State of Internet Freedom in East Africa 2015

Survey on Access, Privacy and Security Online

September 2015

CIPESA

OpenNet Africa

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support from the Humanist Institute for Co-operation with Developing Countries (Hivos) and the Open Technology Fund (OTF).

The report presents the findings of a study on the threats to access, privacy and security online, as well as the knowledge, attitudes and practices of citizens on internet freedom in East Africa. Full length country reports for Burundi, Kenya, Rwanda, Tanzania and Uganda are also available.

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, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Marilyn Vernon, Wairagala Wakabi

Country researchers

Burundi: Jean Paul Nkurunziza - Internet Society Burundi Chapter and Alain Ndikumana - Institut des Statistiques et Etudes Economiques du Burundi (ISTEEBU)

Kenya: Kenya ICT Action Network (KICTANet)

Rwanda: Jean Claude Niyibizi – Independent researcher

Tanzania: Jamii Media

Uganda: Esther Nakkazzi and Edris Kisambira – Independent researchers

Design

Ish Designs
muwonge_issa@yahoo.com

State of Internet Freedom in East Africa 2015
Published by CIPESA, www.cipesa.org
September 2015

CONTENTS

1. INTRODUCTION

The internet and other digital technologies have become key platforms for East African citizens to enjoy their rights to expression and to associate with other citizens as well as to engage with leaders. Internet access continues to rise, with penetration in Kenya standing at 69% of the population, Uganda (20%), Rwanda (31%) and Tanzania (22%). The mobile phone access rate in Kenya stands at 84%, Rwanda (74%), Uganda (62%), Tanzania (71%), and Burundi (31%). There is also growth in broadband access with the expansion of fibre bandwidth supplied through submarine cables[1] landing at the East African coast and national fibre backbones deployed by governments, often in consort with private actors. In Kenya, Rwanda, Uganda and Tanzania, universal access funds are being used to extend modern Information and Communication Technology (ICT) services to rural and remote areas, and to offer free or subsidised internet access at community anchor institutions such as schools, hospitals, community centres and local government offices.

As the number of internet users grows, so does the content questioning governments' democratic and transparency credentials. Increasingly, however, there are numerous challenges to free expression online in the region and these are affecting the way citizens and organisations communicate over digital technologies. Governments are enacting laws that threaten the right to freedom of expression, both online and offline. The region has registered a rise in abuses and attacks on internet freedom, including a proliferation of laws, legal and extra-legal affronts, with limited judicial oversight over surveillance and interception.

Exploratory research published by CIPESA in May 2014 showed that since 2010, East African countries have enacted numerous laws that provide for the interception of communications, place responsibility on internet intermediaries to monitor users and block or remove content, and in various ways, introduce or extend the reach of the law in regulating online content and activity. Uganda enacted its Interception of Communications Law in 2010, Rwanda in 2013, while 2013 amendments to Burundi's Code of Criminal Procedure provides for interception of communications as does Kenya's 2012 National Security Services Act.[2]

Other recent developments also make it crucial to explore ways to advance internet freedom and cyber security in the region. In December 2014 Uganda solicited citizens' inputs to a Data Protection and Privacy Bill that falls short of safeguarding privacy rights, but eight months later remained quiet on what it planned next with the bill.[3] Tanzania passed a Cybercrimes Act that leaves the door open for trampling internet rights, after ignoring civil society protests about the shortcomings of that law.[4] The country also enacted a statistics law that drew civil society criticism for limiting citizens' access to information. Kenya passed the Security Laws (Amendment) Act 2014 that restricts civic space and gives state agencies more powers over citizens' digital communications, and its Cybercrime and Computer related Crimes Bill (2014) equally threatens free speech.[5] In Burundi and Rwanda, online journalists and bloggers continue to be cowed, and fear of surveillance continues to entrench wide-scale self-censorship. During upheavals of March 2015 and throughout the coup attempt of May 2015, media freedom in Burundi took a big hit with several radio stations getting closed, many journalists fleeing into exile, and at the heart of the civil unrest, government is reported to have ordered service providers to cut access to short messaging service (SMS) and WhatsApp.[6]

Even with the plethora of new laws that are being passed, old laws dating back to the 1970s have been used as recently as 2013 to curb internet freedom in countries like Uganda and Tanzania. Meanwhile, in Kenya, Rwanda and Burundi, hate speech content regulations pose a threat to internet freedom. Kenya's National Cohesion and Integration Commission formed in the aftermath of the 2007-2008 post-election violence, which was partly fuelled via ICT tools (notably by SMS) remains at the forefront of bringing social media 'abusers' to prosecution. Tanzania, which goes to the polls in October 2015, has this year passed a series of laws criticised as aimed at stifling dissent. The country has

[1] *Eastern Africa Submarine System (EASSy), SEACOM/Tata TGN-Eurasia and The East African Marine System (TEAMS)*

[2] *State of Internet freedom in East Africa 2014, http://www.cipesa.org/?wpfb_dl=76*

[3] *Reflections on Uganda's Draft Data Protection and Privacy Bill 2014, http://opennetafrica.org/reflections-on-ugandas-draft-data-protection-and-privacy-bill-2014/*

[4] *Tanzania Cybercrime Bill Should Safeguard Citizens' Rights on the Internet, http://www.opennetafrica.org/tanzania-cybercrime-bill-should-safeguard-citizens-rights-on-the-internet/*

[5] *Is Kenya Putting the Chill on Internet freedom? http://www.cipesa.org/2015/03/is-kenya-putting-the-chill-on-internet-freedom/*

[6] *Burundi's radio silence: Political crisis forces stations off air, http://america.aljazeera.com/articles/2015/5/20/burundis-radio-silence-independent-stations-forced-off-air.html and Protest-hit Burundi cuts mobile networks, blocks Twitter and Facebook as strongman brings hammer down, http://mgafrica.com/article/2015-04-29-protest-hit-burundi-cuts-mobile-networks-blocks-twitter-and-facebook-as-strongman-puts-the-hammer-down*

also issued tough new rules for bloggers in relation to elections reporting.[7] Ugandan authorities have similarly stepped up actions against social media users under the pretext of promoting public order and unity as well as preventing the spread of false information.[8]

Meanwhile, instances of cybercrime such as cyber fraud, identity theft, website hacking, and online violence against women including revenge pornography also seem to be on the rise, providing governments a duty to protect citizens, private businesses and state interests.[9] Unfortunately, counteractive government actions often come at the expense of individuals' privacy and the right to freedom of expression.

With the mandatory registration of phone users in all five countries in the region, it is a concern that none of them has explicit data protection laws. Although governments in these countries argue that the SIM card registration process is neccessary to enhance national security – including to fight terrorism - the absence of laws to safeguard the privacy of users' data means that government agencies could easily mishandle and misuse telecom services users' data.

This report therefore aims to generate an understanding on the state of internet freedom in East Africa including the knowledge, attitudes and practices of East African citizens on internet freedom. It documents the nature of threats to online access, privacy and security in East Africa, and the effect of information controls on the online behaviours of citizens, journalists and human rights defenders. The findings of the study are aimed at serving as an insightful guide for media, academia, development partners, government and civil society's interventions in promoting human rights in the digital age and the safety and security of communications for citizens and organisations in the region.

[7] Tough New Laws for Tanzania's Bloggers, http://www.cipesa.org/2015/08/tough-new-election-reporting-rules-for-tanzanias-bloggers/

[8] Hunting Down Social Media 'Abusers' in Uganda as Elections Near, http://www.cipesa.org/?wpfb_dl=190

[9] See for Example, Revenge Pornography is on the Rise and Should be Addressed, http://www.opennetafrica.org/revenge-porn-is-rising-and-it-should-be-addressed/ and Keriako Tobiko and NCIC want Moses Kuria prosecuted for hate speech and incitement, http://www.nation.co.ke/news/Tobiko-NCIC-want-Moses-Kuria-locked-up/-/1056/2626550/-/lmmg7a/-/index.html

2. METHOD

The research presented in this report was conducted through a mixed methods approach: researchers based in the focus countries conducted policy and literature reviews plus interviews with key informants. In addition, Focus Group Discussions (FGDs) and stakeholder workshops whose participants were drawn from the media, civil society, private sector and government were conducted in Kenya, Rwanda, Tanzania and Uganda. The research mostly covered developments in the period between May 2014 and August 2015. For a list of organisations that participated in the study, see Annex 1.

Personal Interviews

OpenNet Africa country researchers interviewed more than 235 key informants. The respondents were drawn from stakeholder groups that either affected internet freedom, those whose internet freedom was likely to be violated, and those deemed knowledgeable about the subject. They included telecommunications regulatory authorities, government Ministies, Departments and Agencies (MDA) in charge of ICT, telecom companies and Internet Services Providers (ISPs), journalists, application developers, human rights defenders and activists, members of opposition political parties, and members of academia and the private sector.

The interviews centred on the common communication technologies citizens use; explored the general understanding of internet freedom among the respondents; probed them about who was most likely to violate citizens' online privacy and security; and what should be done to protect citizens' internet rights. The research also sought to understand the challenges faced relating to surveillance and information controls and how these challenges influence communications behaviour including any precaution to protect their privacy and security online.

Key Informants by Affiliation

Most respondents were drawn from the media (31%), followed by telecom companies/ ISPs (13%). Human rights defenders and NGOs each constituted 10% of the study participants. The private sector and academia each constituted 8%. The other stakeholder categories combined represented 10% of the individuals interviewed.

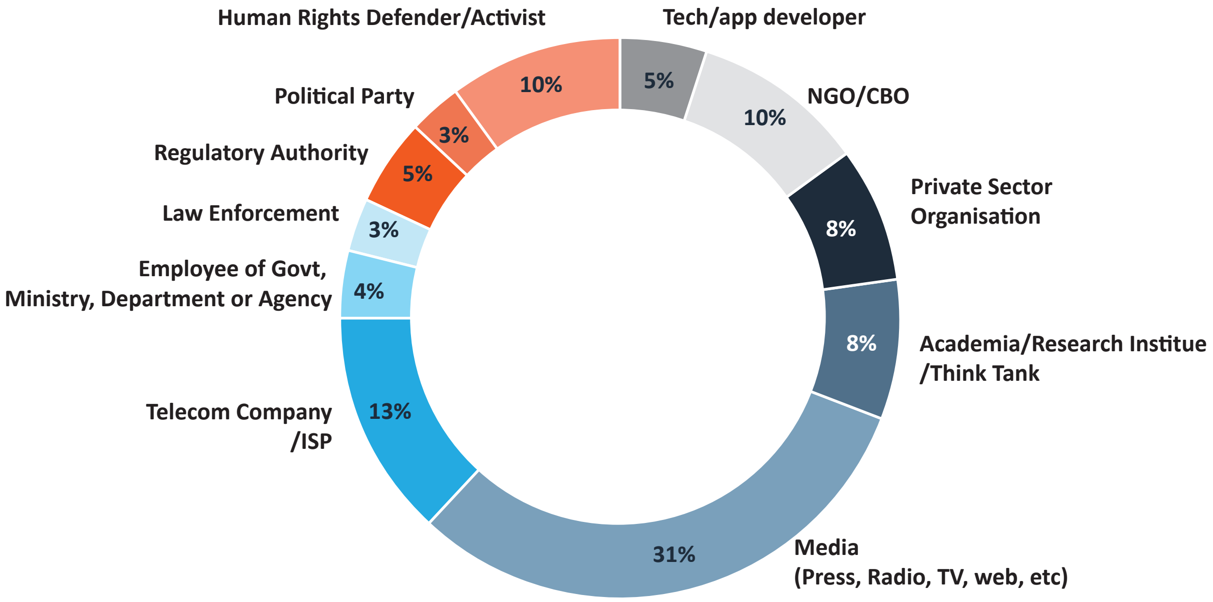

Figure 1: Affiliation of key informants

Focus Group Discussions

Focus groups involving 22 individuals were conducted in Kenya and Rwanda. The Kenya FGD had seven participants drawn from the government, civil society, media and private sector. In Rwanda, 15 participants were involved in the discussions, representing print, broadcast and online media institutions.

Stakeholder Workshops

The research also collected the views of a total of 75 human rights defenders, bloggers, journalists, editors, media rights organisations, sexual minorities and gender equality activists in Kenya, Tanzania, and Uganda who participated in digital safety and security training workshops during 2015.[10]

Descriptive statistics and Excel software were used as statistical tools to describe the data in terms of quantitative approaches, while thematic analysis was used to assess open-ended survey questions, workshop participants' views and focus group discussions.

