>

¹⁵¹ Text of the bill, <https://bit.ly/2N4xzxs>

¹⁵² Dausi hints on Data protection act as Malawi moving towards digital economy <https://www.nyasatimes.com/dausi-said-hints-data-protection-act-malawi-moving-towards-digital-economy/>

5.2.2 Abuse of Laws to Undermine Privacy

There have been instances where law enforcement agencies have flouted existing legislation in ways that undermine privacy. In Tanzania, security agencies have on several instances demanded access to identifying details of individuals who have posted content online. Section 32 of the Cybercrimes Act, 2015 authorises the police to compel the disclosure of data for purposes of criminal investigations. This provision has been abused by police officers to infringe privacy rights. For instance, the popular online platform JamiiForums was in January and February 2016 issued with several letters compelling it to disclose the Internet Protocol (IP) addresses of its anonymous users or other information that would help the police to identify them.¹⁵³ When Jamii declined, its founders were arrested and charged with the offence of obstructing investigation.¹⁵⁴ The individuals whose information was sought had allegedly posted information on the forum about political tensions among members of the ruling party Chama Cha Mapinduzi, and scandals in one of the country's leading banks. In addition, Jamii's founders were charged with the equally controversial offence of management of a domain not registered in Tanzania under Section 79(c) of the Electronic and Postal Communications Act (2010).¹⁵⁵

Tanzania's Cybercrimes Act, which made three years old in September 2018, has been used extensively to rein in voices critical of president Magufuli's government, as well as voices critical of powerful business interests. More than 15 social media users have been arrested under the Act, with many charged in court just like the JamiiForums founders.¹⁵⁶

Meanwhile, there is an emerging trend in Tanzania, whereby law enforcement agencies seize phones and personal computers from individuals and hold them for several days on the pretext that they are conducting investigations. In April 2018, police briefly detained two popular musicians, Naseeb Abdul Juma (whose stage name is Diamond Platnumz) and Faustina Charles (popularly known as Nandy), after they each posted video clips on Instagram and WhatsApp respectively, which authorities deemed obscene.¹⁵⁷ They were released on bail without charge after questioning and two mobile phones were confiscated as part of the investigation. If charged, the two face fines of at least five million shillings (USD 2,200), a minimum prison sentence of 12 months, or both.

In November 2017, the leader of the opposition Alliance for Change and Transparency, Zitto Kabwe's phones were confiscated by police following his arrest and detention in October the same year. The politician was under investigation for uttering a seditious statement against the government, hence was held to be in violation of the Cybercrimes Act and Statistics Act.¹⁵⁸ In July 2018, the Home Affairs Minister had called for his arrest for incitement.

Earlier, during the October 2015 election period, police detained 40 volunteers of Tanzania's opposition party Chadema, and confiscated computers and phones they were using to tally election results.¹⁵⁹ The party termed the arrest a government bid to intimidate the opposition. Similarly, in October 2015, human rights defender Imelda Urio and 35 other members of the Tanzanian Civil Society Election Consortium (TACCEO) were arrested and detained over their election observation activities, which authorities said contravened section 16 of the Cybercrimes Act, which prohibits publication of false information.¹⁶⁰ The police confiscated the group's computers, office phones and mobile phones for nine months. No charges were preferred against the group.

¹⁵³ Tanzania Court Deals a Blow to Intermediary Liability Rules <https://www.opennetafrika.org/tanzania-court-deals-a-blow-to-intermediary-liability-rules/>

¹⁵⁴ BBC, Tanzania Police Charges Jamii Forums Founder, <https://www.bbc.com/news/world-africa-38341151>

¹⁵⁵ UPDATE: Maxence Melo Charged with Obstruction of Investigations and Operating a Domain Not Registered in Tanzania <https://bit.ly/2OP8wA1>

¹⁵⁶ Five Tanzanians charged with insulting the president <https://bit.ly/2xRJzg7>

¹⁵⁷ Popular Tanzanian singer arrested in latest internet crackdown <https://reut.rs/2xlEvkP>

¹⁵⁸ Police confiscate Zitto's mobile phone, raid ACT-Wazalendo offices <https://bit.ly/2Q6CRKI>

¹⁵⁹ Tanzanian opposition says 40 volunteers arrested after election <https://bit.ly/2NKI03n>

¹⁶⁰ Tanzania: Ongoing police harassment against Imelda Urio and 35 other human rights defenders <https://www.awid.org/get-involved/tanzania-ongoing-police-harassment-against-imelda-urio-and-35-other-human-rights>

Whereas Uganda's Computer Misuse, 2011 Section 28 requires police officers to produce a court warrant to enter, search and seize any computer system, this requirement is often flouted. In June 2018, MTN Uganda's data centre in Mutundwe, Kampala was raided by security personnel in what the media said was an operation to counter security surveillance on behalf of a foreign government.¹⁶¹ The raid appears to have been conducted without warrants or a court order as the company stated in a letter that it had reported to the police a case of trespass and illegal intrusion into the data centre and the disconnection of the four information servers by security personnel alleging to be officers of the Internal Security Organisation (ISO).¹⁶² Moses Keefah Musasizi, a manager data facilities at Huawei Uganda who was at the time responsible for the physical access to the MTN Data Centre, was detained for four hours at the ISO headquarters and thereafter forced to provide access to the servers, four of which were disconnected. As a result, key services of MTN Uganda, the largest mobile network operator with 11 million subscribers, such as processing of call data records, resolution of customer queries, and mobile money micro-lending, were affected.¹⁶³ A week later, the company stated that despite several attempts, security personnel who raided the data centre were unable to log into their servers owing to MTN's robust information security systems and thus no data was accessed or compromised.¹⁶⁴ Senior government officials declined to comment on the matter.

Prior to this raid, premises of Civil Society Organisations (CSOs) in Uganda had been targeted by unknown parties who reportedly took mostly computer disk drives and other electronic devices. Since 2012, there have been over 24 break-ins into premises of CSOs.¹⁶⁵ While the organisations fault the police for failing to investigate the incidences, the prevalence of the raids poses a threat to the privacy of information held by CSOs.

Similarly, in Zambia, the Computer Misuse and Crimes Act, 2004, Section 16 has been violated by officials from the communications regulator ZICTA and the police. The two agencies raided CEC Liquid Telecom's head office in Lusaka in April 2017, in search of suspected phone tapping equipment used to eavesdrop on conversations between senior government officials.¹⁶⁶ The raid followed the leakage of a phone recording of conversation where the Special Assistant to the President for Press and Public relations, Amos Chanda, was heard directing the Inspector General of Police to use maximum force when dealing with opposition political supporters.¹⁶⁷ CEC Liquid Telecom denied any involvement in phone tapping.¹⁶⁸ In June 2018, a ZICTA official indicated that the Authority was coming up with a new law that would require WhatsApp administrators to register their groups and set up codes of ethics or risk being arrested if there was a breach.¹⁶⁹ The statement was denied by the ZICTA Director General, saying the Authority had no such plans.

5.2.3 Legal Provisions Compelling Telecom Companies to Cooperate on Surveillance

All the countries under review have legal provisions require the cooperation and compliance of service providers to information requests or surveillance assistance. This cooperation includes the requirement to install technical surveillance capability, to actively enable communications monitoring, and to hand over data when asked.

Uganda's Regulation of Interception of Communications Act, 2010 grants government agencies power to conduct interception in real time with court warrants and includes a broad framework that requires telecom operators to install technical surveillance capability within their systems and to facilitate the interception of communication.¹⁷⁰ Section 3 of the Act provides for the establishment of a Monitoring Centre for the interception of communications.

¹⁶¹ MTN Uganda data centre raided over security <https://bit.ly/2ueGsgo>

¹⁶² Monitor Reporter, "Trespassers break into MTN data centre, disconnect four servers," July 6, 2018, <https://bit.ly/2NHRxTG>

¹⁶³ Security personnel raid MTN Uganda data centre, disconnect servers https://www.the-star.co.ke/news/2018/07/06/security-personnel-raid-mtn-uganda-data-centre-disconnect-servers_c1783205

¹⁶⁴ ISO Agents Failed to Penetrate Our Servers – MTN <https://chimpreports.com/iso-agents-failed-to-penetrate-our-servers-mtn/>

¹⁶⁵ Emmanuel Ainebyoona, "Police on the spot as break-ins into NGO offices remain uninvestigated," March 11, 2017, <http://www.monitor.co.ug/SpecialReports/Police-spot-break-ins-NGO-offices-remain-uninvestigated-ACCU/688342-3843648-11dydsi/index.html>

¹⁶⁶ Zambia police raid CEC Liquid Telecom <http://www.itwebafrica.com/business-continuity/771-zambia/237732-zambia-police-raid-cec-liquid-telecom>

¹⁶⁷ Kanganja Records and Deliberately Leaks Recording With Amos Chanda <https://www.zambianobserver.com/kanganja-records-and-deliberately-leaks-recording-with-amos-chanda/>

¹⁶⁸ Statement <https://www.facebook.com/Mwebantu/posts/cec-liquid-telecom-press-statement-on-raid-by-zicta-and-state-police-yesterday-w/1298897223563703/>

¹⁶⁹ ZICTA angers WhatsApp users over threats on group admins <https://www.themastonline.com/2018/06/01/zicta-angers-whatsapp-users-over-threats-on-group-admins/>

¹⁷⁰ The Regulation of Interception of Communications Act, 2010, <https://bit.ly/2pxoEv4>

Section 8 of the Act requires service providers to among others, technically assist government to intercept communications by ensuring systems are technically capable of supporting lawful interceptions at all times; installing hardware and software facilities and devices to enable interception; and ensuring their services can render real time and full time monitoring facilities for interceptions.

Under section 11, telecommunication service providers are required to provide telecommunication services which have the capability to be intercepted; and to store call-related information in accordance with directives issued by the ICT minister. Such a directive to telecommunication service providers is required to specify details such as the period within which the directive must be complied with; and, the security, technical and functional requirements of the facilities and devices to be acquired by every telecommunication service provider to enable the interception of communication and the storing of call-related information. A service provider who fails to give assistance commits an offence and shall be liable to a fine not exceeding 120 currency points (USD 628) or to imprisonment for a period not exceeding five years, or both. Further, the service provider's license may be cancelled.

Ethiopia's Proclamation 804 of 2013 Re-establishing National Intelligence and Security Service (NISS) requires all persons to cooperate with NISS by providing information. Similarly, Rwanda's interception law provides in Article 3, that the interception of communications shall be considered lawful where it is done in the interest of national security and in accordance with this law.

Article 7 of Rwanda's interception of communication provides that a communication service provider shall ensure that systems are technically capable of supporting interceptions at all times upon request by the competent organ.¹⁷¹ Similarly, Article 123 of the Law No. 24 of 2016 governing ICT requires that service provider "must equip the electronic communications network and service with technical instruments and features that allow and facilitate the lawful interception of electronic communications and monitoring. Further, in both instances, where a provider upgrades its electronic communications network or service, it must notify any authorised entity that carries out lawful interception of the upgrade.