[10] See CIPESA workshop activities: CIPESA Promotes Digital Safety Awareness and Skills for Media Practioners in Kenya, http://www.cipesa.org/2015/07/cipesa-promotes-digital-safety-awareness-and-skills-for-media-practitioners-in-kenya/; CIPESA Conducts Digital Safety Training for Journalists and Activists in Tanzania and Uganda, http://www.cipesa.org/2015/04/cipesa-conducts-digital-safety-training-for-journalists-and-activists-in-tanzania-and-uganda/; and World Press Freedom: Ugandan Journalists Convened for Digital Security Training, http://www.cipesa.org/2015/05/world-press-freedom-ugandan-journalists-convened-for-digital-security-training/

3. COUNTRY BACKGROUNDS

3.1 Burundi

ICT Access

Burundi has the lowest ICT access figures among the five members of the East African Community. As of June 2014, the industry regulator known as L'Agence de Régulation et de Contrôle des Télécommunications (ARCT) reported 3.2 million mobile phone subscribers. This represented a 31% mobile penetration rate amongst the country's population of 10 million.[11] Burundi's internet penetration as of December 31, 2014 was estimated to stand at 4.9%.[12]

In March 2015, a new telecom company - Viettel Burundi - launched commercial operations, having been licensed a year earlier.[13] The company, a subsidiary of the Vietnam-based Viettel Group, operates under the commercial name LUMITEL.[14] Lumitel joined five other players: Onamob, Africell Tempo, Econet and Ucom in the voice market. Previously, there were eight licensed Internet Service Providers, namely CBINET, OSA NET, Spider Net, USAN, Onatel, Africell Tempo, Econet, and Leo (UCOM). However, in October 2014, the global arm of Econet announced the acquisition of the assets of Leo (UCOM).[15] Onatel and Onamob are state-owned.

The national backbone infrastructure, Burundi Backbone System (BSS) which was launched in January 2014, now covers all the country's 17 districts. A consortium of the country's telecom operators is implementing the project, with support from the World Bank and the government.[16]

Meanwhile, a new mobile telephony taxation structure that started on December 24, 2014 imposed a tax of 42 Burundian Francs (US$ 0.024) per minute on local calls. The move is aimed at increasing income sources for the country's 2015 budget.[17] After the new tax measures were implemented on January 1, 2015, all promotional offers by mobile phone operators were stopped. The increased cost of communication led to protests by civil society organisations, such as the general strike organised on March 5, 2015.[18] Government talks with protestors were futile and the tax remains applicable to-date.[19]

Legal Developments

On May 15 2015, judges at the East African Court of Justice (EACJ) ruled that Articles 19 and 20 of the Burundian Press Law of 2013 were against the principles of democracy and press freedom as enshrined in the Treaty for the establishment of the East African Community (EAC).[20] However, the court upheld several other clauses, including those related to regulation of print and online media. The judges stated that they would direct Burundi to "take measures, without delay, to implement the Judgement within its internal legal mechanisms."[21] The ruling was made after the Burundi Journalists Union (BJU) petitioned the regional court to rule on the constitutionality of various clauses.[22]

Immediately after the law was promulgated in June 2013[23], journalists petitioned the local Constitutional Court which in January 2014 invalidated some of the clauses of the law.[24] Thereafter, the government proposed some revisions to the media law which were tabled and approved before parliament on March 4, 2015. Whilst BJU welcomed the move by government, the Union's president regretted that some regressive clauses remained and stated that they still await the decision from the EACJ.[25] Hearings in the case before the regional court started on February 9, 2015.[26]

[11] ARCT, Market Observatory First Half of 2014, http://www.arct.gov.bi/index.php/statistiques/43-observatoire-des-marches-premier-semestre-2014

[12] Internet World Stats, Africa, http://www.internetworldstats.com/africa.htm

[13] International Telecommunications Union (ITU), Statistics News Log, Viettel Wins Mobile Concession in Burundi, http://www.itu.int/ITU-D/ict/newslog/Viettel+Wins+Mobile+Concession+In+Burundi.aspx

[14] Lumitel, www.lumitel.bi and Facebook page at https://www.facebook.com/lumitelburundi/info?tab=page_info

[15] EconNet Announces Acquisition of Telecel Globe Operations in Burundi and CAR, http://www.techzim.co.zw/2014/10/econet-announces-acquisition-of-telecel-globe-operations-burundi-car/

[16] Burundi Backbone System Company, http://bbs.bi

[17] Burundi/Economie: Le Parlement Burundais Vote Le Budget de 2015, http://www.burundi-gov.bi/spip.php?article3744

[18] Burundi: appel à une grève générale à partir de jeudi, http://www.rfi.fr/afrique/20150304-burundi-appel-une-greve-generale-prevue-jeudi-collectif-contre-vie-chere-pierre-nku/

[19] A New General Strike in Burundi, http://www.rfi.fr/afrique/20150309-vers-nouvelle-greve-generale-burundi-collectif-contre-vie-chere-pierre-nkurunziza-s/

[20] East African Court Declares Sections of Burundi's Media Law "Undemocratic", http://www.cipesa.org/2015/05/east-african-court-declares-sections-of-burundis-media-law-undemocratic/

[21] EACJ Ruling, BJU Vs. The Republic of Burundi, http://eacj.org/wp-content/uploads/2015/05/Reference-No.7-of-2013-Final-15th-May-2c-2015-Very-Final1.pdf

[22] http://eacj.org/wp-content/uploads/2015/05/Reference-No.7-of-2013-Final-15th-May-2c-2015-Very-Final1.pdf

[23] Law Governing the Press 2013, http://www.presidence.bi/spip.php?article3779

[24] Constitutional Court quashes several repressive provisions of Burundian media law, http://www.ifex.org/burundi/2014/01/08/articles_quashed/

[25] La loi sur la presse enfin sur le bon chemin au Burundi!, http://www.ubj-burundi.org/la-loi-sur-la-presse-enfin-sur-le-bon-chemin-au-burundi/

[26] Burundi Journalists Association Case Comes Up For Hearing, http://eacj.org/?p=2722

Meanwhile, in November 2013, government begun drafting a Cyber Security Law. However, this process was halted as the required budget was yet to be granted.[27]

Other Relevant Laws

Articles 31 and 32 of the Burundi's 2005 constitution guarantee freedom of expression, opinion and assembly.[28] There is no mention of online freedom of expression. The country does not have a freedom of information law.

The 2013 Press Law prohibits the dissemination of information (whether in print, broadcast or digital) that undermines national security, incites civil disobedience and serves as propaganda for enemies or insults the country's president. Article 29 of the Press Law requires the owners of online publications and news agencies to disclose certain information, such as the first edition of the publication, full identity and address of the director of the publication, the editor's criminal record, and full address of the web host to the National Communications Council (CNC).

The Law No. 1/10 of April 3, 2013 on the reform of the Code of Criminal Procedure elaborates on the conditions under which lawful intrusion into personal communication can be done.[29] It states that the Public Prosecutor has the right to seize telegrams, letters and objects of any kind, if they appear to be essential to establishing the truth during a criminal investigation. Whereas this text does not include internet-based communications, phone calls or SMS, there is scope for these to be seized under the vague statement "objects of any kind if they appear to be essential to the manifestation of truth."

Article 24 of the 1997 law which governs telecommunications states that a service provider may be required to provide confidential information on demand if that demand is proven to be lawful according to the constitution of the regulatory authority (ARCT).

27 OpenNet Africa interview with ARTCT official, May 2015

28 The Constitution of Burundi, http://www.assemblee.bi/Constitution-de-la-Republique-du

29 Burundi Code of Criminal Procedure, http://www.assemblee.bi/IMG/pdf/n%C2%B01_10_2013.pdf

3.2 Kenya

ICT Access

There are 29.6 million internet users in Kenya, representing a 69% penetration rate, while mobile penetration stands at 84%.[30] The growth of ICT access in Kenya has been attributed to massive investments in infrastructure by telecommunications service providers as well as aggressive promotions to entice users. In 2014, the Kenya government launched The National Optic Fiber Backbone which has now connected 57 towns in 35 counties.[31]

According to the July 2015 sector updates by the Communications Authority of Kenya (CAK), the amount of international internet bandwidth available in the country grew to 1.6Gbps. The used bandwidth increased by 57% to 783,761 mbps.[32] The mobile phone and 3G modems continue to dominate in provision of connectivity. However, distribution of the 3G network is still low outside the major towns of Nairobi, Kisumu, and Mombasa. Disruptions have been experienced when the undersea fibre optic cables were cut.[33]

There are around 15,000 registered blogs in Kenya with about 3,000 being active.[34] The most popular platforms for blogging are Wordpress, Blogspot and blogger.

Governance Landscape

In 2010, Kenya adopted a new Constitution that offers citizens broader freedom, reduces the powers of the president, devolves government, and raises transparency in government operations. However, the government of President Uhuru Kenyatta has in the past year taken a number of actions and introduced regressive laws that have undermined citizens' civil liberties as provided for in the Constitution.

The restrictive laws have been justified by a need to fight the Al Shabaab militia that have made several fatal attacks in Kenya since the country's troops deployed in neighbouring Somalia in 2011. Meanwhile, the arraignment of social media users has mostly been justified by a need to stamp out the kind of hate speech that fuelled the 2007-2008 post-election violence that left more than 1,000 people dead, but some say it is only critics of the Kenyatta government who fall foul of the law. According to the Committee to Protect Journalists, Kenyan journalists are often at risk when they cover sensitive issues such as terrorism, cases of the International Criminal Court, (ICC) and corruption.[35]

Legal Developments

In December 2014, President Kenyatta signed into law The Security Laws (Amendment) Act 2014 amidst protests from human rights defenders. The law allows admissibility in court of electronic messages and digital material regardless of whether they are not in their original form. The law also contains unclear procedural safeguards especially in the interception of communications by "National Security Organs" for the purposes of detecting or disrupting acts of terrorism. Part V of the Act regarding "special operations" raised particular concerns, as it expanded the surveillance capabilities of the Kenyan intelligence and law enforcement agencies without sufficient procedural safeguards.[36] It gave broad powers to the Director General of the National Intelligence Service to authorise any officer of the Service to monitor communications, "obtain any information, material, record, document or thing" and "to take all necessary action, within the law, to preserve national security."

The government had sought to give the Director General of the National Intelligence Service or his representatives powers to intercept and monitor communications without acquiring a court warrant but this was dropped following a public outcry. Aggrieved civil society groups petitioned the constitutional court, which declared certain sections of the law unconstitutional[37], but left those relating to interception of communications intact.[38] The Government justified the amendments to the security law, arguing that the country was at war with Somalia's Al Shabaab militia and needed decisive measures to fight terrorism.[39]

[30] Communications Authority Statistical Report, Financial year 2014/2015

[31] National Optic Fibre Backbone of Kenya http://www.icta.go.ke/national-optic-fibre-backbone-nofbi/

[32] Communications authority Q3 report year 2014/2015 http://www.ca.go.ke/images/downloads/STATISTICS/%20Sector%20Statistics%20Q3%202014-2015.pdf

[33] Business Daily, Seacom cable cut disrupts internet links.http://www.businessdailyafrica.com/Corporate-News/Seacom-cable-cuts-disrupt-telcos-internet-link

[34] State of Blogging and Social Media Report in Kenya report 2015 BAKE

[35] Community to Protect Journalists (CPJ), Kenya Falls Short on Promises for Press Freedom, https://cpj.org/2015/07/kenya-falls-short-on-promises-for-press-freedom.php

[36] CIPESA, Is Kenya Putting the Chill on Internet freedom?, http://www.cipesa.org/2015/03/is-kenya-putting-the-chill-on-internet-freedom/#more-2444

[37] Peter Kagwanja, Ruling on anti-terrorism law a triumph for Kenya's Judiciary,

http://www.nation.co.ke/oped/Opinion/Security-Laws-High-Court-Ruling-Terrorism/-/440808/2638706/-/105k8hf/-/index.html

[38] Kenya: High Court ruling on security amendment act a victory for free speech,

https://www.article19.org/resources.php/resource/37866/en/kenya:-high-court-ruling-on-security-amendment-act-a-victory-for-free-speech

[39] What the NGOs are not telling Kenyans; http://www.the-star.co.ke/news/what-ngos-are-not-telling-kenyans

In September 2015, civil society in Kenya also lodged a major lobby against government attempts to amend the Public Benefits Organisation Act (2012), which would limit foreign funding to civil society organisations to no more than 15%, and set up a central government-controlled account for funds received from overseas.[40] They would also require all CSOs to register afresh, which raised fears that organisations that were not in the good books of the Government would be locked out.[41]

Other Relevant Laws

The Constitution of Kenya of 2010 contains provisions on fundamental human rights and freedom in Chapter 4 of the Bill of Rights. They include the right to privacy; protection against infringement of an individual's communication; to access to information; to consumer protection; to fair administrative action; to access to justice and fair hearing; to freedom of conscience; religion and opinion; to freedom of expression; and to freedom of media.

However Article 24 of the Constitution, provides limitations on fundamental rights and freedom, stating that they may be limited "by law to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, and taking into account all relevant factors."

Section 29 of the Kenya Information and Communication Act 2013 [42] provides that a person is punishable on conviction to a fine not exceeding 50,000 Kenya shillings (US$ 470), or to imprisonment for a term not exceeding three months, or to both specifically for sending grossly offensive or indecent messages through a licensed telecommunication system.