Likewise, in Kenya under section 69 of the Security Laws (Amendment) Act (2014), which amends the Prevention of Terrorism Act, telecommunications operators may be required to allow the installation of a lawful interception capability.¹⁷² In the DRC, the 2014 Agence Nationale de Renseignement (ANR), the Intelligence Service Agency, requires operators to install lawful interception capability while article 11 of the Inter-ministerial Decree of 2015 obliges network operators to communicate to the relevant state authorities the identification elements of the subscribers contained in their databases, before any deletion, removal, or overwriting.

Similar requirements are contained in Tanzania Prevention of Terrorism Act and Tanzania Intelligence and Security Service Act. In 2016, Vodacom Tanzania indicated that it had not implemented the technical requirements necessary to enable lawful interception and therefore had not received any government demands for lawful interception assistance.¹⁷³

Requiring telecommunication service providers to install 'backdoor' access to their systems opens the door for unlimited mass surveillance. Further, the laws are sometimes vague on the type of cooperation, facilitation or technical capabilities or standards expected from service providers. Moreover, they do not factor in the cost of financial and technical resources required to implement interception capabilities prescribed. This imposes an unnecessary burden on service providers. Since these measures are of a permanent nature, they negate and render the privacy protections afforded to persons almost meaningless.

¹⁷¹ LAW N°60/2013 OF 22/08/2013 Regulating the Interception of Communications <https://bit.ly/2QWxOh5>

¹⁷² Text of the Act <https://bit.ly/1HeTwFa>

¹⁷³ Country-by-Country Disclosure of Law Enforcement Assistance Demands 2015-16, Vodafone <https://bit.ly/2xNkoLE>

5.2.4 Unreasonable Search and Seizure Provisions

Some of the countries studied have laws with unreasonable search and seizure provisions. These laws do not require oversight over information requests by a competent, impartial and independent judicial authority.

In Ethiopia, laws such as the Anti-Terrorism Proclamation, the Computer Crime law and the Telecom Fraud law, weaken the protection of privacy and personal data. The Proclamation 804 of 2013 Re-establishing National Intelligence and Security Service (NISS), is peculiar. While it requires NISS to obtain a court warrant for directly conducting surveillance and data interception, it does not require NISS to obtain court warrants when it seeks information from third-party data collectors. Ethiopia's Computer Crime Proclamation 985/2016 stipulates that the regulatory organ is not expected to obtain a court warrant "where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is about to be committed." Under article 25(3) and 25 (4) of the proclamation,¹⁷⁴ it can readily conduct interception and surveillance with permission of the Attorney General. However, the Attorney General is required to report to the court within 48 hours with reasons why the interception or surveillance was conducted without court warrant.¹⁷⁵

Article 46 of Ethiopia's corruption crimes proclamation introduced special rules of investigation which permit the interception of correspondence by telephone, telecommunications and electronic devices as well as by postal letters, where it is necessary for the investigation of corruption offences, with authorisation of the head of the appropriate organ.¹⁷⁶ Such orders do not require judicial warrant and the duration of such interception orders may not exceed four months. Meanwhile, Article 22 of Ethiopia's Anti-Terrorism Proclamation obliges institutions that collect personal data, such as banks, tax authorities and medical institutions, to disclose such information whenever it is needed for investigation of terrorism cases.¹⁷⁷ Moreover, it gives wide discretion to the police to make the disclosure happen, if they "reasonably" believe that such disclosure is essential in the investigation process, without any judicial oversight. Article 16 authorises the police to conduct "sudden search and seizures" only with the permission of the Director General of the Federal Police.

Burundi's Code of Penal Procedure was promulgated on May 11, 2018 (Law No 1/09) in response to what a government official termed as an environment where criminals were increasingly using ICT tools in committing crime. The code introduces "special methods of investigation" which include the interception of electronic communications. It gives security services authority to install hidden cameras in suspects' homes or cars, to check their digital devices, and to check their electronic messages. Also, it authorises security services to monitor electronic devices and communications remotely using hacking tools. In August 2016, members of a WhatsApp group were arrested at a meeting, giving credence to suspicions that their conversations were being monitored. In May 2016, public security minister issued a statement warning the public against using social media to spread trouble, and said security forces and the telecoms regulator were working together and were getting the capacity to track criminals.¹⁷⁸

The provisions of Rwanda's privacy and personal data regulatory framework on search, seizure, and surveillance measures in different laws do not provide for judicial oversight, which may lead to abuse. Article 9 of Rwanda's 2013 law regulating the interception of communications provides that "an interception warrant shall be issued by a National Prosecutor designated by the Minister in charge of Justice", who is a member of the Executive to whom National Prosecutors report to. Further, that in urgent public security interests, the National Prosecutor may, upon the request of the minister, issue a verbal interception warrant to be completed within 24 hours. If the period expires without a written warrant, the interception is presumed to be illegal. Different laws including the ICT Law and interception of communication law contain provisions that facilitate the interception and monitoring of communications by government, which actions are not subject to court approval.

¹⁷⁴ Computer Crime Proclamation 958/2016 <http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/103967/126636/F1922468791/ETH103967.pdf>

¹⁷⁵ Telecom Fraud Offense Proclamation, Federal Negarit Gazeta, Proclamation No. 761/2012, Article 14.

¹⁷⁶ Revised Anti-corruption Special Procedure and Rules of Evidence Proclamation, Federal Negarit Gazeta, Proclamation No. 434/2005 <http://www.aau.edu.et/?wpdmact=process&did=MTQ5LmhvdGxpbnms=>

¹⁷⁷ Anti-Terrorism Proclamation, Federal Negarit Gazeta, Proclamation No. 652/2009

¹⁷⁸ https://cipesa.org/?wpfb_dl=230

Article 180 of Rwanda’s law on ICT empowers an authorised officer from the regulatory authority RURA to enter any business place where electronic certification services are conducted; enter and inspect any computer system and any associated material suspected to have been in use; and use or authorise to use any such computer system to search any data contained in or available to such computer system. Similarly, its Article 33 empowers a judicial police officer to enter, inspect and seize a system or equipment in any place if there are ‘reasonable grounds’ to believe they are operated in contravention of the law.

5.3 Data Collection Programmes by Governments

5.3.1 Mandatory Data Collection

In all surveyed countries, several government agencies are collecting and processing data yet they lack harmonised legal framework for data protection. The common areas which by law require mandatory collection of personal information by government, and which are regulated by law, include registration of SIM cards, voters, births, marriages, deaths, driving licenses, national identity cards, passports, tax payers, health insurance, social security, and national census.

Under the circumstances, the lack of sufficient judicial or independent oversight puts the protection of privacy and personal data in danger, as there is no sure way of assessing compliance with legal requirements. Save for Ghana and Senegal, the rest of the countries under review lack a single dedicated institution responsible for regulating privacy and data collection. Malawi’s Electronic Transaction Act establishes the office of the Data Controller, but it has not been appointed.

Section 5 of Kenya’s Registration of Persons Act requires the capturing of registration number; name in full; sex; declared tribe or race; date of birth or apparent age, and place of birth; occupation, profession, trade or employment; place of residence and postal address, if any; finger and thumb impressions (or toe and palm impressions in case of missing fingers and thumbs); and date of registration. Further, section 9 requires that every identity card contain a photograph of the registered person. This data is stored in the Integrated Population Registration System (IPRS), and the recently announced National Integrated Identity Management System (NIIMS). Kenya’s election management body, the Independent electoral and Boundaries Commission (IEBC) has registered 19.6 million Kenyans through biometric voter registration for general elections held in March 2013 and August 2017.¹⁷⁹

On the other hand, all mobile network providers are required under rule 4 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015¹⁸⁰ to register all SIM cards issued with corresponding subscribers details like those required by the Registration of Person Act. Failure to provide the information as per SIM card regulations is an offence punishable by a fine of KES 300,000 (USD 3,000) or to imprisonment for a term not exceeding six months, or both. In September 2018, the Communications Authority of Kenya directed mobile operators to switch off all unregistered SIM cards on their networks.¹⁸¹ The directive followed a forensic audit by the Authority which showed that while all the operators had data access security policies in place, some of their agents did not request for identification documents or verify identities by subscribers upon registration, while others charged SIM cards buyers additional fees for registration. The Authority directed operators to ensure that agents verify identification documents with the Integrated Population Registration System (IPRS) at the time of registration.

¹⁷⁹ Capital FM, 19.6mn on voters’ roll for August polls as over 80,000 expunged,

<https://www.capitalfm.co.ke/news/2017/06/19-6mn-on-voters-roll-for-august-polls-as-over-80000-expunged/>

¹⁸⁰ Regulations, <https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf>

¹⁸¹ Press statement on findings of the forensic audit on registration of SIM cards,

<https://ca.go.ke/wp-content/uploads/2018/09/Press-Statement-on-Forensic-Audit-on-SIM-Card-Registration1.pdf>

In Burundi, the Ministerial Order N°215/224 requires that passport details are taken in biometric form since March 2011.¹⁸² The personal data collected includes fingerprints, national identity card, passport photograph, attestation of residence, work certificate (Attestation de service) and the person must be physically present. The Ministerial Order Number 01 of 2014 requires that before a mobile phone subscriber gets a SIM card, they must provide personal data such as names, address, birth date, passport photographs, copy of identity card or passport, and the serial number of their phone.¹⁸³ Additional details such as gender, names of parents, birthplace, employment and marital status, can also be found on identity cards. Moreover, a subscriber must be physically present during registration, and minors must be accompanied by their guardian.