Under Section 36 of The National Intelligence Service Act of 2012, the Director General of the National Intelligence Service is allowed to monitor or otherwise interfere with the privacy of a person's communications. Similarly, the prevention of Terrorism Act of 2012, Section 36 (1) and 36 (2) allows a police officer (subject to consent from the Inspector-General or the Director of Public Prosecutions) to apply for an interception of communications order.

[40] *KHRC's Response to the Deregistration of Charities by the National NGO Board; http://www.khrc.or.ke/media-centre/press-releases.html*

[41] *Ally Jamah, 'State keen on crippling civil society', http://www.standardmedia.co.ke/article/2000174284/state-keen-on-crippling-civil-society*

[42] *Kenya Information and Communication Act 2013,*

http://www.ca.go.ke/images/downloads/sector_legislation/Kenya%20Information%20and%20Communication%20Amendment%20Act%202013.pdf

3.3 Rwanda

ICT Access

As of June 2015, there were 3.5 million internet users in Rwanda. Mobile telephone subscriptions stood at 74% in July 2015.[44] The Rwanda Universal Access Fund (UAF)[45] financed by a 2% contribution from the annual turnover of licensed telecommunications operators aims to accelerate the use of ICT. Initiatives under UAF include, provision of internet connectivity to all districts, and to telecentres, public and private universities, secondary schools, police sites, army sites, and immigration border posts.

In November 2014, Rwanda rolled out the Fourth Generation (4G) broadband network in partnership with a South Korean telecom company, Korea Telecom.[46] The high-speed wireless broadband technology builds on more than 3,000 kilometres of fiber optic cable that is rolled out countrywide. The 2015 Alliance for Affordable Internet (A4AI) report, ranked Rwanda as the top developing country with the most affordable internet.[47]

To increase access to the internet, in March, 2015, the Ministry of Youth and ICT, Kigali City Public Transport Operators and Olleh Rwanda Networks spearheaded the Smart Kigali initiative to provide free wireless internet on public transport.[48] Kigali Bus Services, Royal Express and Rwanda Federation of Transport Cooperative are some of the buses that as of August 2015 have wireless internet access available to passengers.

Governance Landscape

In July 2015, the Rwanda Senate approved amendments to Article 101 of the Rwanda Constitution[49] to allow for the removal of presidential term limits.[50] This paved the way for incumbent president Paul Kagame to run for a third term in office in the next presidential elections sheduled for 2017. The amendments have drawn wide support from the president's supporters who credit him for restoring peace and unity in the country since the 1994 genocide.[51]

However, members of the opposition, particularly the Democratic Green Party, strongly disagreed and opposed the term limit amendments to the constitution, calling them undemocratic and likely to cause insecurity in the country.[52] These new amendments to the constitution are likely to further curtail opposition participation in democratic processes in the country as the current government has in the past been critised for cracking down voices seen critical of it.

Legal Developments

In March 2015, Rwanda approved the National Cyber Security Policy aimed at safeguarding public and private infrastructure, personal information of web users, financial/banking information as well as sovereign data from cyber-attacks.[53] The policy was developed in consultation with stakeholders through the Ministry of ICT.

Consequently, the Rwanda National Police has set up a Cybercrime and Digital Forensics unit, which provides anti-cybercrime trainings with the help of Interpol to equip the police with skills to detect and investigate cybercrime, understand cyber terrorism, principles of evidence collection for cybercrime, electronic money transfer technology, and basic ICT tools in analysing cybercrime evidence.

In April 2015, the ICT ministry launched the "Stay Safe Online" campaign aimed at raising public and organisational awareness on the current cyber security threats and ways of preventing them.

[43] Rwanda Utilities Regulatory Authority, Statistics and Tariff Information in Telecom Sector as of June 2015, http://www.rura.rw/fileadmin/docs/Statistics_report_2nd_quarter___2015_to_publish.pdf

[44] Active Mobile Telephone Subscriptions as of July 2015, http://www.rura.rw/fileadmin/docs/Monthly_telecom_subscribers_of_July_2015.pdf

[45] Universal Access Fund, http://www.rura.rw/index.php?id=7

[46] Olleh Rwanda Networks, http://www.orn.rw/index.php?id=2

[47] Alliance for Affordable Internet (2014), Affordability: A Global Picture, http://a4ai.org/affordability-report/report/#affordability_a_global_picture.

[48] Mwai. C. (2015) New joint initiative rolled out to increase Internet adoption, The New Times Rwanda, March 07, 2015, http://www.newtimes.co.rw/section/article/2015-03-07/186664/

[49] The Constitution of the Republic of Rwanda, Article 101, "The President of the Republic is elected for a term of seven years renewable only once. Under no circumstances shall a person hold the office of President of Republic for more than two terms, http://www.rwandahope.com/constitution.pdf

[50] Steven Baguma (2015), Rwandan parliament votes to amend constitution, okays Kagame's third term bid, The Afrika reportor, July 15, 2015, http://www.afrikareporter.com/rwandan-parliament-votes-to-amend-constitution-okays-kagames-third-term-bid/

[51] Hundreds throng Parliament as term limits debate gets underway, The New Times, July 14, 2015, http://www.newtimes.co.rw/section/article/2015-07-14/190606/

[52] Morgan Winsor, Paul Kagame Third Term In Rwanda? Supreme Court To Hear Opposition Case Challenging Constitutional Amendment, International Business Times, September 09, 2015, http://www.ibtimes.com/paul-kagame-third-term-rwanda-supreme-court-hear-opposition-case-challenging-2089617

[53] Cabinet Approves CyberSecurity Policy, The NewTimes, March 22 2015 http://www.newtimes.co.rw/section/article/2015-03-22/187138/

Other Relevant Laws

Articles 33 and 34 of Rwanda's Constitution guarantee citizens' free speech and access to information. The country's 2013 Media Law further extends these rights to the media including through online platforms as provided for under Article 19.

Article 54 of the 2001 Law Governing Telecommunications[54] recognises privacy and data protection, and forbids interception of communications. However, restrictions apply if a court has authorised the interception or recording of communications in the interests of national security and the prevention, investigation, detection and prosecution of criminal offences.

Amendments made to the 2008 Law relating to the interception of communications in 2013 allow national security services to apply for an interception warrant to monitor citizens' voice and data communications on grounds of national security.[55] Whereas Article 12 of the law provides for the appointment of "inspectors" to ensure that authorised interceptions are enforced in accordance with the law, the independence of these inspectors may be called into question given that they are appointed by the president.

The 2008 law on Genocide Ideology prescribes heavy prison sentences and fines for any offender who disseminates genocide ideology described as "aggregate of thoughts characterised by conduct, speeches, documents and other acts" aimed at inciting others in public.[56] The law has been criticised for failure to uphold freedom of expression.[57] Since 2013, government has introduced amendments to the law to include less ambiguous definition of offenses, a requirement to prove criminal intent of a suspect, and a lesser prison term.[58]

[54] *Law No. 44/2001 of 30/11/2001 Governing Telecommunications, http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf*

[55] *Law No.60/2013 Regulating the Interception of Communications, http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf*

[56] *Genocide ideology according to this law is described as "aggregate of thoughts characterised by conduct, speeches, documents and other acts" aimed at inciting others in public. See: - Law N°18/2008 Relating to the Punishment of the Crime of Genocide Ideology, http://www.refworld.org/docid/4acc9a4e2.html*

[57] *Amnesty International, Restrictions on Freedom of Expression in Rwanda, http://www.amnesty.org/en/library/asset/AFR47/002/2011/en/ef7cd1a3-d1db-46da-b569-818b7555b83b/afr470022011en.pdf*

[58] *Senate Approve Genocide Law, http://www.africareview.com/News/Rwandan-senate-approves-amended-anti-genocide-law/-/979180/1932950/-/ddevp9z/-/index.html*

3.4. Tanzania

ICT Access

The government of Tanzania is working towards building nationwide high-speed data connections through construction of optical fibre cable all over the country. This, coupled with increasingly affordable smart phones, has enabled internet use to increase at a fast rate. Internet penetration rose from 3.5 million users in 2008 to 11.3 million users in 2014. There are 34 million fixed and mobile telephone subscriptions for the country's population of 49 million which represents a teledensity of 71%.[59]

Governance Landscape

Tanzania failed to complete the constitution review exercise ahead of the October 2015 elections.[60] The draft constitution proposed to raise the breadth of rights and broadened the definition of the right to freedom of expression. Impasse over division of powers between mainland Tanzania and the semi-autonomous Zanzibar Island was a primary cause of the deadlock. The October 2015 polls will thus be held under the old constitution.

President Jakaya Kikwete's ruling Chama Cha Mapinduzi (CCM) faces a formidable challenge from its former senior party member and the country's ex-Prime Minister Edward Lowassa. The CCM is Africa's longest-ruling party and has not taken the challenge lightly. Some say restrictive laws and regulations introduced in the run-up to the elections were aimed to stifle dissent and media freedom.

Legal Developments

During 2015, Tanzania enacted laws that shrink civic space, thwart online freedom of expression, and restrict the role of independent media in advancing greater transparency and access to information. The country passed the Cybercrimes Act 2015[61] and the Statistics Act 2015[62], and it attempted to rush through parliament the Media Services Bill and the Right to Information Bill without allowing any inputs from citizens.

The Cybercrime Act 2015 was reportedly passed in the middle of the night[63] and has been criticised for disregarding freedom of expression, granting excessive powers to the police, and affording limited protections to ordinary citizens.[64] It imposes fines and at least one year of jail time for sending unsolicited messages via computer, and prohibits publication of false, deceptive, misleading or inaccurate information. Furthermore, it penalises citizens who receive unauthorised computer data, regardless of whether content is received with intent or not. On the upside, this law imposes heavy penalties for cyber bullying. It also proscribes production and dissemination of racist or xenophobic material and publication of material that incites or justifies genocide or crimes against humanity.

The stated objective of this law was to fight rising incidents of cyber crime. Bank fraud, mobile money theft, phishing attacks, website hacking and spoofing attacks are reportedly the common security threats in the country.[65] However, critics have suggested that the timing and content of the laws were intended "to control the media" ahead of the October 2015 elections. As stated by one activist: "We usually use various internet platforms to communicate our information—Twitter, Facebook, blogs, SMS, WhatsApp, etc. The use of all these forms will be rendered useless by the Act which in part criminalises transmission of any information deemed misleading, defamatory, false or inaccurate by the government." [66]

The Statistics Act 2015 has been criticised for slapping a minimum fine of Tanzanian Shillings (TZS) 10 million (US$ 4,664) or imprisonment of up to a year, or both, on any communication media that publishes false or misleading statistical information. Human rights groups slammed the law for purportedly making it illegal for anyone to publish or communicate statistics that are unauthorised by the National Bureau of Statistics (NBS).[67] The NBS defends the law,

[59] *Tanzania Communications Regulatory Authority (TCRA) Quarterly Statistics Reports, June 2015, https://www.tcra.go.tz/images/documents/telecommunication/telcomStatsJune15.pdf*

[60] *Sylivester Domasa, TZ civil society concerned gov't is mum on proposed new constitution, http://www.afrikareporter.com/tz-civil-society-concerned-govt-is-mum-on-proposed-new-constitution/*

[61] *Tanzania Cybercrime Bill Should Safeguard Citizens' Rights on the Internet, http://www.cipesa.org/2015/04/tanzania-cyber-crime-bill-should-safeguard-citizens-rights-on-the-internet/*

[62] *The Statistics Act, 2013, http://www.parliament.go.tz/assets/uploads/files/64318-A-BILL--STATISTICS-ACT--2013.pdf*

[63] *Karen Attiah, The U.S. needs to stop ignoring Tanzania's media crackdowns, http://www.washingtonpost.com/blogs/post-partisan/wp/2015/05/15/the-u-s-needs-to-stop-ignoring-tanzanias-media-crackdowns/*

[64] *Tanzania Cybercrime Bill Should Safeguard Citizens' Rights on the Internet, http://www.cipesa.org/2015/04/tanzania-cyber-crime-bill-should-safeguard-citizens-rights-on-the-internet/*

[65] *Kirsten Doyle, Cyber security laws not enough, ITWeb, http://www.itweb.co.za/index.php?option=com_content&view=article&id=143067*

[66] *In Tanzania, Activists Worry a New Law Will Land Them in Jail for Spam, http://motherboard.vice.com/read/in-tanzania-activists-worry-a-new-law-will-land-them-in-jail-for-spam?utm_source=mbtwitter*

[67] *Statistics Act, Cybercrime law unconstitutional - rights group, http://www.ippmedia.com/frontend/?l=7894*

stating that it does not prohibit any person or agency such as research institutions, NGOs, and development agencies from producing and publishing their own statistics.[68] The bill was stringently opposed by opposition politicians and civil society actors who argued that introducing the law was a "desperate and calculated move by a draconian government keen on stamping out dissent and alternative views." [69]

In 2015, Tanzania introduced the draft Access to Information Bill, nine years after the bill was initially published. The draft introduced in early 2015 was criticised for lacking detail in the procedures for requesting information and lodging appeals against decisions on information requests.[70] It imposes a 15-year prison term on any person who discloses exempt information withheld by the public authority. The bill has been praised, however, for its fairly broad scope, fairly narrow regime of exceptions and for handing an oversight role to the independent Commission for Human Rights and Good Governance (CHRAGG).