Ethiopia's state-owned telecom company, Ethio-Telecom, has a mandatory SIM card registration system where users are obliged to register with their names, photo ID, signature, relatives' phone numbers, and addresses. Users are required to show an identification card and allow the telecom to keep a scanned copy of the ID. From September 2017, the government required the company to register all new mobile devices brought into the country to prevent illegal smuggling of new devices and unwarranted use of the network.¹⁸⁴ The Equipment Identity Registration System (EIRS) matches each mobile device with the SIM card of the user.¹⁸⁵

In Malawi, mandatory SIM card registration, which was rolled out in June 2017, is provided for under Article of 92(1) of the Electronic Transaction Act.¹⁸⁶ The exercise was temporarily suspended in February 2018 by the information minister, who cited the lack of civic education. However, the broader issue to the suspension was to address public concerns that the registration exercise was intended to enable the government to conduct surveillance of citizens' communications. The suspension was lifted after two weeks.¹⁸⁷

In Uganda, The Regulation of Interception of Communication Act, 2010 requires mandatory registration of SIM card holder by telecom service providers. The details include name, residential address, business postal address and identity number. The process which began in 2012, was reinforced by the 2015 Registration of Person Act, which establishes National Identification and Registration Authority (NIRA). NIRA has been carrying out a nation-wide issuance of national identity cards where 14.8 million citizens have been registered. Registration and issuance of a national ID requires applicant to provide names, copies of national IDs of both parents and birth certificate. Between May and August 2017, NIRA in collaboration with the education ministry commenced a national project to biometrically register all learners aged 5-16 years.¹⁸⁸ In addition to SIM card registration online data communication service providers including online news platforms and radio and television operators are required to apply and obtain authorisation for their online services.¹⁸⁹

Zambia's Information and Communications Technologies (Registration of Electronic Communication Apparatus) Regulations, 2011 in rule 11, requires all subscribers to register their SIM cards in an electronic register maintained by the service provider.¹⁹⁰ The details collected include names and addresses of the subscribers, serial numbers of the SIM cards, and the mobile subscriber integrated service digital network (MSISDN) numbers. Identification

¹⁸² See the Ministerial order here: http://www.securitepublique.gov.bi/IMG/pdf/tarif_du_passeport_biometrique.pdf

¹⁸³ <http://www.arct.gov.bi/images/circulaires/circulaire2.pdf>

¹⁸⁴ Aptantech, Ethiopia government in mobile phone registration drive to curb smuggling, fraud, <http://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/>

¹⁸⁵ Aptantech, Ethiopia government in mobile phone registration drive to curb smuggling, fraud, <https://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/>,

¹⁸⁶ Malawi Start Mandatory SIM Card Registration, <https://bit.ly/2xQO9LP>

¹⁸⁷ Malawi Government Lifts Suspension on SIM Card Registration, <https://www.nyasatimes.com/malawi-govt-lift-suspension-sim-card-registration-dausi-tells-parliament/>

¹⁸⁸ NIRA, Mass registration of pupils handbook, <https://www.nira.go.ug/wp-content/uploads/Publish/Handbook.pdf>

¹⁸⁹ Registration Of Online Data Communication And Broadcast Service Providers, http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf; See also, Daniel Mwesiwa, "Uganda Moves to Register Online Content Providers," CIPESA, March 25, 2018, <https://cipesa.org/2018/03/uganda-moves-to-register-online-content-providers/>

¹⁹⁰ Regulations, <https://bit.ly/2xGcynR>

documents are required at the time of registration. The regulation requires the Zambia Information and Communication Technology Authority (ZICTA) to establish a Central Equipment Identification Register under rule 16, and an Information and Deactivation Centre under rule 17, while service providers are required under rule 18 to keep equipment identification registers, all which aids in the management of information on subscriber and their devices. On several occasions, ZICTA has issued ultimatums for the public to register their cards or update their information, with failure to comply resulting in permanent disconnection.¹⁹¹ By April 2016, the country's three operators had temporarily blocked one million SIM cards for not being properly registered.

Similarly, Zimbabwe's Postal and Telecommunications (subscriber registration) Regulations of 2013 mandate collection of specified data from all persons as a precondition for registration with and receipt of services from telecommunication service providers.¹⁹² The data to be collected includes names, addresses, gender and national identification numbers. The law requires telecom operators to regularly provide copies of this data to the Central Subscriber Information Database. Penalties for non-compliance include possible revocation of the service provider's operating license. It has been suggested that the consolidated database was inappropriately accessed and used by the ruling party ZANU PF,¹⁹³ and doubts linger about the independence and integrity of the telecoms regulator POTRAZ.¹⁹⁴ This regulation also requires POTRAZ to appoint data controllers to take responsibility of subscriber data collected and stored in the Central Subscriber Information Database. The SIM card registration exercise in the country was criticised for undermining the ability of users to communicate anonymously, and because it could facilitate surveillance and make tracking and monitoring of users easier for authorities.¹⁹⁵

In the DRC, the Inter-ministerial Decree of June 2015 provides for the registration of telephone subscribers.¹⁹⁶ The decree states that collection of subscribers' data is solely for security, financial and legal reasons. In Article 3, it provides a list of subscribers' information to be collected prior to registration, which is like that required in other countries in the region. Further, Article 7 of the decree prohibits the disclosure of subscribers' information except where the user's consent has been obtained, or where the information is required by a competent government department.

In October 2015, the Nigerian Communications Commission (NCC) slapped MTN Nigeria with a fine of USD 5.2 billion for failing to disconnect 5.2 million of its subscribers who had unregistered SIM cards.¹⁹⁷ The regulator termed MTN Nigeria's actions a "grave security risk", noting that the company had failed to act despite receiving several warnings on the matter.¹⁹⁸ The fine was reportedly reduced to N330 billion (USD 1.7 billion) after negotiations with the government.¹⁹⁹

In Nigeria, section 14 of the National Identity Management Commission (NIMC) Act provides for the establishment of a National Identity Database which contains data on citizens and non-Nigerian citizens. Part of the objective of the database is to provide a medium for the identification, verification and authentication of citizens of Nigeria and other registrable persons entitled to the Multi-purpose Identity Cards. Section 17 of the law and its second schedule provides for the types of information that can be collected, but do indicate types of information that cannot be collected.

¹⁹¹ Register your SIM card or face permanent disconnection – ZICTA <https://bit.ly/2O65c6L>

¹⁹² Section 4(1)

¹⁹³ Access to the consolidated database was to be availed for purposes of law enforcement, upon the written request of a law enforcement agent, or for "safeguarding national security", as well as for "undertaking approved educational and research purposes."

¹⁹⁴ In the 2013 election year, POTRAZ was placed under the Office of the President and Cabinet and operated under the same for several years.

¹⁹⁵ "The right to privacy in Zimbabwe, the Digital Society of Zimbabwe, Zimbabwe Human Rights NGO Forum and the International Human Rights Clinic at Harvard Law School, and Privacy International in their "Stakeholder Report Universal Periodic Review 26th Session – Zimbabwe, March 2016

¹⁹⁶ Text of the decree, <https://www.leganet.cd/Legislation/JO/2015/Numeros/JO%2001%2006%202015.pdf>

¹⁹⁷ Reuters, MTN fined \$5.2 bln in Nigeria over phone registrations, <https://bit.ly/2OdtPOS>

¹⁹⁸ Nigeria suspends \$5 bln fine for MTN over SIM cards until talks end, <https://bit.ly/2xSIFaE>

¹⁹⁹ News 24, Nigeria hits MTN with new, \$2bn tax bill, <https://bit.ly/2leX6D9>

In 2014, Tanzania expanded its nationwide program of issuing National Identity Cards to its citizens and residents through a biometric system. In 2015, the country introduced a Biometric Voter Registration System with a private Dutch company, GenKey, working as a subcontractor for South Africa-based Lithotech Exports, contracted to implement the system through which 24 million eligible voters were registered.²⁰⁰ The Tanzania Revenue Authority also collects biometric data prior to the issuance of driving licenses. The country has no law in place to provide safeguards against possible violations even as personal data continues to be collected en masse.

In March 2018, Tanzania's communications regulator TRCA, in collaboration with the National Identification Authority, commenced a 30-day pilot project for biometric registration of customers of all telecommunication service providers.²⁰¹ According to TCRA, the provision of fingerprints would be establishing proof of identity, seal existing loopholes, and prevent criminal activities such as fraud, verbal abuse and threats, and collect correct subscription statistics from the telecom sector. Operators Tigo and Zantel hailed the initiative as necessary to discourage misuse of mobile phones, abusive language, fraud, and said it would reduce customer complaints.

Ghana's Subscriber Identity Module Registration Regulations, 2011²⁰² requires service providers to register subscribers before SIM cards can be activated. Subscribers are required to furnish service providers with name; residential or occupational address; date of birth (for individuals), date of incorporation (for corporate entities, date of registration (for partnerships); and an identity document. According to the National Identification Register (Amendment) Act, 2017,²⁰³ Act 950, in registering for Ghana Card, an individual is expected to provide full name; sex; date of birth; place and country of birth; nationality; residential address; postal address; marital status and where applicable, name of spouse; level of education; employment status; electronic mail address; telephone number; Tax Identification Number; social security number and a number of other personal information.

5.3.2 Scaling up Digitisation Programmes

The integration of ICT, including internet powered applications and services in government functions and operations can revolutionise in the delivery of services while at the same time promoting business and growth.²⁰⁴ Such e-government programmes geared at shifting from old paper systems to electronic processes can enhance efficiency and effectiveness of public services; strengthen trust and combat corruption; enhance transparency and accountability; promote financial inclusion; and promote innovation, education and job creation.²⁰⁵ Accordingly, a number of governments in the countries studied are introducing digitalization programmes that require citizens to provide detailed personal information, including biometrics.

In 2015, Rwanda rolled out the Irembo e-platform, a one-stop shop for government services and applications. The online portal offers access to personal information in databases relating to at least 80 different services, including the registration for birth certificates and driving licences; land registration and transfers; payment for fees and permits; NGO registration; and visa, national ID and passport applications.²⁰⁶ The portal is managed by RwandaOnline Platform Limited, who have entered a 25-year Public Private Partnership with the government to digitise all Government-to-Citizen and Government-to Business services, with 100 services coming online in three years from 2017.²⁰⁷

²⁰⁰ THRC, *Report on the Right to Privacy in Tanzania*, 2015. pg 8.

²⁰¹ The Citizen, *Why TCRA opted for biometric plan*, <https://bit.ly/2zsmVND>

²⁰² <https://www.nca.org.gh/assets/Uploads/Subscriber-Identity-Module-Registration-Regulations-2011-L.I.-2006-24th-Nov-2011.pdf>

²⁰³ https://www.nia.gov.gh/act_950.pdf

²⁰⁴ Africa urged to expand digital connectivity for growth, <https://bit.ly/2NChcx3>

²⁰⁵ PWC, *Disrupting Africa: Riding the wave of digital revolution*, <https://bit.ly/2lg296g>

²⁰⁶ , <https://irembo.gov.rw/rolportal/web/rol>

²⁰⁷ RwandaOnline Platform Ltd https://www.jobinrwanda.com/employer/rwandaonline_platform_ltd

Rwanda is also implementing ICT initiatives in the health sector through the Open Medical Record System (OpenMRS), which facilitates nationwide tracking of patients' data, providing support for nutrition and child health, and database synchronisation tools. Another e-health system is the Treatment and Research AIDS Centre (TRAC), which collects, stores, retrieves, displays and disseminates critical information about drug distribution and HIV/AIDS patient information to facilitate anti-retroviral treatment.²⁰⁸

Rwanda's e-government portal contains a privacy policy on the website which details the nature of information collected and the purposes for which it is applied.²⁰⁹ It notes that personal information provided willingly may be shared with Government Institutions, Ministries and Agencies in the performance of their official duties or providing the services requested for. The policy notes that services on the platform are not intended to be used anonymously. However, it guarantees the security of the information collected and adds that the website does not capture data that allows a user to be identified individually.