Government also attempted to pass The Media Services Bill 2015 but shelved it following civil society protests about the lack of citizens' inputs and some restrictive clauses. Proposals criticised including professional fees, annual licencing, hefty fines for offenses, and a heavy government influence in choosing members of media regulatory boards.

The Broadcasting Services (Content) (The Political Party Elections Broadcasts) Code 2015 was gazetted in June 2015 to regulate the elections of October the same year. Section 10 of the 2015 code deals with "online content providers", defined as "any person or entity who develops files of content for the online users or on behalf of others to be made accessible online." It stipulates requirements for online content providers "residing within or outside Tanzania territory" who create "content intended for Tanzania mainland using Swahili or any other languages which have large audiences." These content providers have to register with the Tanzania Communications Regulatory Authority (TCRA); comply with Tanzania's laws and regulations governing the operations of electronic media; and ensure that information provided in blogs is accurate, fair, factual, and balanced to all parties and independent candidates in the elections.[71]

The rules also require online content providers to edit interactive discussions likely to hurt the feeling of any person, as well as offensive or blasphemous language that may provoke violence, sedition, or breach of peace. They are also required to screen information and reports before posting, to "take care to ensure the accuracy on publishing election results or public opinion polls" and to adhere to the bloggers' code of conduct. Section 14 states that should a broadcaster wish to use results from SMS opinion polls, they have to indicate the number of respondents and to provide select representative responses. Where the SMS poll has less than 1,000 respondents, broadcasters shall inform the audience that it is not scientific and the conclusions are not valid and reliable.

In February 2015, Tanzania enacted the Electronic Transaction Act.[72] Communications minister Makame Mbarawa, defended this law and the Cybercrimes Act, both of which took effect on September 1. "There is a perception that the laws have been introduced to weaken people's freedom of opinion and expression, but they are aimed at protecting the people" from computer and cyber crimes.[73]

Other Relevant Laws

Tanzania has various laws that cater for lawful interception of communications. The most explicit is the Prevention of Terrorism Act, which states in Section 31 that subject to a police officer obtaining prior written consent from the Attorney-General, he may apply to court for an interception of communications order for the purposes of obtaining evidence of the commission of an offence of terrorism. The Court may make an order requiring a communications service provider to intercept and retain specified communications or it may authorise the police officer to enter any premises and to install any device for the interception and retention of communications.

68 NBS, Statement of clarification on misconception of Statistics Act 2015, http://www.nbs.go.tz/nbs/takwimu/ACT/Misconception%20of%20Statistics%20Act%202015.pdf

69 Tanzania passes draconian Bill that could hit publishers hard,

http://www.africareview.com/News/Tanzania-passes-draconian-bill-that-could-hit-publishers-hard/-/979180/2667704/-/ds2wocz/-/index.html

70 Tanzania: Analysis of Right to Information Bill, http://www.law-democracy.org/live/tanzania-analysis-of-right-to-information-bill/

71 CIPESA, Tough New Election Reporting Rules for Tanzania's Bloggers, http://www.cipesa.org/2015/08/tough-new-election-reporting-rules-for-tanzanias-bloggers/

72 Electronic Transactions Act, http://parliament.go.tz/polis/PAMS/docs/1-2015-6.pdf

73 Ludovick Kazoka, Tanzania: Govt Allays Fears As Cyber Act Takes Effect, http://allafrica.com/stories/201509011213.html

The Electronic and Postal Communication Act, 2010 (EPOCA) also provides for making an application under “any other law” to the director of public prosecution for authorisation to intercept or listen to any customer communication. The Tanzania Intelligence and Security Service Act of 2002 and the Criminal Procedure Act 2002 are also relevant to interception of communication because of the powers they give security agencies to collect intelligence and investigate crimes.

Vodafone, a major operator in Tanzania, notes that while the EPOCA and its regulations can also be used for blocking URLs, IP addresses and performing services shutdown, this law does not provide for judicial review of the TCRA’s use of its power. It is not clear, however, whether Tanzania undertakes interception of communications. For its part, Vodafone stated that it has not implemented the technical requirements necessary to enable lawful interception and therefore did not receive any agency or authority demands for lawful interception assistance during 2014.[74]

Tanzania also maintains some archaic laws such as the Newspaper Act of 1976, which gives authorities the power to “exclude” any newspaper from operation in the “interest of the public.” In 2013, government used this law to bar Mwananchi - the country's largest selling newspaper - from publishing on its website for 14 days after accusing the paper of publishing confidential government information and inciting Muslims.[75]

[74] Vodafone Law Enforcement Disclosure Report, Legal Annex, June 2014,

http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf

[75] Government now bans ‘Mwananchi’ website, http://www.opennetafrica.org/government-now-bans-mwananchi-website/

3.5 Uganda

ICT Access

There are 11.9 million internet users in Uganda, implying a 34% penetration rate. Telephone penetration stands at 62%.[76] The entry of Vodafone into the sector in the first half of 2015 brought the total number of voice operators to seven. [77] The others include Airtel, Africell (formerly Orange), Uganda Telecom, MTN, Smart Telecom and K2 Mobile. Africell completed acquisition of Orange in November 2014.[78] Also, in November 2014, Liquid announced take over of Infocom, an ISP.[79]

Through the national broadband initiative, government has laid a total of 1,400 kms of fibre optic cable connecting major towns and government agencies.[80] As a landlocked country, Uganda's major service providers are connected to high-speed submarine cables landing at the East African coast through Kenya and Tanzania.

The Rural Communications Development Fund (RCDF) implemented by the Uganda Communications Commission (UCC) and funded by a 2% levy on licensed telecommunications operators' revenue, was established in 2003. It has since seen the establishment of numerous internet points of presence (POPs), internet cafes and ICT training centres, and the establishment of 1,000 ICT labs in schools and training of over 18,750 rural people, 691 teachers and 486 head teachers in use of ICT.[81]

Governance Landscape

Uganda has 29 registered political parties and to date three general elections have been held since the reintroduction of mulitparty politics. The next elections are sheduled for February 2016 with President Yoweri Museveni who has been in power for 29 years among the contestants. Uganda is also regularly criticised by human rights organisations for clamping on media freedom, witch-hunting the LGBTI community, and silencing critical civil society.[82]

On June 17, 2015, political tensions mounted when Amama Mbabazi, Uganda's former Prime Minister and secretary general of the ruling party, took to Youtube to officially announce his intention to run in the 2016 presidential elections.[83] In a rebuttal video to Mbabazi's announcement, Museveni linked Mbabazi aides to the WhatsApp audio recordings whose authors he had asked the police to arrest and to other "false" documents circulating on social media, which he said were tarnishing his government's image and inciting ethnic tensions.[84]

Legal Developments

In 2015, Uganda proposed the Non-Governmental Organisations (NGO) Bill to replace the existing Act from 2006. The bill was drafted in response to the "rapid growth of Non-Governmental Organisations" which had led "to subversive methods of work and activities, which in turn undermine accountability and transparency in the sector." Under the proposed law, NGOs will have to declare their sources of income and obtain permits from local authorities to operate. Furthermore the NGO Board will be able to revoke permits if NGOs contravene their constitutions or the bill, or if "in the opinion of the board it is in the public interest to do so".[85]

The Bill includes the requirement to indicate where exactly activities will be carried out in order to receive a permit as stipulated in Section 31 (5)(3), a concern as the use of crowdsourcing and social media tools are increasingly becoming core to the work of many NGOs.

[76] *Post, Broadcasting and Telecommunications Market and Industry Report, January – March 2015, http://ucc.co.ug/files/downloads/Q1-Market%20Report%202015.pdf*

[77] *BiztechAfrica, Vodafone seeks a share of saturated Ugandan market http://www.biztechafrica.com/article/vodafone-seeks-share-saturated-ugandan-market/9684/#.VgO_bxGqqko*

[78] *PR News Wire, Africell Completes Acquisition of Orange Uganda, Reaches 11 Million Active Subscribers, http://www.prnewswire.com/news-releases/africell-completes-acquisition-of-orange-uganda-reaches-11-million-active-subscribers-282900521.html*

[79] *New Vision, Liquid Telecom completes Infocom takeover, http://www.newvision.co.ug/news/661445-liquid-telecom-completes-infocom-takeover.html*

[80] *"NBI/EGI Project," National Information Technology Authority – Uganda, accessed March 16, 2015, http://www.nita.go.ug/projects/nbiegi-project.*

[81] *RCDF Annual Report 2013/2014, http://ucc.co.ug/files/downloads/RCDF%20Annual%20Report%20201314%20Abridged.pdfhttp://www.ucc.co.ug/files/downloads/RCDF%20Annual%20report%2012-13%20abridged.pdf*

[82] *CIPESA, 2014; Hurting Down Social Media Abusers in Uganda as Elections Near, http://www.cipesa.org/2015/07/hunting-down-social-media-abusers-in-uganda-as-elections-near/*

[83] *Amama Mbabazi, My Declaration, https://www.youtube.com/embed/fN-T4Ud91IA?fs=1&width=640&height=480&hl=en_US1&rel=0&iframe=true*

[84] *Museveni reacts to Mbabazi's 2016 Presidential bid , https://www.youtube.com/watch?v=Yf7FnT2BYXg*

[85] *Uganda: NGO Bill Aims to Muzzle Civil Society, Say Activists, http://www.theguardian.com/global-development/2015/jun/24/uganda-ngo-bill-aims-muzzle-civil-society-say-activists*

In late 2014, Uganda issued a draft Data Protection and Privacy Bill for public comment.[86] The Bill seeks to protect the privacy of individual and personal data by regulating the collection and processing of personal information. It provides for the rights of persons whose data is collected and the obligations of data collectors and data processors; and regulates the use or disclosure of personal information. However, the bill falls short of its expectations, with numerous clauses undermining privacy.[87] Since the calls for public comment, there has been no evidence of the bill's progression.

Uganda enacted the Access to Information Act in 2005, becoming one of the first African countries to have such a law. The Act, however, remained unimplemented until 2011 when the enabling regulations were enacted. To-date, proactive disclosure and citizens' requests for public-held information remain low.[88]

In a landmark case, on February 6,2015, a Chief Magistrate's Court in Kampala ruled that the reasons for which information is requested or the belief about how it will be used "are irrelevant considerations" in determining government's approval or denial of a request. The ruling came after the Hub for Investigative Media was denied access to information related to activities of the National Forestry Authority funded by the World Bank between 2009 and 2011. The landmark ruling set a precedent that could make it easier for journalists and citizens to exercise the right to information.[89]

Other Relevant Laws

The Regulation of Interception of Communications Act 2010 allows for the interception of communications. The law gives the ICT minister the powers to set up a monitoring centre which maintains connections with telecommunication systems. To-date, however, there is no evidence that such a centre exists. Additionally, the Anti-Terrorism 2002 which gives security officers the power to intercept the communications of a person suspected of terrorist activities and to keep suspected persons under surveillance including journalists who "promote terrorism". The scope of the interception and surveillance includes letters and postal packages, telephone calls, faxes, emails and other communications, access to bank accounts, as well as monitoring meetings of any group of persons.

Meanwhile, the Anti-Pornography Act 2014 provides for the prohibition of the production, traffic in, publishing, broadcasting, procuring, importing, exporting and selling or abetting any form of pornography and punishment for those found to be in possession of any pornographic materials. Under section 17 (1), an ISP through whose service pornography is uploaded or downloaded is punishable with a fine of up to UGX 10 million (US$4,000) or five years imprisonment or both. Subsequent conviction of the ISP may lead to the suspension of their operating license.

The Public Order Management Act 2013 and the Anti-Homosexuality Act 2014 (later annulled by the constitutional court) drew criticism from human rights activists locally and internationally due to their severe infringement on privacy, access to information and freedom of expression, association and assembly.

[86] *Uganda Draft Data Protection and Privacy Bill 2014, http://www.nita.go.ug/publication/draft-data-protection-and-privacy-bill*

[87] *CIPESA's Comments on the Draft Data Protection and Privacy Bill, 2014, http://www.cipesa.org/?wpfb_dl=184*

[88] *Using ICT to Promote the Right to Information: Perceptions of Ugandan Citizens and Public Officials, http://www.cipesa.org/2015/03/using-ict-to-promote-the-right-to-information-perceptions-of-ugandan-citizens-and-public-officials/*

[89] *African Centre for Media Excellence (ACME), Ugandan media silence on 'Access to Information' victory a travesty, http://acme-ug.org/2015/02/17/uganda-media-silence-on-access-to-information-victory-a-travesty/*

4. FINDINGS

4.1 Knowledge, Attitudes and Practices on Internet Freedom

This subsection presents findings on the communication practices of the respondents, including the technologies they used, as well as their knowledge of internet freedom.

Commonly Used Communication Technologies

Study findings show that the most frequently used communication technology means was voice over mobile and landline with 77% of respondents indicating using it daily. Mobile short message service (SMS) came in second with 69% of respondents using it daily. None of the respondents indicated never using SMS. Email, and the instant messaging application WhatsApp, were used daily by 64% and 57% of respondents, respectively. About 30% of respondents did not use the social networking platforms Twitter and Google Plus, and a similar percentage did not blog or use Viber.

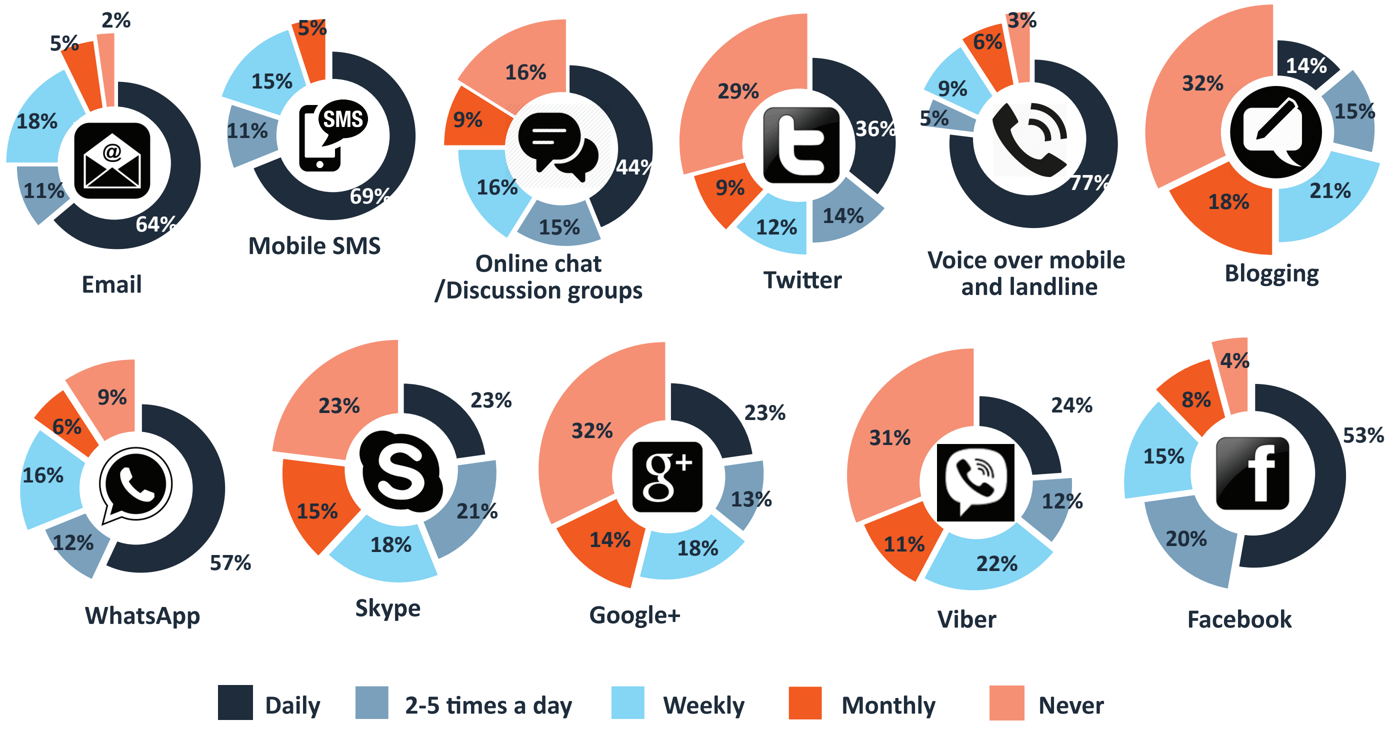

Figure 2: How regularly do you use these communication technologies?

Understanding of Internet Freedom

Across the five countries, there was a fair understanding of the meaning of the term "internet freedom". Although definitions varied in wording, privacy, the right to access affordable and uncensored internet, and freedom to use the internet were the recurrent themes. In Burundi, many respondents associated the term with unrestricted use of the internet for freedom of expression and access to applications and information, with guarantees of privacy and data protection. The quality and reliability of the internet connection, as well as financial affordability, were also noted.

In Kenya, similar responses were received as most of the research participants understood internet freedom as the ability to navigate the internet without limitations such as censorship or surveillance. A few Kenyan respondents said their understanding of internet freedom went hand in hand with responsible use of the internet that upheld human rights and protected national security.

Many Tanzanian respondents provided a description of internet freedom that included aspects of use of the internet free of interference or censorship by the government and telecoms service providers. In Uganda, most respondents understood internet freedom as the ability to use the internet and other digital communication technologies without commercial or state restrictions.

Notable quotes of understanding of internet freedom

Ability to communicate only with wanted partners (no spam, no unwanted advertisement) – Private sector employee
Internet usage without any Government control - Human Rights Defender
Internet use without any censorship and freedom of expression when using social media tools - ISP
Safety of the network, safety of users, i.e. protection of the data and communication content from hackers and any other intrusion or fraud - Journalist
Total privacy while surfing - Human Rights Defender
Internet freedom means the ability to communicate about any topic as a journalist without intrusion by another internet user - Journalist
The ability to operate in cyberspace without threat of invasion, but also respecting other peoples' rights - Government employee
Being able to navigate anywhere and responsibly express myself freely without interjections or harassment - Human Rights Defender
Being allowed to click on any sites, write, create and develop - Human Rights Defender
Usage of internet without infringement of human rights and without violating the affairs of the state - Law enforcement agency
Ability to access information online without limitation regardless of what you are searching for - Journalist.
Freedom to exchange ideas and post content on the internet without infringing on other peoples' rights and without being over-censored - Journalist.
Where your privacy in the social web network is treated confidential and not made available to any third party - ISP/Telecommunications representative
To access and utilise the internet as part of my human rights as stipulated in the constitution of Tanzania of 1977 – Human Rights Defender
Use of the internet as a platform to learn and socialise without restriction except in cases of insults or disrespect – ISP/Telecommunications representative

Knowledge of Privacy and Security in Digital Communications

The level of knowledge of privacy, security and unfettered access in digital communications was low, with only 10% of the respondents indicating having excellent knowledge. Almost an equal number (11%) had no knowledge at all, while 61% of those surveyed had between good and workable knowledge.

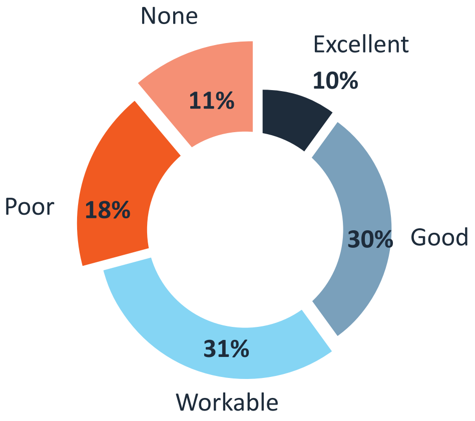

Figure 3: How would you rate your knowledge of privacy, security and unfettered access in digital communications?

In Uganda and Tanzania, none of the respondents indicated having no knowledge at all. In Uganda, those who indicated excellent knowledge (17%) were mainly academics and techies. In Tanzania, those with excellent knowledge (9%) were techies and human rights defenders. None of the Burundi respondents had excellent knowledge although officials working in MDAs were the majority among the 40% who indicated they had a good level of knowledge. In Kenya, of the 20% of respondents who did not have any knowledge, the majority were from the media. In Tanzania, 16% had excellent knowledge, with academics dominating this group. In Burundi, 40% of respondents indicated having working knowledge of privacy and security in digital communications. A good level of knowledge was indicated by 13% of respondents in Burundi, while 4% indicated excellent knowledge and 23% had no knowledge at all.

Privacy and Security Concerns in Communications

The most common uses of communication technologies in which security/privacy could be a concern were indicated as voice and SMS over mobile, email and social media platforms like Facebook and Twitter. Online transactions including trading, banking, shopping and mobile money were indicated as activities where respondents had security concerns. Also, the use of free and unsecured wireless networks (Wi-Fi) was said to increase the vulnerability of users. This indicates that privacy and security concerns were not only associated with perceived government surveillance of communications but also threats from other internet users, hackers and fraudsters.

Some of the research participants in Tanzania indicated having been direct victims of privacy invasion on WhatsApp, Facebook and Twitter, hence they had particular concerns over these platforms. They gave examples of instances where their voice calls were recorded without their knowledge and “used negatively”. In other cases cited, screenshots of private messages were shared with non-intended recipients. The circumstances under which the recordings and screenshots were taken were not political but social relating to friends, acquaintances and family.

One blogger in Uganda said that because bloggers are free to write and publish without fact checking, chances of them using false information and passing it on as the truth can compromise security or tarnish reputations of individuals or corporations.

The "unethical" use of social media platforms particularly WhatsApp and Twitter to promote hate speech and infringe on other people's rights was also cited as a concern. Respondents, particularly in Kenya and Tanzania, noted security concerns when communicating information deemed as “sensitive” via any technology. One Tanzania respondent noted that security concerns were common for any communication involving “negative issues that may trigger violence in the community,” giving the example of messages intended to trigger religious hatred.

Without pointing to any evidence, Burundian respondents had the perception that e-mail and phone calls in the country were “constantly under surveillance.” A respondent from the Burundi Journalist Union suspected that “e-mail messages were monitored by the secret service.” He claimed passwords of email addresses belonging to some of his colleagues had been stolen and changed by officials of the secret service. This respondent failed to provide details of any such case.

Other than in Rwanda, there have been no reported incidents of national security agencies producing private communication records in cases against individuals in the other four countries in this study. The general percepition of surveillance among citizens in all five countries may be caused by mistrust between the government and independent media, opposition, and human rights defenders.

Use of Digital Safety and Security Tools

Most respondents had never used tools and technologies to help protect their privacy or safety online.

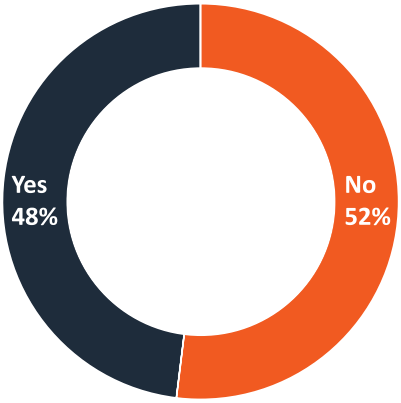

Figure 4: Do you use/have you ever used tools and technologies intended to help protect your privacy and security online?

At country level, the use of tools was lowest in Rwanda and highest in Uganda.

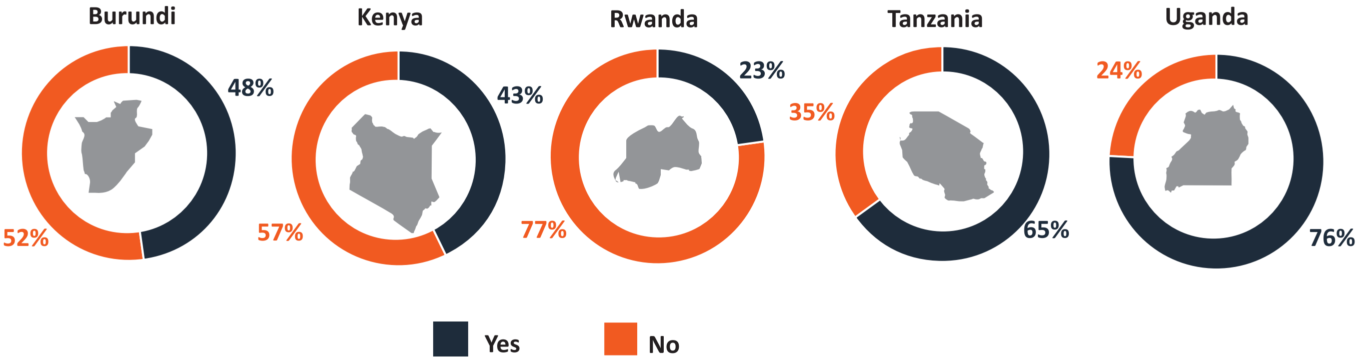

Figure 5: Country analysis of use of tools and technologies intended to protect privacy and security online.

The most common digital security measures included “complex” passwords and pass codes, two-factor authentication, frequently changing passwords, secure calling and messaging, anonymous browsing, firewalls, malware & virus protection, and utilising pre-installed and in-built safety features on platforms and devices such as disabling geo-location and activating privacy settings. Also used were password vaults, anti-theft locks, encryption and virtual private networks (VPN).