Kenya also runs an e-platform for government services similar to Irembo, known as eCitizen, which was rolled out in July 2014.²¹⁰ The platform offers access to personal information in databases relating to at least 33 different services, including passport application, visa applications, land searches, business registration, driving license renewal, marriage applications, and various tax services. The management of the World Bank funded project has come under intense scrutiny as it is not clear who between the Ministry of ICT, the ICT Authority, National Treasury and Office of the President has overall responsibility for the portal.

However, a recent court dispute between the National Treasury and three companies, Webmasters Africa, Webmasters Kenya and Goldrock Capital over the sharing of funds collected from the platform is telling.²¹¹ Currently, users pay a convenience fee of KES 50 (USD 0.5) per transaction on the platform, which between November 2014 and April 2016 totalled to KES 5.6 billion (USD 56 million) through its Safaricom mPesa Paybill account.²¹² The other e-government service platform available online is iTax portal managed by the Kenya Revenue Authority;²¹³ the Independent Electoral and Boundaries Commission Register, which contains biometric records of 19.6 million Kenyans;²¹⁴ the Integrated Population Registration System (IPRS); and the recently announced National Integrated Identity Management System (NIIMS).

This Integrated Population Registration System (IPRS) is a single national database that consolidates personal information including biometrics, stored in registries such as births and deaths, marriages and divorce, as well as those relating to passports, alien IDs, ID cards and citizenship for ease of verification by government and private bodies.²¹⁵ The development of the system was informed by heightened public concern around national security in the wake of the 2013 terror attacks, and was thus expected to be a "single source of truth" relating to citizenship and immigration. The previous system was fragmented and largely paper-based, which made it difficult to verify and authenticate information in official documentation, detect or prevent fraud, impersonation or other criminal activity.²¹⁶ The IPRS was launched in March 2015, and as of October 2016, the database had captured biometric details of 35 million Kenyans and foreigners.²¹⁷

²⁰⁸ Big dreams for Rwanda's ICT sector <https://www.un.org/africarenewal/magazine/april-2014/big-dreams-rwanda%E2%80%99s-ict-sector>

²⁰⁹ Privacy Statement <https://irembo.gov.rw/rolportal/web/rol/privacystatement>

²¹⁰ eCitizen www.ecitizen.go.ke

²¹¹ Battle for control of Sh5.6bn eCitizen takes new twist, <https://bit.ly/2Q5P5mO>

²¹² Company sues Treasury over eCitizen payments <https://bit.ly/2ND9anI>

²¹³ iTax Portal <https://itax.kra.go.ke/>

²¹⁴ IEBC Register <https://www.iebc.or.ke/iebcreports/index.php/2017-register/>

²¹⁵ Personal data system launched, Nation <https://bit.ly/2O80rcP>

²¹⁶ Business Daily Africa, Integrated data system to make e-government a reality, <https://bit.ly/2O7LNSF>

²¹⁷ The Star, Banks reap big from digital population register, <https://bit.ly/2lcUN3D>

In August 2018, the Kenya government announced plans to implement the NIIMS from September 2018. The system has been proposed to be established under a new section 9A of the Registration of Persons Act, through an amendment contained in the Statute Law Miscellaneous Amendment Bill, 2018, which is yet to be passed.²¹⁸ Under the system, the state seeks to establish a single national population register of personal information of all citizens and registered foreigners residing in Kenya and assign them a unique identification number. In addition, the system will consolidate information from other government databases relating to the registration of persons; centrally produce official registration documents; verify and authenticate registration information; and, ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register.

Kenya's eCitizen also contains a simple Terms of Use, which contains a privacy statement.²¹⁹ The statement provides that no personally identifiable information is automatically collected users of the site, nor does eCitizen release any information about IP addresses to any third party, except under court order or as required by law. The statement also provides for data security, and states that it may share information provided to other government agencies if necessary for the service required or court order. The site also doesn't share information with third parties for marketing purposes, and only does so where it necessary to complete transactions or services on the platform.

Uganda's e-government platform, also known as eCitizen, offers access to personal information in databases relating to 74 transactional services, ranging from eTax, Business registration, trading license registration and social security statements, among others.²²⁰ The portal is managed by the National Information Technology Authority – Uganda (NITA-U), a statutory body established under the NITA-U Act 2009 to coordinate and regulate Information Technology services in Uganda. Uganda's eCitizen portal does not contain a privacy statement or policy on the website.

These efforts to transform public services through digitisation and the offer of e-services have resulted in consolidation of existing government databases and the collection of new data from citizens, including biometric data. The programmes are largely being implemented by third parties or through public-private partnerships, meaning personal records of citizens are being handled by third party contractors outside government. There has been no assessment of the risk to privacy and personal data currently being handled by such contractors. Worryingly, such programmes are continuously being scaled up in the absence of comprehensive policies, legal and institutional frameworks for privacy and data protection.

As countries increase their digitisation programmes, vast amounts of data of become available to the government in digital formats. National e-government programmes such as eCitizen in Kenya and Rwanda's Irembo require registration with mobile numbers for verification of accounts.

In addition, the mandatory SIM card registration rules across the different countries require the authentication of the identities of registered persons with official documents and from online national government population databases. In Kenya, government institutions and private sector actors such as banks and telecommunication service providers are required to authenticate official documents from the IPRS database through an Application Programming Interface (API) - such as at the time of opening bank accounts or registering SIM cards.²²¹

²¹⁸ Text of bill, <https://bit.ly/2Q6zsM8>

²¹⁹ Terms of Use, <http://www.ecitizen.go.ke/terms-of-use.html>

²²⁰ eCitizen, www.ecitizen.go.ug

²²¹ Kenya Govt Pushes For Banks, Telcos to Authenticate Customer Data With Central IPRS Database <https://techweez.com/2015/06/22/telcos-to-use-iprs/>

In Uganda, NIRA in April 2018 offered biometric card readers to telecom operators to facilitate real time verification of the National Identity cards.²²² In order to verify their identities, holders of national ID cards will have the cards read by the machine and a thumbprint taken. Telecoms were expected to have installed their own machines through countrywide service centres within 30 days from April 2018. According to NIRA, the real time connectivity between UCC, telecoms and NIRA is facilitated by an API that validates SIM cards using National IDs.

The danger with the linked online databases is the ease with which it presents authorities with complete profiles of citizens. In the absence of comprehensive policy, legal and institutional frameworks for data protection in Kenya and Uganda, such data is at high risk of abuse.

5.4 Enhanced State Surveillance Capacity

5.4.1 Permitted Interception and Surveillance

Laws in the countries under study stipulate the procedures for conducting surveillance and making information requests to intermediaries such as telecom companies. These laws apply generally to communication and information within the countries and are not limited to the nationality of the individual whose information is sought. In Kenya, section 42 of the National Intelligence Service (NIS) Act specifies the procedures.²²³ In Burundi, the procedure is provided under the Ministerial Law No 540/356 of March 17, 2016 and in Article 92 of the Law No. 1/10 of 3 April 2013 on the reform of the Code of Criminal Procedure. Ethiopia's Computer Crimes Proclamation, under Article 25(1), authorises the regulatory organ to intercept in real time or conduct surveillance on computer data, internet and other communications of persons suspected of computer crimes upon obtaining a court warrant.²²⁴

Section 31 of Tanzania's Prevention of Terrorism Act provides that "a police officer may for the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order."²²⁵ Section 14 of the Tanzania Intelligence and Security Services Act, 1996²²⁶ empowers the Tanzania Intelligence & Security Service (TISS) to collect, analyse and retain information and intelligence regarding activities that may on reasonable grounds be suspected of constituting a threat to the security of the country.²²⁷

However, section 5(2) of this law bars TISS from instituting surveillance of any person or category of persons by reason only of their involvement in lawful protest, or dissent in respect of any matter affecting the constitution, the laws or the Government of Tanzania."²²⁸ Similarly, Section 120 of Tanzania's Electronic and Postal Communication Act, 2010 prohibits the interception of any communication, disclosure of content of communication, or use of the content of intercepted communications without lawful authority.²²⁹ It provides a penalty of five million Tanzanian shillings (USD 2,191) or to imprisonment for a term not less than 12 months, or both.

Further, regulation 5(1) (e) of the Electronic and Postal Communications (Online Contents) Regulations, 2018 requires content providers to have mechanisms in place to identify the source of their information or content. This may jeopardise the privacy of the persons who wish to contribute or share content anonymously. Regulation 11(1) provides that personal information obtained by the communications regulatory authority in exercise of its powers or duties under the regulations can only be disclosed if required by any law enforcement agency, court of law or other lawfully constituted tribunal. The regulations do not provide the procedure for making such requests.

²²² Biometric Card readers handed over to Uganda Communications Commission <https://www.nira.go.ug/index.php/2018/04/14/biometric-card-readers-handed-over-to-uganda-communications-commission/>

²²³ Section 42 National Intelligence Service Act

²²⁴ Computer Crime Proclamation, Proclamation No.958/2016, <https://bit.ly/2QXdCvF>

²²⁵ Prevention of Terrorism Act, <https://bit.ly/2Dsgdul>

²²⁶ Tanzania Intelligence & Security Service Act, <https://bit.ly/2NDlbtN>

²²⁷ Tanzania Intelligence & Security Services Act, http://www.vertic.org/media/National%20Legislation/Tanzania/TZ_Intelligence_Security_Services_Act.pdf

²²⁸ See section 5(2) of the Tanzania Intelligence and Security Services Act, 1996.

²²⁹ Text of the Act, https://www.researchchictafrica.net/countries/tanzania/Electronic_and_Postal_Communications_Act_no_3_2010.pdf

Rwanda's law No. 60/2013 on interception of communication authorises relevant security organs to apply for an interception warrants.²³⁰ Further, Under Article 126 of Rwanda's Law No. 24 of 2016 governing ICT, the minister is empowered to interrupt or cause to be interrupted, any private communication that appears detrimental to the national sovereignty, contrary to any existing law, public order or good morals; or suspend wholly or in part any electronic communications service or network operations for a specified or undetermined period. Further, under Article 127, electronic communication service providers are under an obligation to provide to the Minister and the Regulatory Authority any information sought for the guidance and supervision of activity relating to ICT. Similar provisions are contained in the Framework Law number 013/2002 of October 16th, 2002 on Telecommunications in the DRC which authorises the Attorney General to prescribe the "interception, registration and transcription of correspondence made by telecommunication."

Ghana's Anti-Terrorism Act, 2008 allows a senior police officer (not below the rank of an Assistant Commissioner of Police) with the written consent of the Attorney-General (AG) and the Minister of Justice to apply to a court for an order to require the interception of communications for the purpose of obtaining evidence of commission of an offence under the Act. Further, under section 100 of the Electronic Communications Act, the President can make written requests and issue orders to operators or providers of electronic communications networks or services requiring them to intercept communications, provide any user information or otherwise in aid of law enforcement or national security.

In Uganda, the Regulation of Interception of Communications Act, 2010 is solely for lawful interception and monitoring of communications during their transmission whether through telecommunication media or postal services or any other service.²³¹ Section 2 of the Act bars unlawful interception of communication by any person save where there is consent or an authorised warrant. Despite the protection guaranteed in section 2, section 3 established a monitoring centre for the interception of communications which is placed under the Ministers responsibility. Further, the Act lists several individuals who are authorised to apply for a warrant of interception to a judge as including the: Chief of Defence Forces or his or her nominee; Director General of the External Security Organisation or his or her nominee; Director General of the Internal Security Organisation or his or her nominee; and the Inspector General of Police or his or her nominee. Further, section 5 -12 provide for grounds for which interception may be authorised by a judge as including; gathering information that threatens life or loss of life, trafficking in drugs and humans, actual threat to national security, public safety or to any national economic interest and threat to the national interest involving the State's international relations or obligations. These provisions are problematic as they threaten the confidentiality of personal communications between persons in the respective countries. Hence, the use of encryption technology or practicing anonymity can be difficult under the circumstances.

²³⁰ Law n°60/2013 of 22/08/2013 regulating the interception of communications, Article 3, Official Gazette n° 41 of 14/10/2013, <https://bit.ly/2QWxOh5>

²³¹ Regulation of Interception of Communications Act, 2010. Long title.

5.4.2 State Acquisition and Deployment of Surveillance Technologies

Technology advancement and increased digitisation have reduced the logistical barriers to accessing information and grown to an unprecedented scale the means through which personal data can be acquired, stored, or processed. The study has found that different technologies have been acquired by states, handing them the capacity to enhance their surveillance capabilities.

The Ethiopian Government has been reported as having a significant capacity to use intrusive technologies to conduct surveillance activity compared to other countries in the study. In 2013, government targeted opposition members through malware attacks.²³² In 2015, the Ethiopian was accused of using an intrusive spyware, Remote Control System (RCS), to steal files and passwords, intercept Skype calls and instant messages of the Ethiopian Satellite Television (ESAT), a critical media based abroad.²³³ The government has also been accused of infringement of privacy using FinSpy spyware technology in 2015²³⁴ and in 2014 to intrude into electronic communications of an Ethiopian political refugee in UK.²³⁵

Ethio-Telecom previously used the EIRS, which enabled it to automatically register every device that used a SIM card.²³⁶ Although the company announced in August 2018 that it had stopped device registration,²³⁷ concern remains over the management of data collected and in its possession. The company still utilises ZSmart, a technology installed by the Chinese company ZTE which, enables law enforcement to access phone call records; personal information of the subscriber; phone call information including the originating and receiving phone numbers, the location of originator or receiver, the time, date and duration of every call; and the content of SMS; and audio of phone calls from any selected number.²³⁸

In 2017, Kenya's Communications Authority announced plans to install a device management system (DMS) to access information on the IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), Mobile Station International Subscriber Directory Number (MSISDN) and Call Detail Records (CDRs) of mobile network subscribers. According to the Authority, the system was to be used to identify and ban counterfeit, stolen or illegal mobile devices from being used on local networks.²³⁹ Safaricom, Kenya's leading mobile operator, opposed the system stating it could affect the sector given the threat of surveillance.²⁴⁰ The matter was taken to court in *Okiya Omtatah Okioti v Communication Authority of Kenya & 8 others* [2018] eKLR²⁴¹ where the court declared that the Authority had no mandate in combating counterfeit goods, that the programme was unconstitutional, null and void to the extent that it was arrived at unilaterally, without adequate public participation, and that it threatened the right to privacy of subscribers and presented a gross violation of their constitutionally and statutory protected consumer rights.

²³² Citizen Lab, 'You Only Click Twice: FinFisher's Global Proliferation', <https://bit.ly/2IkYpRc>.

²³³ Citizen Lab, 'Hacking Team and the Targeting of Ethiopian Journalists', February 12, 2014, <https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/>; Citizen Lab, 'Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware', March 9, 2015, <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/>

²³⁴ Electronic Frontier Foundation, *Kidane v. Ethiopia*, <https://www EFF.org/cases/kidane-v-ethiopia>

²³⁵ Privacy International Seeking Investigation into Computer Spying on Refugee in UK, Press Release, 17 February 2014, <https://ecadforum.com/2014/02/19/ethiopian-refugee-illegally-spied-on-using-british-software/>

²³⁶ Aptantech, Ethiopia government in mobile phone registration drive to curb smuggling, fraud, September 26, 2017, <https://bit.ly/2OeC1OR>.

²³⁷ Ethiopia Abandons Mobile Apparatus Registration, Cut Service Rate, <https://bit.ly/2xloa9S>.

²³⁸ Human Rights Watch Report, "They Know Everything We Do"; Telecom and Internet Surveillance in Ethiopia, <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>

²³⁹ CA sparks storm with plan to spy on users of mobile telephones, <https://bit.ly/2DzaCmA>.

²⁴⁰ Safaricom affirms opposition to CA's calls snooping device, <https://bit.ly/2OS7vaF>.

²⁴¹ *Okiya Omtatah Okioti v Communication Authority of Kenya & 8 others* [2018] eKLR, <https://bit.ly/2xNkL8U>

In Malawi, MACRA procured the Consolidated ICT Regulatory Management System (CIRMS) in 2011 to enable the regulator monitor service providers for quality of service and fair pricing.²⁴² The implementation of the CIRMS, locally known as “Spy Machine”, faced a challenge in court from telecom operators and Civil Society Organisations (CSOs), who feared that it would be used by state organs to eavesdrop on private communications, compromise the telcos’ obligations of ensuring privacy of subscribers, and violate article 21 of Malawi’s constitution.²⁴³ In October 2011, the High Court ruled in favour of the applicants, but on appeal the decision was overturned in favour of MACRA in September 2014. In April 2015, an application for review of MACRA’s decision to start using the machine was made at the High Court by Telekom Networks Malawi Limited (TNM), arguing that there was no framework to protect customer confidentiality and that it should not therefore implement the machine. In June 2017, the Supreme Court of Appeal ruled in favour of MACRA with a proviso that the system should not be connected to access content.²⁴³ Following the decision, MACRA installed the system which has been operational since September 2017.²⁴⁵

In July 2018, the Uganda Communications Commission (UCC) installed an Intelligent Network Monitoring System (INMS) with capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification.²⁴⁶ The system is hosted on communications infrastructure owned by mobile network operators, and the UCC will be able to monitor multi-vendor data, network performance, and customer experience records, among others.²⁴⁷ The president had long accused telcos of tax evasion and under-reporting revenues to the government.²⁴⁸ In January 2018, it was revealed that the UCC had set up a Centralized Equipment Identity Register system in a bid to identify, and stamp out fake and illegal mobile devices said to be hazardous to health and used to commit crime.²⁴⁹

In April 2017, ZICTA Zambia’s regulatory body claimed that it had the capacity to disable any communication devices and read personal messages.²⁵⁰ Further, that it was able to blacklist subscribers and also recover deleted content from mobile phones.

The full capabilities of these systems are not known. Despite some purported good intentions such as to mitigate tax evasion or stem fraud, their continued acquisition by governments and deployment in the absence of legal safeguards of their use is problematic, and threatens the full realisation of the right to privacy..

5.4.3 Increased Information Requests from Governments

Laws in various focus countries require relevant government departments to make lawful requests for telecom users’ information typically through applications to courts of law to obtain orders for the disclosure of the information. However, in all countries reviewed, these requests are kept secret. Hence it is difficult to establish the full extent of government requests for users’ data, the surveillance of citizens’ communications, and censorship of content. What is clear though, is that the trend is on the increase, and the types of users’ information which governments request is varied. One of the key developments has been the practice of transparency reporting by intermediaries such as telecom companies and online platforms. While the practice has not been adopted by most intermediaries, it has become vital to understanding government practices regarding requests for information, for interception assistance, and for content removal. It has also highlighted the commitment of some service providers to protecting the privacy of their users and promoting freedom of expression online.²⁵¹

²⁴² ‘Spy machine’ roll out in September, says Malawi regulator, <https://bit.ly/2R1toWo>.

²⁴³ “Spy Machine” Brings Telecoms Fears, <https://bit.ly/2NKBfzW>.

²⁴⁴ Court Nods to Macra’s “Spy Machine”, <http://mw.nation.com/court-nods-to-macras-spy-machine/>

²⁴⁵ Macra Unleashes Spy Machine, <http://zodiakmalawi.com/top-stories/macra-unleashes-spy-machine>

²⁴⁶ ITWeb Africa, Uganda’s UCC, telcos clash over network monitoring technology, <https://bit.ly/2NEMVON>.

²⁴⁷ Government installs system to track telecoms revenues, <https://bit.ly/2OQ7DXU>

²⁴⁸ All Africa, Uganda: Fight Over Shs44 Trillion Mobile Money, <https://allafrica.com/stories/201802260042.html>

²⁴⁹ Unwanted Witness, Uganda Communication Commission sets up mobile phone monitoring system, <https://unwantedwitness.or.ug/uganda-communication-commission-sets-up-mobile-phone-monitoring-system/>

²⁵⁰ ZICTA claims they can read your WhatsApp Messages and Disable any Communication Device, <https://www.lusakatimes.com/2017/04/20/zicta-claims-can-read-whatsapp-messages-disable-communication-device/>

²⁵¹ CIPESA, The Growing Trend of African Governments’ Requests for User Information and Content Removal From Internet and Telecom Companies, Policy Brief July 2017, https://cipesa.org/?wpfb_dl=248

Global intermediaries such as Facebook, Yahoo, Google and Twitter have been leaders in transparency reporting, in some instances increasing the amount of information they reveal about requests received from government and how they were received. Similarly, global actors such as Vodafone, Orange, and Millicom, have taken front row seats in transparency reporting on all their operations, including in Africa. Disappointingly, some laws in African countries bar the telecom intermediaries from publishing information on government requests, which has tied the hands of such operators. It means that in other regions where they operate (such as Europe, the Americas), they reveal details of what information they give governments annually about their customers, but maintain a blackout regarding requests in Africa. Equally, and perhaps more, worryingly, the operators with operations in the largest number of African countries, such as Bharti Airtel, MTN Group, Econet Wireless, Africell, and Etisalat fall in the opaque category that do not reveal any information at all about government requests received and how they are handled.