"I have put a security code on my phone and disabled posts on my Facebook account from people who are not my friends. They can only send messages. This has worked well for me," said a Kenyan government employee on the security measures taken for their Facebook account. A different respondent from Kenya noted the use of "disposable email" to serve undisclosed specific purposes for information sharing.

Digital safety tools utilised included Pretty Good Privacy (PGP), True caller, Jitsi, Mcafee, Tor, RedPhone, Cyberoam, Hotspot Shield, TextSecure, Wired Equivalent Privacy (WEP), Telegram, KeePassX, and AxCrypt.

In Tanzania, the use of digital safety tools was common among respondents from telecoms service providers, and NGOs. Of those who had never used safety tools in Kenya, half were journalists or human rights defenders and activists. Among the reasons stated for non-use were lack of knowledge and skills, seeing no need for them, because passwords were considered sufficent, and the high cost of acquiring paid-for tools.

In Uganda, reasons for not using the tools included belief by some respondents that they were careful not to compromise their security by not sharing more than they should. Some were just unaware of the security risks online or the tools to protect them. But for one private sector respondent, the lethargic attitude to online safety resulted from a belief that hackers could breach any security system. “I am not really assured that even if I used such technologies, the information will not be hacked especially if government agencies are interested in accessing the information in question,” she said. This was echoed by a respondent in Tanzania who delcared: “I don’t trust any technological tool for my privacy and security online.”

However, even those that were familiar with digital safety tools highlighted that the practice did not come without challenges. “Sometimes I download security apps on my phone... [but] they tend to make the phone slower,” said a human rights activist from Kenya.

Some of the respondents who did not use the tools acknowledged their importance, as several of them felt they needed to secure their digital communications. Others felt secure enough with the existing safety and security measures provided by their institutions hence they saw no need for extra safeguards.

Sources of Digital Security Tools

Those who used the tools sourced them from the internet, some had received prior training on digital security or had been introduced to the tools by colleagues who had benefited from such training. Some received the tools from their employers who needed to safeguard company and employee information or on recommendation of organisations that worked in the area of internet freedom.

In Burundi, human rights defenders indicated that the utilisation of digital safety tools was a requirement by human rights partners and networks that they work with worldwide. In Kenya, one respondent stated that he utilised paid for tools as opposed to open source ones as he considered them "safer." "I get pirated software from the net," stated one respondent. Those with advanced skills indicated using the various online forums on anonymity/privacy for recommendations on tools to utilise.

Perceptions of Government Monitoring and Surveillance

Of the respondents, 61% believed that government agencies monitored and intercepted citizens' communications while 39% disagreed. The belief that government agencies were monitoring communications was highest in Kenya (91%) followed by Tanzania (80%). Over three quarters of respondents in Rwanda thought that their government did not monitor or intercept citizens' communications.

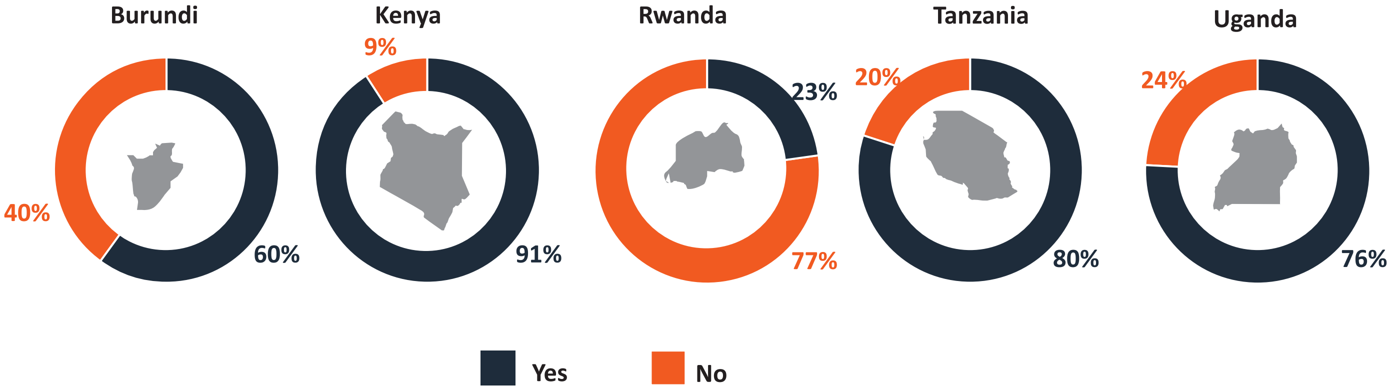

Figure 6: Country analysis of the belief that government agencies are monitoring and intercepting citizens' communications.

Respondents from all countries cited promotion of national security and fighting terrorism as the reasons most used for government monitoring and surveillance of communications. Another reason provided was combating hate speech.

The Kenyan respondents who believed that government agencies were monitoring and intercepting communications cited the personal social media accounts of some of the controversial bloggers such as Robert Alai and Member of Parliament Moses Kuria as the ones monitored most. Respondents believed that activists, journalists, NGOs, opposition leaders, Muslim leaders, suspected criminals and members of militia groups, especially those with "mass followings" and considered "opinion makers" were among the groups whose communications were monitored the most. Others believed that, in efforts to curb hate speech, all communications of "every citizen" online were monitored, in particular those of individuals "known for posting inflammatory messages" and "touching on matters of security". Some bloggers and activists said information tapped from mobile phones to establish their physical location held them back from expressing themselves freely online on some topics.

In terms of the people and organisations whose communications are likely to be monitored in Uganda, respondents mentioned politicians, critical media, NGOs engaged in political work, Ugandans with a significant presence on Facebook and Twitter, civil servants and LGBTI groups.

"The phone tapping [Interception of Communications] law gives Government the right to monitor anyone. I think all our conversations are monitored," said a respondent from the Uganda academia. Without giving specifics, an official from the Uganda Communications Commission stated that the communications of suspected criminals were monitored. "The communications monitored are for security of citizens. This is done world over," he said.

Burundian respondents linked government's snooping to suspected criminals and fraudulent activities as well as to political opponents. A local political opposition leader stated that suspected monitoring of voice communications over UCOM – the state owned telecommunications company - was affecting his party's activities. He added that since most of the leaders of the party at grassroots level were subscribed to UCOM, communicating with them on the alleged monitored network would be revealing strategic information to the ruling party.

Tanzanian politicians, especially opposition leaders, were listed by most of the respondents as the ones whose communications were most likely monitored, followed by media and activists "that fight for freedom of speech and human rights" and "any person who is seen as a threat to the regime." An ISP representative stated that the email communications of all individuals registered under the Tanzania Network Information Centre (TZNIC) – the internet registry for dot tz (.tz) domain names - were monitored.

Technologies and Tactics Used in Monitoring, Surveillance, Filtering and Censorship

State monitoring was believed to be achieved through police orders and directives from telecommunications regulatory authorities and intelligence services to service providers. In Kenya, while the judiciary is increasingly visible in prosecution of internet related crimes, other Government agencies cited by respondents included the National Cohesion and Integration Commission.

However, most of the respondents were not aware of the government tactics and techniques used in information controls or surveillance. Others were convinced there was no government surveillance. Nonetheless, the following were mentioned:

- Monitoring communications through IP address activity and telephone logs
- Geographic Position Systems (GPS) technologies for tracing individuals' movements and locations, particularly made possible by the SIM card registration exercises.
- FinFisher (surveillance software)
- Website blocking
- Password cracking

4.2 Threats to Online Access, Privacy and Security In East Africa

This section presents findings on threats to internet freedom in East Africa, including the likely violators and victims, major causes of privacy and security vulnerabilities, and adequacy of measures in place to mitigate threats to digital rights.

Who is Likely to Violate Citizens' Internet Freedom?

Law enforcement agencies and adversaries such as hackers and fraudsters were perceived by 58% and 55% of respondents respectively as the likeliest violators of internet freedom. Regulators came in next with 48% ranking them most or very likely violators. Those considered least likely to violate the privacy and security of communications were friends, family, spouses and colleagues. These were ranked by 44% of respondents as unlikely or not at all likely to be violators. Journalists were the second least likely violators at 44%.[90]

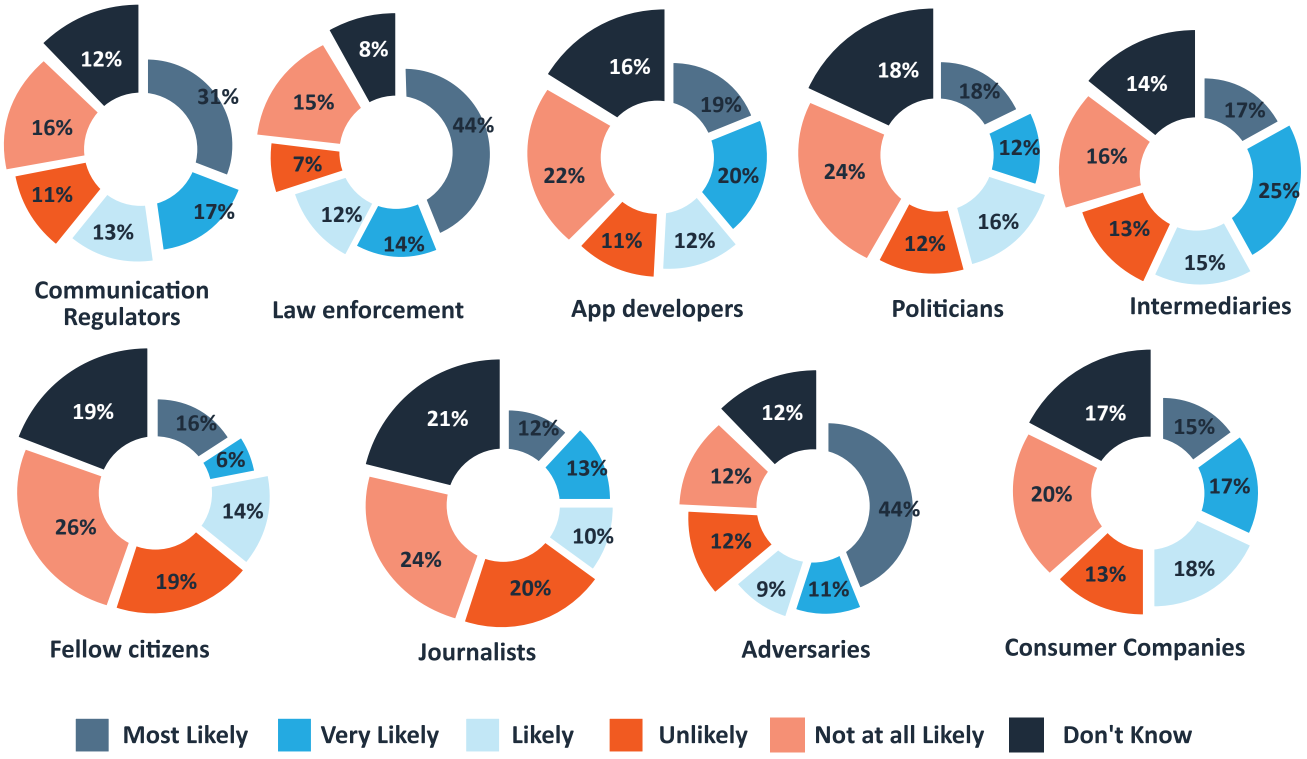

Figure 7: In your country who are the most likely to violate privacy and security of citizens' and organisations' communications?

However, at country level, perceptions of most and least likely violators varied. In Burundi and Tanzania, law enforcement agencies were considered the most likely violators, while in Kenya hackers and fraudsters emerged the most likely violators. Ugandans ranked communications regulators and law enforcement agencies jointly as the top most likely violators. Kenyans and Burundians considered journalists the least likely violators.

For Tanzanians, law enforcement agencies were deemed the likeliest violators, whereas in Rwanda, journalists were considered by majority of respondents as the most likely to violate privacy of communications. Fellow citizens including friends, family, spouses, and colleagues came in second place in Rwanda.

[90] *Data on Rwanda not available*

Major Causes of Privacy and Security Vulnerabilities in East Africa

Respondents were asked to name the major causes of privacy and security vulnerabilities in East Africa, and the following were the major ones mentioned:

1. Corruption and lack of transparency in administration leading to government surveillance practices for fear of an informed citizenry.
2. Lack of professionalism and ethics before sharing information online. Examples cited here included posting graphic pictures of the dead and injured with no consideration of the victims' next of kin. Also, publishing the details of the personal lives of individuals that was "of no importance to the community aside from cyber bullying".
3. Inadequate technical skills and knowledge amongst citizens in securing their communications, leading to exposure of user data to third parties with malicious intent.
4. Low awareness among citizens of communications related laws.
5. Computer Emergency Response Teams (CERTs) in the region were cited as ill equipped and ineffective in dealing with cyber crime. One respondent referred to the CERTs as having "widespread lack of relevant technical knowledge."
6. Weak or non-existent legal and regulatory frameworks to address data protection, privacy and consumer rights.
7. The growing threat of cybercrime such as hackers and online fraud.
8. Emerging threat of terrorism leading to governments justifying surveillance of citizens' communications.
9. Absence of guarantees from telcom and internet service providers for the integrity and confidentiality of subscribers' personal information and communications.