As of December 2017, Facebook had an estimated 177 million users across Africa.²⁵² Facebook's Transparency report includes information about requests related to its various products and services including Facebook, Instagram, Messenger, Oculus and WhatsApp.²⁵³ According to the report, government requests globally for data is on the rise, as the company received a total of 82,341 information requests between July to December 2017, compared to 64,279 during a similar period in 2016. For Google, government requests globally for user account details stood at 87,263 while user data disclosure requests stood at 48,877 between July and December 2017.²⁵⁴ This was an increase from 74,074 user account details requests and 45,550 user data disclosure requests recorded in the same period in 2016. Among African countries, Morocco and Sudan ranked highest having made 22 and 11 requests respectively for data from Facebook.²⁵⁵ Among the focus countries, Kenya and Nigeria made the most requests to Facebook at eight and seven respectively. During the period, only Kenya made an information request from Google, while Nigeria made two requests to Twitter.

Requests for user data from telecommunications service providers were much higher than those made to internet intermediaries. This is likely because the telecom intermediaries are locally licensed and are answerable to communications regulators who can sanction them including by withdrawing their licences. But telecom operators also say that they receive from African governments various requests which they are not able to carry out, such as those requesting for content that the telcos do not hold, for example from social media services such as WhatsApp and Facebook. According to the Orange transparency Report for 2016, Cameroon had 25,047 information requests from government, followed by Senegal at 18,653, Mali at 10,315, Cote d'Ivoire at 4,320, Guinea at 987, Madagascar at 888, and Botswana at 401.²⁵⁶

Last year, Millicom which operates in Chad, Rwanda and Tanzania, saw an increase in metadata requests from government agencies, and cited unnamed "security efforts" in one of the countries for driving up the numbers. There were no interception requests (relative to five in 2016), mobile financial services (MFS) requests were 251, metadata requests were 7,705 (up from 6,827 in 2016). The kind of metadata requested includes biographical details of the phone number owner, coverage data and antenna locations, details related to potential acts of fraud, Internet Protocol address location, requests to redirect emergency service calls, and code to unlock SIM card.²⁵⁷ According to Millicom, While some judicial oversight exists for requests in most of its African operations, in two countries the president can also order interception, and only in one country are the laws and processes clear on who is allowed to make requests for surveillance, customer data or service suspensions, as well as how and in what circumstances those requests may be made. As an example, in one African country, Millicom received requests for customers' meta data from the Attorney General's Office, the national police force, judges, the General Comptroller of Accounts, the national army, the national tax authority, and lawyers.

²⁵² Internet Users Statistics for Africa, <https://www.internetworldstats.com/stats1.htm>

²⁵³ Facebook, Government Requests for User Data, <https://transparency.facebook.com/government-data-requests>

²⁵⁴ Requests for user information <https://transparencyreport.google.com/user-data/overview?hl=en>

²⁵⁵ Government Requests for User Data <https://transparency.facebook.com/government-data-requests>

²⁵⁶ Orange Transparency Report on Freedom of Expression and Privacy Protection

https://www.orange.com/en/content/download/43262/1315009/version/2/file/2017%20RAPPORT%20DE%20TRANSPARENCE_20.06.2017_final_eng.pdf

²⁵⁷ Millicom, Law Enforcement Disclosure Report 2017, <https://www.millicom.com/media/3223/law-enforcement-disclosure-report.pdf>

Vodafone Group notes in its report that the legal position in Kenya remains unclear regarding whether or not it would be lawful for Safaricom or Vodafone to disclose statistics related to agency and authority communications data demands.²⁵⁸ The company cites section 3 of the Official Secrets Act and Section 37 of the National Intelligence Service Act which read together limit the right to information by providing for certain instances where publication or unauthorised disclosure of information is deemed an offence, for example the publication of data collected by security agencies in Kenya or where such publication would be prejudicial to safety and the interest of the Republic of Kenya. However, in its report, Vodafone says information requests from the Tanzania government stood at 2,127, while in DRC there were 635 requests.

Ideally, communication surveillance is justifiable where it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.²⁵⁹

5.5 Privacy Breaches by Business Entities

Like other actors in society, business enterprises should respect individuals' privacy and other human rights. Many private enterprises play a key role in the design, development, and dissemination of technologies; provision of communications; and some of them facilitate state surveillance activities. In the digital economy, there is increased concern about business models that threaten privacy rights. The integration of platforms and services, data sharing between organisations, cross-border data flows, business models reliant on data, data analytics, can all be a threat to the privacy and personal data, if not well managed.

5.5.1 Legal Responsibility of Business Entities

Laws in different countries require telecommunication services providers and other agencies collecting personal information to ensure the security of such information. In Rwanda, Article 125 of the Law on Information and Communication Technology requires electronic communications network or service providers to take all technical and organisational measures necessary to ensure that the services and associated electronic communications networks are fully secured. They are also required to inform users about any security risks which may occur as a result of a breach of network security measures, or protocols and the necessary remedies available to address the breach of network security.

Tanzania's Electronic and Postal Communication Act, 2010 protects customers' data from unwanted disclosure.²⁶⁰ In addition, the Electronic and Postal Communications (Consumer Protection) Regulations, 2018 requires the protection of information collected by mobile operators, such as SIM card registration information, against improper or accidental disclosure.²⁶¹ The provision thus restricts disclosure to third parties. Moreover, section 8(1) of the Cybercrimes Act, 2015 makes it a punishable offence to "obtain computer data protected against unauthorised access without permission". It also states that "without prejudice to the National Security Act, a person shall not obtain computer data protected against unauthorised access without permission". Whereas this provision protects personal data, it allows access for national security reasons.

²⁵⁸ Country-by-Country Disclosure of Law Enforcement Assistance Demands 2015-16, Vodafone https://www.vodafone.com/content/dam/vodafone-images/sustainability/dfp/pdf/vodafone_drf_law_enforcement_disclosure_country_demands_2015-6.pdf

²⁵⁹ Necessary and Proportionate Principles <https://necessaryandproportionate.org/principles>

²⁶⁰ See regulation 6(2) (e) of the Electronic and Postal Communication (Consumer Protection) Regulations, 2018.

²⁶¹ See Regulation 6(2) (e) of the said Regulations.

In Burundi, the practices of agents selling SIM cards of the different telecommunication operators in the streets were of concern. The agents were responsible for the collection of personal details as requested by the ARCT's order No 1 in a form. After that, they took a photograph of individuals and sent them to the operators from their phones. One of the concerns was that the collection was done openly with the forms left exposed. Further, agents had no guidance on how to secure, store or dispose the filled-in forms, while ensuring confidentiality. The Kenya Information and Communications Act (Consumer Protection) Regulations, 2010 under rule 15, does not permit licensees to sell or offer for free to third parties, any information they collect without the prior consent of the consumer concerned.

In the DRC, there has been concern regarding incidents of fraud through the Vodacom Congo mPesa mobile money transfer service. In June 2018, the company took steps to educate their users. In a message to its subscribers, it stated: "Vodacom Congo informs the public of the presence of a fraud mechanism set up by a criminal who calls subscribers on behalf of the operator for the purpose of defrauding their M-PESA account. This fraud is essentially based on the knowledge of the subscriber's personal data."²⁶² Similar campaigns have been conducted by other network operators in the country.

5.5.2 Mishandling of Customer Data

Business entities should not facilitate violation of rights to privacy by complying with government information requests that are illegal, or implementing technical measures that violate privacy rights. There have been reports of data breaches in Kenya by private entities and government institutions.²⁶³ Privacy breaches in the social context are much more commonplace and rarely considered violations. For example, appeals for blood donations are common in Kenya and the public are required to provide details of the patient in need of blood, their national identity number, the hospital they are in, their condition, blood type and mobile phone number. Privacy breaches on social media are also common and take the form of posts with exposés of private information; screenshots of private correspondence, criminal charge sheets, academic transcripts, national identity cards, and details of places of work and residence. These social breaches are not treated as threats to privacy often due to lack of awareness even by the data subjects themselves.

In October 2016, Laura Wambi made a complaint to Telkom Kenya on Twitter about one of their customer service employees who had contacted her on WhatsApp late at night after retrieving her number from the registration sheet of the customer care service centres, requesting to get to know her.²⁶⁴ While the company apologised publicly on their official Twitter handle, the action it took remains unknown. It also raises questions on the integrity of staff handling data, internal privacy policies, the extent to which employers take steps to sensitise their employees on data security and privacy, as well as provide corrective measures on the same.

Kenya was also affected by the Cambridge Analytica scandal, where the company is said to have used data mined from Facebook to influence the political outcomes.²⁶⁵ There being no law regulating breaches, data mining, data processing of citizen data and the sale of personal information. However, for privacy breaches involving a licensee of the Authority, complaints may be made to the Communication Authority or seek redress from the courts.

²⁶² <http://interkinois.cd/vodacom-congo-communique-de-presse-protection-donnees-abonnes/>

²⁶³ #OpAfrica hacks on the Ministry of Foreign Affairs communication system, and data leaks for example of National Oil Corporation employees. (<https://www.reuters.com/article/us-cyber-kenya/hackers-leak-stolen-kenyan-foreign-ministry-documents-idUSKCN0XP2K5>; <https://www.hackread.com/anonymous-hacks-kenyan-oil-firm-against-police-brutality/>)

²⁶⁴ Richard Mureithi, *Invasion of privacy: The case of Laura Wambi vs Telkom Kenya*, <https://hapakenya.com/2016/10/03/invasion-of-privacy-the-case-of-laura-wambi-vs-telkom-kenya/>.

²⁶⁵ Justina Crabtree, *Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections*, <https://www.cnn.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html>

In Kenya, the Election (Technology) Regulations 2017 under rule 14 require the Independent Electoral and Boundaries Commission (IEBC) to put in place mechanisms to ensure information security, data availability, accuracy, integrity, and confidentiality.²⁶⁶ The Commission is required to adopt tools to detect, prevent and protect against attacks and compromise of the election technology. In March 2017, the Commission admitted that hackers had attempted to breach its systems to steal crucial information ahead of the 2017 election.²⁶⁷ Similar allegations of hacking were made by opposition leader Raila Odinga during the August 2017 presidential election petition at the Supreme Court, which were denied by both the Commission and OT-Morpho, the French biometrics firm that supplied the election technology system.²⁶⁸ The Commission was criticised for hosting critical election data in the cloud, and it has been suggested by experts that such critical databases should be hosted in-country.²⁶⁹

In Rwanda, cases of breach of privacy and data protection may result in a prison sentence or hefty fines as provided by the penal code and other laws.²⁷⁰ The redress, however, seems more effective where it concerns the private sector as compared to breaches by state actors. Although the law does not explicitly provide for data residency, Rwanda's biggest telecom company, MTN, was fined USD 8.5 million in May 2017 for breaches of privacy and data protection.²⁷¹ The regulatory authority, Rwanda Utilities Regulatory Authority (RURA), found MTN guilty of storing data of Rwandan clients in a Ugandan data centre rather than locally as required.²⁷² The country's penal code and ICT laws also punish cybercrimes related to personal data protection, such as: unauthorised access to computer data; unauthorised access to and interception of computer service; and damaging or denying access to computer system among others.²⁷³

In 2011 state-owned Ethio Telecom was reported to have introduced Deep Packet Inspection (DPI),²⁷⁴ a technology that allows internet service providers to examine communications on the internet, including emails and web searches. While the technology is ideally meant for commercial purposes, it can also be used to monitor personal communication and thus, highly prone to abuse. The company also uses the ZSmart customer information system installed by the Chinese telecom company ZTE.²⁷⁵ The technology manages all customer information and it can automatically record certain personal information, such as location, SMS, and calls made on Ethio Telecom networks. Further, the company uses ZXMT, also installed by ZTE, which is capable of monitoring internet traffic and intercepting web browsing, web-based emails and other similar communications. Some informants in the study indicated that with a bribe of not exceeding a 1000 birr (USD 35), one can access call records of Ethio Telecom's customers.