Adequacy of Measures to Protect Citizens From Illegal Monitoring of Communications

On whether there are adequate measures to protect citizens from illegal monitoring in East African countries, 69% of those surveyed said no. Only 31% of those surveyed thought sufficient measures were in place. These made reference to national Constitutions, communications laws and Penal Codes. At country level, the recently enacted Cybercrime Act of 2015 (Tanzania), the draft Data Protection and Privacy Bill 2014 (Uganda), Computer Misuse Act 2011 (Uganda) which allow aggrieved parties to go to court in case their rights and freedom have been infringed were mentioned. Several respondents stated the mandatory registration of all mobile phone users and regulation of mobile operators' use of subscribers' personal information as measures that could help to combat crime.

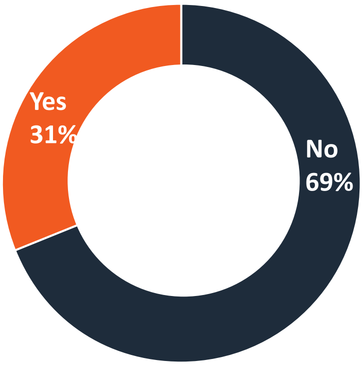

Figure 8: Are there adequate measures to protect citizens in your country from illegal monitoring of communications?

Role of Telecom and Internet Service Providers in Promoting Internet Freedom

There was strong indication among respondents that communications service providers have a role to play in supporting internet freedom, particularly by safeguarding clients' information and not sharing it with third parties. "Telecoms have a big role to play given they are Internet Service Providers who register and host users' data, register domains and as such they have access to all of this information," said one respondent. Others echoed him, noting that telecoms operators need to guarantee the privacy of their clients.

However, many respondents felt that telecom and internet services providers were doing "very little" or nothing to protect the security and privacy of their subscribers.

"We need to see more transparency in how they handle our data," said a human rights defender. Some respondents said service providers were "fully controlled by the government" and were complicit in surveillance of citizens. "Currently I don't see any role played. In most cases the love for profit will compel most telcos to disregard the privacy of their customers whenever it is expedient e.g. a government request for unfettered access to customer data, a merger/takeover or where selling customer data will give them a windfall in revenue," said a techie from Kenya.

A respondent from Burundi detached telecom companies from the role of protecting privacy and ensuring user safety, arguing that "only end users have the responsibility to protect themselves."

But others said telcos and ISPs were doing commendable work, such as by updating their security systems to curb the evolving and rising cases of cyber security. Such respondents said the companies were doing their best to protect subscriber privacy and security but they received requests from regulatory authorities to disclose private information which they were obliged or pressured to comply with.

Respondents recommended that service providers should secure their subscribers' information to guard against privacy breaches, including by employees of the telecom companies. Others stated that service providers should be at the forefront of educating subscribers about digital safety; widely employ encryption policies to protect users' information; and not censor anything on their networks.

A notable number of respondents mentioned that regular release of transparency reports by service providers would highly contribute to the promotion of internet freedom. "They need to publish all government requests for data," said one respondent. Another suggested that service providers should inform their customers about any breach of privacy ordered by governmental agencies. Similarly, they should inform subscribers of incidents of breach of privacy through the intrusion of their systems by hackers or other actors.

4.3 Effect of Information Controls on Communication Behaviour

This sub-section examines how respondents are affected by real or perceived monitoring and what measures they tend to take in view of the risks to their privacy and security in the online sphere.

To Communicate or Not to Communicate Because of Security Risks

The number of respondents who had ever decided not to communicate or not to share information because of a perceived security risk was 49% - almost equal to those who had never at 51%**.**

The decision not to communicate was informed by various reasons and sometimes events across the different countries. In Uganda, a human rights defender working with sexual minorities stated that at the time when the anti-gay law was passed, "I had to withhold information in order not to endanger others." In early 2014, Uganda enacted the Anti-Homosexuality Act that prohibited any forms of sexual relations between persons of the same sex and promotion of homosexual relations. Although the law was subsequently nullified by court, members of the local LGBTI community have reported ongoing malicious attacks on their email and social media accounts, theft of devices and blackmail, among others.[91]

A Ugandan journalist who covers politics reported that his personal email and social media accounts have been hacked into before by Government agents whom he did not name. After the hacking incidents, he said when sourcing on sensitive stories, his communication is mostly done offline.

In Kenya where over 82% of the respondents had ever made decisions not to communicate or share information online because of perceived security risks, the majority were journalists and human rights defenders. One Kenyan activist stated that his decision not to communicate was because he suspected his online accounts had been hacked but he could not say by whom. A respondent from the NGO community noted that communication records such as SMS and chat were "being watched" by government and "could be used as evidence against you."

Fear of unsolicited email and SMS was cited by respondents in most countries as a reason for not sharing information particularly on social media. Further, the fear of personal information being used against the owner was also cited as a concern. A Ugandan apps developer who was fearful of revenge pornography stated: "I don't share personal pictures on social media and WhatsApp because they can be abused." His Kenyan counterparts had the same perceptions with one stating that he did not share personal photos of himself or members of his family for "fear of potential abuse." Another developer said that he used his discretion before communicating any sensitive information. "I deploy Pretty Good Privacy (PGP) [an encryption software] whenever the need arises."

Respondents who had never decided not to communicate due to a perceived security risk, felt confident that they could secure their communications. Others did not feel the need to secure their communications while others did not feel insecure online. "My entire existence is dependent on the internet. When my data runs out it's worse than when there is a power cut so I cannot think of not using the internet, communicating online or sharing things online."

How Access to Safety Tools Would Affect Individuals' Communication Practices

Respondents were asked how their communication behaviour would be affected if they were provided with anonymisation and circumvention tools. There were mixed reactions on whether providing such tools to citizens would be wise, and whether it would change the communication practices of recipients. One academic stated that it would "be a source of motivation for bad behaviour because no one is monitoring you." An activist concurred, stating that provision of the tools "would promote crime due to a lack of traceability [of perpetrators]." Another respondent pointed out that anonymisation tools "would make people act irresponsibly on the net" and another declared that "anonymity may breed criminals."

For others, provision of these tools would make them to easily and boldly communicate sensitive information, create a feeling of increased freedom, including to write or comment on controversial topics. A Kenyan journalist said if she has such tools, she would communicate more freely on corruption and become motivated to unearth government secrets. A Burundian counterpart shared a similar position, stating, "I would feel more comfortable and be prompt in publishing news."

The tools were also considered valuable in countering cyber stalking and minimising fears of insecurity when browsing online. However, some stated that provision of circumvention and anonymisation tools "would not change anything" about their communication habits.

[91] Gay Ugandans face new threat from anti-homosexuality law http://www.theguardian.com/world/2015/jan/06/-sp-gay-ugandans-face-new-threat-from-anti-homosexuality-law

5. INCIDENTS OF VIOLATIONS OF INTERNET FREEDOM (May 2014 to August 2015)

5.1 Government Disclosure Requests

There is limited information on requests made by governments to intermediaries such as telecom companies and ISPs. This is because most intermediaries do not publish this data as it might jeopardise their operations. However, there are some exceptions, but all of them are multinationals.

In the period July to December 2014, the Kenyan government made five requests to Google for user information disclosure, four of which were through a court order or other legal process and one was described as "an emergency."[92] Google did not comply with the requests nor did it provide further details on the grounds for the requests. In 2014, Kenya made an account information request to Twitter, and another in 2015. Both requests were denied. A request by Kenya for removal of content from a Twitter account in 2014 was also declined.[93]

Facebook also lists Kenya as having made two requests for data related to three user accounts in the second half of 2014. Both requests were denied. Uganda's last request for information from Facebook was submitted in 2013. In 2014, Google and Facebook did not list Burundi, Rwanda, Tanzania or Uganda among the countries that made user data requests.[94]

According to the latest Vodafone Law Enforcement Disclosure Report, during 2014 the government of Tanzania made 933 requests for local subscribers' data. However, it is not possible to compare this figure to that for the previous year, as Vodafone has reported that the figure of 98,765 which it gave for 2013 was erroneous.[95] The company has not published the correct figure for that year. For both 2013 and 2014, Vodafone, which operates in Kenya as Safaricom, was unable to publish statistics related to the Kenyan government's requests for individual communications data due to unclear provisions in the Official Secrets Act and the National Intelligence Services Act.

5.2 Infringements on Freedom of Speech and Press

In Burundi, during the April 2015 demonstrations against President Nkurunziza's bid for a third term in office, in defiance of the two term limit set by the Constitution, mobile access to social media networks such as Viber, Whatsapp and Facebook was reportedly blocked by ARCT to dissuade protestors. The regulator alleged that the networks were being used by protest organisers to mobilise citizens.[96] Radio broadcasters were also affected during the turmoil. Broadcasts by radio Isanganiro, Radio Publique Africaine (RPA), and Radio Bonesha – were suspended beyond the capital Bujumbura.

Amidst the May 2015 coup attempt, the privately owned Radio Publique Africaine (RPA) was hit by a rocket and reportedly set ablaze by police and pro-ruling party youth. Rema radio and television, said to be allied to the ruling party, was torched by protesters.[97] State-owned radio and television stations, Radio-Télévision Nationale du Burundi (RNTB), were forced on and off air and their headquarters was the scene of fierce fighting, as forces jostled for the control of Bujumbura and the channels of mass communication. The upheavals forced even online publishers such as Iwacu to suspend operations and ultimately led to more cases of self-censorship, with many journalists along side human rights activists and opposition politicians being forced to flee to exile.[98] Those who fled include Alexandre Niyungeko, head of the Burundi Journalists' Union.

In Kenya, there were rising incidents of attacks and harassment of journalists and bloggers. In December 2014, blogger Robert Alai was arrested and charged with undermining the authority of a public officer contrary to Section 132 of the Penal Code for allegedly referring to President Kenyatta as an "adolescent president" in a blog.[99] He was again arrested in February 2015 for offending a businessman online by linking him to a land saga that involved the illegal acquisition of the Langata Primary School playground.[100]

[92] Google Transparency Reports, http://www.google.com/transparencyreport/?hl=en

[93] Twitter Transparency Report, https://transparency.twitter.com/country/ke

[94] Facebook Government Requests Report, https://govtrequests.facebook.com

[95] Vodafone, Country-by-country disclosure of law enforcement assistance demands 2015, http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html

[97] Protest Hit Burundi Cuts Mobile Social Network Access, http://www.thesundaily.my/news/1399504

[98] The International Business Week, Burundi descends into communication 'blackout', May 15, 2015, http://www.ibtimes.co.uk/burundi-descends-into-communication-blackout-1501476, @iwacu - https://twitter.com/abakunzi/status/598890805948977152?ref_src=twsrc^tfw New Vision, Burundi journalists seek refuge in Rwanda, http://www.newvision.co.ug/news/670286-burundi-journalists-activists-seek-refuge-in-rwanda.html

[99] Blogger Robert Alai Charged With Undermining President Uhuru Kenyatta, http://www.opennetafrica.org/blogger-robert-alai-charged-with-undermining-president-uhuru-kenyatta/

[100] Blogger Robert Alai arrested over Lang'ata land grabbing saga, http://businesstoday.co.ke/news/media/1423150493/blogger-robert-alai-arrested-over-langata-land-grabbing-saga

Meanwhile, Allan Wadi – a student – was also arrested over “hate speech” and jailed in January 2015 for posting negative comments about the president on Facebook.[101] In the same month, journalist Abraham Mutai was arrested following tweets he posted over alledged corruption in the Isiolo County Government.[102] He was charged with the “misuse of a licensed communication platform to cause anxiety” but was later released.

Nancy Mbindalah, an intern with the department of finance at the Embu County Government, was charged on similar grounds over social media posts dating as far back as 2013, in which she is alleged to have insulted County Governor Martin Wambora.[103]

In all instances, some social media users claimed there were “selective” arrests and prosecution of those critical of government. Critics cited the case of Moses Kuria, a Member of Parliament (MP) for Gatundu South, who allegedly made remarks on Facebook against the Luo Community but did not face the same punitive actions.

In February 2015, the Uganda communication regulator reportedly threatened to “shut down social media sites over misuse by the public.” This came in the wake of concerns over the use of social media to leak and share pornographic content.[104]

In the same month, Ugandan authorities arrested Robert Shaka, accusing him of being behind the pseudonym Tom Voltaire Okwalinga (TVO), whose Facebook account was allegedly used to disclose supposed government secrets. Police ransacked Shaka’s home without a search warrant, and confiscated his personal electronic devices including an iPad, laptop, mobile phone and flash disks.[105]

In June 2015, Robert Shaka was again arrested under Section 25 of the Computer Misuse Act 2011 for using computers and other electronic devices to issue “offensive communication”. Section 25 of the Computer Misuse Act states, “Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor.” A conviction attracts a fine not exceeding UGX 480,000 (US$140), imprisonment not exceeding one year, or both.