In Zambia, there was controversy in January 2014 when a mobile subscriber claimed that his SIM card had been registered by Airtel Zambia without his authorisation.²⁷⁶ The subscriber, Brigadier General Miyanda, an opposition leader who was opposed to the SIM card registration campaign in the country and had vowed not to register his SIM card, even as the deadline had been set for January 31st 2014. Opponents of SIM registration stated that deactivation of unregistered SIM cards violated fundamental rights and liberties under the constitution. Despite this, he received

²⁶⁶ Text of the Regulations, <https://bit.ly/2lIXTKI>.

²⁶⁷ Chebukati admits hackers attacked IEBC servers, <https://bit.ly/2zxfKn8>.

²⁶⁸ IEBC system was not hacked: French firm, <https://bit.ly/2DzHrzM>.

²⁶⁹ Don't fear cloud computing. You already use it, <https://bit.ly/2DzgZGo>.

²⁷⁰ The Penal Code, Article(s) 280-291

²⁷¹ Reuters, Rwanda regulator fines MTN Rwanda \$8.5 mln over external IT hub, May 17, 2017, <https://reut.rs/2zxlj3V>. See also Edmund Kagire, Rwanda slaps \$8.5m fine on MTN, <https://bit.ly/2Q50tzs>

²⁷² Rwanda Utilities Regulatory Authority, Board Decision N°001/Bd/Rura/2017 Of 12th May 2017 Imposing Regulatory Sanctions to Mtn Rwanda Ltd, <https://bit.ly/2NGvj55>

²⁷³ ICT Law, articles 197-207

²⁷⁴ R Sandvik, 'Ethiopia Introduces Deep Packet Inspection' (2012) Tor Project Blog, <https://blog.torproject.org/ethiopia-introduces-deep-packet-inspection>

²⁷⁵ Human Rights Watch, "They know everything we do": Telecom and Internet Surveillance in Ethiopia, 2014, <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>.

²⁷⁶ Airtel Registers Godfrey Miyanda's SIM card without his authorisation

<https://www.lusakatimes.com/2014/01/19/airtel-registers-godfrey-miyandas-sim-card-without-authorisation/>

messages from the company confirming the registration of his SIM card, despite not having filled-in forms or applied to the company or any other service provider for the registration of his SIM card. The company later acknowledged and apologised for registering his SIM card without his knowledge, saying it had been in error.²⁷⁷ Other breaches include colleges and universities collecting biometrics of students without sufficient safeguards.

The company was on the spotlight again in August 2018, when it was sued by its customer, Olypa Chisha Chilembo for negligence and breach of confidentiality.²⁷⁸ Chilembo's claim was that in May 2018, an Airtel employee revealed her Airtel Money account information to a third party, without her consent or authority. The third party, Sharon Musonda, had a day before, deposited money into Chilembo's Airtel Money account and visited an Airtel Customer Care Centre to confirm the transaction.

In August 2017, Malawi Defence Commander, General Supuni revealed that Malawi did not have the equipment and expertise to combat cyber crimes in the government, military, finance and commercial sectors and urged for renewed focus on cybersecurity.²⁷⁹ Nonetheless, Article 84 of the Electronic Transactions provides for offences such as unauthorised access, interception or interference with data.

The website of Nigeria's Independent National Electoral Commission (INEC) was hacked in March 2015.²⁸⁰ A group called Nigerian Cyber ARMY claimed responsibility for the hack, targeting the database of the website and information gathered from the card readers of millions of Nigerian voters. However, INEC claimed no data was jeopardised and that the site was reclaimed hours after.

5.5.3 Targeted and Indiscriminate Communication

With regards to indiscriminate communication, Burundian mobile phone subscriber continue to experience the use of unsolicited bulk SMSes especially for marketing campaigns by third parties. For instance, end users subscribed to ECONET LEO have been receiving advertisement SMSes from PAMOJA Festival (a gospel music festival) held in Bujumbura in July 2018. It is not clear how PAMOJA festival organisers could obtain phone contacts of ECONET LEO subscribers. In Ethiopia, the use of targeted and indiscriminate communication, particularly bulk SMS, has been on the rise. Ethio Telecom abuses its monopoly to send out promotional SMS texts from itself and its partners.²⁸¹ Specifically, the number of bulk SMS marketing calling for lottery draws or demanding to offer information in return for a certain fee are also on the increasing. While many customers are discontent about these actions, those who have tried to stop receiving SMS have been unsuccessful.

Also, during the August 2017 election period, many people in Kenya received unsolicited and targeted campaign messages from politicians in violation of the Guidelines on Bulk Political Messaging.²⁸² According to a recent survey, members of the public are opposed to such measures which they are usually subscribed and charged for without consent thereby forcing the recipients to Opt-out of the subscription instead of having the option to Opt-in.²⁸³ Moreover, many recipients of such messages are not aware of how to opt-out of such messages. Further, the public are not aware of how politicians get access to their contact information. In Senegal, the sending of unsolicited SMS from politicians has also been a common phenomenon.²⁸⁴

²⁷⁷ Airtel apologises to Godfrey Miyanda over SIM registering <http://www.lusakavoice.com/2014/01/28/airtel-apologises-to-godfrey-miyanda-over-sim-registering/>

²⁷⁸ Lusaka woman sues Airtel for breach of confidentiality <http://tumfweko.com/2018/08/14/lusaka-woman-sues-airtel-for-breach-of-confidentiality/>

²⁷⁹ Malawi Lack Capacity to Fight Cyber Security Threats, Say Army Commander: <https://www.nyasatimes.com/malawi-lack-capacity-fight-cyber-security-threats-says-army-commander/>

²⁸⁰ INEC website hacked, reclaimed moments later, <https://bit.ly/2xRMYLW>.

²⁸¹ Getachew T. Alemu, Ethio Telecom's Faulty Choice Theory, 12 April 2012, <https://bit.ly/2N10rqq>.

²⁸² Guidelines for prevention of dissemination of undesirable bulk political sms and social media content via electronic communications networks June 2017, <https://bit.ly/2DzAui3>.

²⁸³ New Report: Biometric Technology, Elections, And Privacy in Kenya, <https://bit.ly/2ONPbzg>.

²⁸⁴ In case of violation of personal data and privacy: Senegalese can now file a complaint before the Protection Commission, <https://bit.ly/2DvgH3e>.

Regulators have shown their ability to take steps to address abuse. In 2015, the UCC imposed a fine of UGX 5 billion (USD 1.7 million) against MTN Uganda for breach of communication directives and non-compliance.²⁸⁵ The fine represented 0.5% of MTN Uganda's gross annual revenue of MTN Uganda. The company was censured under sections 41 (1) (a) and section 41 (2) (b) of the Uganda Communications Act for defying a UCC directive to desist from using SMS short codes 157, 169, 178, and 183.²⁸⁶

5.6 Dispute Resolution and Remedies

Generally, recourse and remedies for violation of the constitutional right to privacy are available from courts which can offer various reliefs, including declarations, judicial review, injunctions, or even awards of compensation to aggrieved parties. Some of these courses of action are contained either in the constitution or acts of parliament.

5.6.1 Existing Frameworks for Remedies

Given the absence of data protection legislation in most of the countries, there are no standard complaint handling procedures. However, there are some remedies for redress for breaches of privacy or data. In Zimbabwe, section 8(13) of the Postal and Telecommunications Subscriber regulations grants anyone aggrieved by the unlawful use of their personal data the right to seek legal redress. Under section 18 of the Interception of Communications Act, a person aggrieved by a warrant or directive relating to interception of communications, may appeal to the Administrative Court within one month of being notified or becoming aware of it. The court may confirm, vary or set aside the warrant, directive or order. However, given that interception is usually done without the knowledge of the subject, it is difficult to know if there has been a breach.

The AIPPA provides for an internal remedy mechanism before recourse can be had to the courts. Section 53 provides for reviews relating to collection or correction of personal information amongst other reviews, to be made to the Zimbabwe Media Commission. However, recourse to this body has been of public contention since the coming into force of this law. This is because the Commission is loaded with multiple regulatory roles such as information requests as well as media regulation matters. Also, its mandate relating to protection of privacy and data protection is very limited. Moreover, this Commission has had no Commissioners since 2015, when the terms of the previous commissioners expired and despite interviews for new commissioners being conducted, no appointments have been made, nor has the government given reasons for the delay.²⁸⁷

Tanzania's Electronic and Postal Communications (Online Content) Regulations provide for a complaints procedure. Rule 16 requires aggrieved persons to file complaints to the online content providers on prohibited content. The content providers are required to resolve the complaints filed within 12 hours, and failure to which the aggrieved person may refer the complaint to the Tanzania Communication Regulatory Authority (TCRA). TCRA shall then handle the complaint through the Content Committee procedures.

²⁸⁵ UCC has Fined MTN UGX 5billion over abuse of short codes and warned other Telecoms of similar Penalties, <https://bit.ly/2R2vNQI>.

²⁸⁶ MTN Uganda Weighing Legal Action over UCC UGX 5 Billion Fine, <https://bit.ly/2NISCLi>

²⁸⁷ Zimbabwe Independent, Misa sounds warning, <https://bit.ly/2QaEWVT>.

5.6.2 Notable Judicial Decisions

There have been some decisions by courts on different aspects of the right to privacy. These decisions are useful in understanding the extent of the right, its implications and the necessary limitations as interpreted by the courts. In *Okiya Omtatah Okioti v Communication Authority of Kenya & 8 others* [2018] eKLR²⁸⁸ the High Court declared the decision by the Communications Authority to install a Device Management system (DMS) to access information on the IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), Mobile Station International Subscriber Directory Number (MSISDN) and Call Detail Records (CDRs) of mobile network subscribers unconstitutional, null and void to the extent that it was arrived at unilaterally, without adequate public participation. The court also found it to be a threat to the right to privacy of subscribers and a gross violation of their constitutionally and statutory protected consumer rights.

In Tanzania, in the case of *Jamii Media Ltd v. Attorney General*²⁸⁹, the Court demanded that the Government puts in place procedures which can be used by the police in requesting information under the Cybercrimes Act, 2015 instead of relying on the general provisions which may be used to infringe the right to privacy. The court ruled that under section 32 (4) of the Cyber Crime Act, police were not allowed to take items but rather to take the evidence needed by way of a printed form. The court emphasised the importance of police seeking the court's intervention in circumstances where the police failed to secure data or information under the provision.

In 2018, the Supreme Court Cassation Division in Ethiopia made a landmark decision on the right to privacy. The Court in *Riyan Miftah vs. Elsewdi Kebels Plc*, ruled that no image or photograph of a person may be publicly exhibited, sold or disseminated without the consent of the person and the latter is entitled to damages for violation of the right of image.²⁹⁰

²⁸⁸ *Okiya Omtatah Okioti v Communication Authority of Kenya & 8 others* [2018] Eklr, <http://kenyalaw.org/caselaw/cases/view/151117/>

²⁸⁹ *Miscellaneous Application No.9 of 2016, High Court of Tanzania at Dar es Salaam.*

²⁹⁰ *Kinfe Michael, Sources of Ethiopian Privacy Laws*, <https://www.abbyssinialaw.com/component/k2/item/1544>

6 Conclusion and Recommendations

6.1 Conclusion

The right to privacy can only be adequately guaranteed when states adopt policy, legal, and institutional frameworks that meet international human rights standards. International and regional human rights laws and instruments provide a robust and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance; the interception of digital communications; and the collection of personal data. However, practices in many countries under review revealed a lack of adequate national legislation and enforcement, weak procedural safeguards and ineffective oversight, which has contributed to widespread impunity for arbitrary or unlawful interference with the right to privacy.

On the continent, different regional economic communities have taken various measures to protect privacy and personal data. The various efforts are in response to the emerging technologies, challenge of globalisation, and the need for the establishment of uniform system of rules between countries to enhance cooperation and create a safe environment for citizens. In recent times, the African Union (AU) has also taken steps to strengthen privacy and personal data protection.

At the national level, the constitutions of the countries under review contain provisions that uphold the protection of the rights to privacy. However, of the 13 countries under the study, only Ghana and Senegal have comprehensive privacy and data protection laws. The lack of a comprehensive standalone policy or legislation to protect the right to privacy and data protection was identified as a major weakness, since the provisions were fragmented and contained in various laws and policies, and did not adequately provide for protection of the right. Whereas some countries such as Kenya, Malawi, Nigeria, and Uganda have data protection bills, the proposed laws have failed to progress through their parliaments for years.

This study has found that states are legitimising and increasing their surveillance capacity, including by requiring mandatory registration of personal details and increasingly compelling service providers to hand over users' data. But the surveillance activity is often not guided by judicial or other independent oversight, and in some instances there is no clarity as to which individuals and government departments have the authority to order surveillance or demand customers' meta data from telecom companies. This means that many government departments make such orders to the operators, who do not have the latitude to reject such requests. Telecom and ISPs are required by law to comply with information requests or requests for surveillance assistance, including the common requirement to install software with the technical capacity to conduct surveillance and to enable active communications monitoring, and to hand over data when asked.

In all countries reviewed, these requests are kept secret so it is difficult to establish the full extent of government requests for users' data, the surveillance of citizens' communications, and censorship of content. What is clear though, is that the trend is on the increase, and the types of user's' information which governments request is varied.

Most countries have adopted mandatory SIM card registration where subscribers are required to furnish telecom companies with extensive personal details, including names, home addresses and their National Identification Numbers (NINs). Without a comprehensive privacy and data protection law (and an accompanying practice by government agencies and telcos which robustly protects such data), such data is at tremendous risk of abuse by state and non-state actors.

There are levels of public awareness about privacy and data protection, with many citizens tending to be indifferent to privacy and data protection issues. This low level of awareness among the public of privacy issues in the digital environment, a lack of transparency by data controllers, insufficient procedural guarantees, and limited independent oversight over the implementation of privacy and data protection, present key risk factors.

The responsibility of protecting the right to privacy and personal data is not only limited to government agencies, but also business entities, specifically telecom companies and ISPs who collect and process clients' data during service provision. While different legislations place some responsibilities on them, they are also required to proactively ensure that the right to privacy is protected through internal policies and terms of services, as well as challenging governments' undue requests for clients' personal data.

Ultimately, the state of personal data protection is a mirror of the state of internet freedom in a country. In most countries studied, there are various worrying developments. There has been an increase in digital rights violations such as arrests and intimidation of social media users, a proliferation of laws and regulations that undermine internet access and affordability, network disruptions, increasing criminalisation of online conduct – all of which weaken the potential for digital technologies to improve livelihoods, catalyse free expression and civic participation. In turn, efforts to promote strong privacy and data protection regimes should go in tandem with multi-stakeholder efforts to advance broader internet freedoms in Africa.

6.2 Recommendations

6.2.1 Government

African governments should:

- Comply with their obligations to respect, fulfil and protect and give effect to the right to privacy, by developing comprehensive policies and legislation or where drafts exist, to finalise them within the next one year. The framework should provide for: data collection, processing, sharing and security, big data, and profiling; define the rights of data subjects and responsibilities of data controllers and processors; provide for dispute resolution and effective remedies for breach including against private entities e.g. compensation, accounting for profits, penalties, cease and desist orders; establish adequate checks and balances, including an independent oversight body; be technology neutral; ensure transparency and accountability, including requiring user notification and transparency reporting.
- Review all current procedures, processes, practices, policies and legislation related to communications surveillance, interception and collection of personal data, and amend them to ensure that they are clear, transparent and in full conformity with international human rights standards on privacy protection, including the International Principles on the Application of Human Rights to Communications Surveillance.
- Ensure the limitations to the right to privacy are based on accessible, transparent, clear, comprehensive and non-discriminatory laws. These limitations should be based on legitimate aim, and proportionate to the aim pursued, and necessary to safeguard the public interest in a democratic society.
- Clearly define what constitutes national security and ensure that national security concerns donot trump human rights.
- Ensure national security or state surveillance programmes of individuals are proportionate, fair, in compliance with international norms and standards, governed by the rule of law, and subject to impartial and independent judicial oversight.
- Invest in and build the capacity of relevant staff including in law enforcement officers, prosecutors, judges, lawyers, and other government officials on privacy and data protection in the digital economy
- Inform and educate the public about the purposes for which their personal data is collected, the agencies or persons authorised to collect data, the implications of such collection, and the measures taken to secure their data.
- Adopt the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention).
- Adopt a multistakeholder approach in engagement and involve and engage all relevant stakeholders law and policy making.

6.2.2 Companies/Business

They should:

- Be transparent about the information requests they receive from government and in how they handle personal data.
- Take responsibility to protect human rights throughout their operations in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, including the right to privacy in the digital age. This responsibility should be independent of whether a State meets its own human rights obligations and should extend to their supply chain e.g. third party suppliers, sub-contractors or vendors.
- Take all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses. This includes commitment to push back on illegal information requests, resisting being compelled or encouraged to sell, build or integrate surveillance capabilities into their systems and to not abuse users’ data for commercial gain.
- Implement the recommendations of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, which calls on companies to “seek to prevent or mitigate the adverse human rights impact of their involvement to the maximum extent allowed by law.”²⁹¹
- Practice transparency and inform users about the collection, use, handling, sharing and retention of their data that may affect their right to privacy and to publish transparency policies and reports, as appropriate;
- Provide redress mechanisms and support for all its customers and users to help them protect their privacy, manage and control the use of their personal data;
- Protect the security of personal data in their custody, including through the enhancing security measures and the conduct of privacy risk audits.
- Develop internal principles and policies on privacy and data collection in accordance with local constitutional and international human rights standards and inform users of their privacy rights before commencing collection of data or use of their services. The policies should be publicly available e.g. on their websites and users should also be regularly informed of changes to such policies.
- Train their employees and subcontractors on how to comply with privacy and data protection laws and policies.

6.2.3 Academia

They should:

- Support civil society to lobby Governments for the development of data protection and privacy policies and enforcement of those policies through research and provision of sound evidence based research.
- Provide intellectual leadership and guidance in society through research and outreach, and highlight concerns on the right to privacy to key stakeholders, politicians and policy makers.

²⁹¹ See: http://op.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

6.2.4 Media

They should:

- Create more awareness and civic education on the importance of the right to privacy while highlighting issues concerning the right, including through the provision of information in the public interest through news stories to erode the state culture of secrecy.
- Continue to expose and investigate breaches of data protection and privacy by custodians of data.
- Take advantage of its watchdog role and agenda setting role to remind the public, the government and key stakeholders of the importance of having policies and laws on privacy and data protection.
- Be mindful and considerate of the privacy rights of others and ensure that some of the stories do not perpetuate the violation of the right. As commercial enterprises, they also have a responsibility to comply with the UN Guiding Principles on Business and Human Rights.
- Report objectively and inform the public in their countries of the various developments on the right to privacy.

6.2.5 Technical Community²⁹²

They should:

- Develop or strengthen the avenues through which privacy breaches can be reported.
- Develop technology with privacy principles integrated as part of the general design and default settings. A useful step is the adoption of the seven principles of the concept of privacy by design to serve as a foundation for privacy and data protection.
- Increase their involvement in processes that seek to influence the development and implementation of data protection laws.
- Offer useful solutions to lawmakers who are often not well versed with the technicalities surrounding the implementation and impact of technology on human rights.

6.2.5 Civil Society

They should:

- Advocate and defend the right to privacy, including in the digital sphere as a priority.
- Sensitise the general public on their rights to privacy and the need for personal data protection.
- Advocate and present tangible and evidence-based proposals to policy makers towards administrative, policy, legislative and institutional changes that are necessary to strengthen the protection of the right to privacy.
- Strengthen cooperation and collaboration between mainstream human rights CSOs and other stakeholders such as academia, the technical community, business and government in order to keep abreast with new technology, find better solutions to privacy challenges in the digital age and appreciate the impact of new technologies on human rights.
- Remain vigilant and monitor the implementation of the right to privacy and continue to document and highlight ongoing violations whenever they occur, giving special attention to excesses by the state and businesses in their collection and processing of personal data.
- Continue to litigate against infringement of the right to privacy and seek progressive judicial interpretations through strategic litigation.
- Conduct studies and research to identify gaps in the management of personal data by private and public bodies.
- Create more awareness among the general public and build their capacity on the right to privacy so that they are better informed, more vigilant, and cautious with their personal data.

²⁹² Technical community to include – telecoms, social media platforms, developers/innovators



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

156-158 Mutesa II Road, Ntinda, P.O Box 4365 Kampala, Uganda.

Tel: +256 414 289 502 | Mobile: +256 790 860 084, +256 712 204 335

Email: programmes@cipesa.org

Twitter: [@cipesaug](https://twitter.com/cipesaug)

Facebook: facebook.com/cipesaug

www.cipesa.org