The charges of making “offensive communications” related to Facebook posts by TVO on President Museveni’s health status. It was alleged that between 2011 and 2015, Shaka had "wilfully and repeatedly using a computer with no purpose of legitimate communication disturbed the right of privacy" of President Museveni "by posting statements as regards his health condition on social media." However, there was no evidence that Shaka was responsible for posting content under the TVO pseudonym. He was released on bail a week after arrest. The Uganda government has in the past made user information requests to Facebook but they were declined. There are unconfirmed reports that the requested user information was for TVO.

Meanwhile in Rwanda, in March 2015, a defamation complaint was brought against Rwandapaparazzi.rw for violating Article 2 and 3 of the Rwandan Journalists and Media Practitioners Code of Ethics.[106] The complainants accused the website of publishing a story referring to them as “gigolos”. The Rwanda Media Council (RMC) found that the website had published “unfounded slanderous and defamatory statements” against the complaints and recommended that the Rwanda Utilities Regulatory Authority (RURA) should suspend the website for one month as fulfilment of Article 29 of the same code.[107]

[101] *Insulting Kenya's president on Facebook lands blogger in prison, http://stream.aljazeera.com/story/201501022145-0024464*

[102] *Genesis and Synopsis of How Isiolo County Government Degenerated, http://www.mareeg.com/genesis-and-synopsis-of-how-isiolo-county-government-degenerated/*

[103] *Please Excuse this Misuse of Licensed Telecommunications Equipment, http://www.brainstorm.co.ke/2015/02/03/please-excuse-this-misuse-of-licensed-telecommunication-equipment/*

[104] *Daily Monitor, UCC threatens to shut down social media platforms over abuse, http://www.monitor.co.ug/News/National/UCC-social-media-platforms-abuse/-/688334/2619032/-/151o4ktz/-/index.html*

[105] *Chimp Reports, TVO Saga: Robert Shaka Indicted, http://chimpreports.com/tvo-saga-robert-shaka-indicted/*

[106] *Rwanda Media Council Decision on Complaint, http://rmc.org.rw/wp-content/uploads/2015/03/Decision-by-Rwanda-Media-Commission-RMC-on-a-Complaint-Filed-by-Hussein-NZEYIMANA-and-Radju-NIYONKURU-against-rwandapaparazzi.Rw_.pdf*

[107] *Local online tabloid, Rwanda Paparazzi given one month suspension over defamation, InywaRwanda.com, March 03, 2015, http://eng.inyarwanda.com/articles/show/EntertainmentNews/63069/Local+online+tabloidRwanda+Paparazzi+given+one++mo*

Pursuant to Article 4 section 6 of the Memorandum of Understanding between RMC and RURA of September 12, 2013, the Commission has the “responsibility to propose to the Authority to suspend or revoke the license previously granted to [a] media Organ in case of violation of any Law and regulations relating to media in Rwanda.”[108] It is not clear whether RURA effected the suspension of Rwandapaparazzi.rw.

Earlier in February 2015, RMC received a complaint filed by Rwanda Health Communication Centre (RHCC) indicating that the news website Igihe.com misquoted the Minister of Health Dr. Agnes Binagwaho in the case of a five-year old who died from a stomach ailment.[109] The contested article, published on February 2, 2015, quoted the minister as stating that the child’s stomach was “the size of a heavily pregnant woman.”

According to RHCC, the minister never made such a statement. RMC found that there was a deliberate attempt to distort what the minister said, which was professionally unethical and contravened the provisions of Article 2 on honesty and search for truth of the Rwanda Journalists and Media Practitioners Code of Ethics. RMC requested Igihe.com to clarify the story based on the provisions of Article 5 of the Code of Ethics that provides for rectification and right of reply.[110] The news website later published an apology.

In October 2014, Rwandan authorities indefinitely suspended the BBC's vernacular radio news service - the Kinyarwanda Great Lakes Service including its website.[111] To-date, the broadcast service and the websites – www.bbcswahili.com, www.bbcafrica.com, www.bbcafrique.com remain inaccessible from within the country. The suspension followed criticism of the BBC televised documentary "Rwanda's Untold Story", released in early October 2014 which questioned the official accounts of the 1994 genocide. RURA accused the BBC of “genocide denial, promoting division and inciting hatred.”[112]

5.3 Interception of Communications

Evidence on interception of communication remains scanty. Nonetheless, there are pointers to incidents of interception happening in some countries and to efforts by other countries to grow their interception capacity. All countries in the region have laws that specifically provide for interception of communications. Notably, all countries lack sufficient judicial or parliamentary oversight over interception procedures and powers.

Rwanda has provided the clearest evidence of the existence of interception of communications. Popular musician Kizito Mihigo and radio journalist Cassien Ntamuhanga were sentenced to 10 years and 25 years respectively, for terrorism and incitement.[113] In February 2015, the two were convicted of planning to kill President Paul Kagame and inciting hatred against the government. During their trials in April 2014, prosecutors displayed messages the singer shared over the phone, WhatsApp and Skype to show that he conspired with an exiled opposition group to topple the government.

Meanwhile, in July 2015, reports emerged that the Uganda Police and the Office of the Presidency were in advanced stages of acquiring hi-tech surveillance software from Israel and Italy to begin large-scale spying in Uganda.[114] Information released by Wikileaks shows email exchanges between the Italian surveillance malware vendor Hacking Team and its local vendor Zakiruddin Chowdhury, who seemed to have strong contacts with senior Uganda government officials.[115]

It was suggested that the LGBTI community could be among the targets of the surveillance.[116] Earlier, in April 2014 after the Anti-Homosexuality Bill was signed into law, the LGBTI community in Uganda was reportedly targeted by Zeus, a spyware which steals confidential information from computers.[117] Human rights defenders interviewed as part of the present OpenNet Africa research reported incidents of office break-ins and hacking of websites of organisations working on LGBTI issues.

[108] *SIBOMANA Eugene, RMC Recommends RURA to Suspend Rwandapaparazzi.rw for one Month, March 25, 2015 http://rmc.org.rw/rmc-recommends-rura-to-suspend-rwandapaparazzi-rw-for-one-month/*

[109] *SIBOMANA Eugene, Decision by Rwanda Media Commission (RMC) On a Complaint Filed by Rwanda Health Communication Centre (RHCC) Against Igihe.com, March 04, 2015, http://rmc.org.rw/decision-by-rwanda-media-commission-rmc-on-a-complaint-filed-by-rwanda-health-communication-centre-rhcc-against-igihe-com/*

[110] *Rwanda Media Commission, Decision by Rwanda Media Commission (RMC) on a complaint filed by Rwanda Health Communication Centre (RHCC) against igihe.com, http://rmc.org.rw/wp-content/uploads/2015/03/Decision-by-Rwanda-Media-Commission-RMC-On-a-Complaint-Filed-By-Rwanda-Health-Communication-Centre-RHCC-Against-Igihe.Com_.pdf*

[111] *Tom Rhodes, BBC's Rwanda documentary leads to illogical, illegal suspension, https://cpj.org/blog/2014/10/bbc-rwandan-documentary-leads-to-illogical-illegal.php*

[112] *Rwanda BBC Inquiry, Inquiry Committee On The BBC Documentary “Rwanda’s Untold Story" http://rwandabbcinquiry.rw/*

[113] *BBC, Rwanda singer KizitoMihigo planned to kill Paul Kagame, http://www.bbc.com/news/world-africa-31656169*

[114] *Police in Shs 5bn spy deal, The Observer Uganda, http://observer.ug/news-headlines/38889-police-in-shs-5bn-spy-deal*

[115] *Wikeleaks (2015), The Hacking Team - Re: R: I: Uganda Police, https://wikileaks.org/hackingteam/emails/emailid/11829*

[116] *Buzzfeed, Emails Reveal Israeli And Italian Companies’ Role In Government Spying, http://www.buzzfeed.com/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy#.alWw9nveDK*

[117] *Unwanted Witness (UW) News Brief: LGBTI online community experiencing “Zeus malware”, https://unwantedwitnessuganda.wordpress.com/2014/04/25/unwanted-witness-uw-news-brief-lgbti-online-community-experiencing-zeus-malware/*

Wikileaks also revealed that Kenya's government was in the process of acquiring surveillance software from Hacking Team. In one email, a one Chris Kinyanjui tells Hacking Team to bring down the website www.kahawatungu.com either by defacement or by making it completely inaccessible to "serve as a great proof of concept for your capabilities and also provide a means of immediate engagement." According to Daily Nation newspaper, the website is associated with renowned blogger Robert Alai.[118] As of August 2015, the website could still be accessed.[119]

6. CYBERCRIME

In all countries, authorities such as security agencies and regulatory authorities are more willing to discuss the nature and extent of cyber fraud than they are of interception of communications. Although statistics may not be current, in most countries authorities have general figures on cybercrime which they are willing to make public.

In Tanzania, according to research conducted in 2012, a total of 627 cybercrime cases were reported to the forensic section of the Tanzania police force that year – nearly double those reported in 2007.[120] And more recently, according to Abuse Watch Alerting & Reporting Engine (AWARE), there were 28 reported internet abuse incidents originating from Tanzania to the outside world, between January and February 2015. Of these three were for web defacement, seven were related to phishing, five were malware and 13 were Spam.[121]

In Kenya, cybercrime is on the rise as well. The Kenya Cyber Security Report 2014 shows a 108% increase in detected cyber threat incidents, from 2.6 million attacks in 2012 to 5.4 million in 2013.[122] The Kenyan government has fallen victim to a number of hacker attacks. For instance, in 2014, the Twitter accounts for the Kenya Defense Forces, its spokesman and the deputy president were hacked by a group called 'Anonymous Kenya.'[123]

According to the Uganda Police Annual Crime and Road Safety report 2012, a total of 62 cybercrime cases were reported and investigated in which Uganda shillings (UGX) 1.5 billion (US$ 410,000) was lost through hacking victims' emails, phishing, mobile money and ATM fraud. In 2013, fewer cases (45) were reported but these resulted into UGX18.1 billion (US$ 4.9 million) losses. Between the month of August and November 2014, mobile money fraud caused a loss of over UGX 207 million (US$ 56,000) to the users.[124]

In Rwanda, cybercrime came to the fore when police in November 2014 arrested two Rwandans suspected of being part of a cybercrime ring that conducted a sophisticated scheme through which they illegally obtained Rwanda francs (Rwf) 495 million (US$ 676,170) from mobile operator Tigo Rwanda.[125]

No statistics were obtained for Burundi. Nonetheless, an official from the Burundi SETIC (Governmental Secretariat in charge of ICT) told OpenNet Africa researchers about an incident of money theft that occurred in FINALEASE BANK via e-banking. There appears to be no information on this case in the public domain. Another case reported by a Burundian Police officer was that of three individuals who lost money while trying to order second hand cars from Japan online. The police officer did not provide details to OpenNet Africa researchers.

6.1 Online Violence Against Women

The extent of online violence against women (VAW) in Africa remains unknown. However, there are anecdotal indications that it is becoming more rampant, fuelled by increased access to ICT and the lack of laws to punish those who commit online VAW.[126]

Incidents of revenge pornography targeting women have been registered in some East African countries. The region has witnessed an increase in incidents where women's private information, including pictures and videos, are published on social media without their consent.[127] In Uganda, the victims who have included musician Desire Luzinda and television personalities Anita Fabiola and Sanyu Mweruka, were further subjected to threats of prosecution.[128]

In Burundi, a respondent working for a telecom company revealed that there had been incidents of widespread publication of nude photos of women through WhatsApp without the victims' consent. Poor knowledge about securing digital communications has been cited as a cause for growing numbers of women falling victim to this kind of violence.[129]

[118] Vincent Achuka & Walter Menya, WikiLeaks: NIS purchased software to crack websites, http://www.nation.co.ke/news/NIS-WikiLeaks-Hacking-Team-Surveillance/-/1056/2784358/-/o1hyp2/-/index.html

[119] https://www.wikileaks.org/hackingteam/emails/?q=kensi.org

[120] Cyber Crimes Incidents in Financial Institutions of Tanzania by Edison WazoelLubua (PhD) of Muzumbe University, published in the International Journal of Computer Science and Business Informatics

[121] Tanzania Computer Emergency Response Team (TZ-CERT), Incident Statistics, https://www.tzcert.go.tz/index.php/resources-2/incident-statistics/

[122] Telecommunications Service Providers Association of Kenya (TESPOK), The Kenya Cyber Security Report 2014, http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf

[123] 'Anonymous Kenya' Group Hacks Government Twitter Accounts, http://www.itworld.com/article/2696841/security/-anonymous-kenya--group-hacks-government-twitter-accounts.html

[124] Uganda Police Force, Cybercrime Barometer, http://www.upf.go.ug/cyber-barometer/

[125] Rwanda National Police, http://www.police.gov.rw/news-detail/?tx_ttnews%5Btt_news%5D=2977&cHash=21b20085f03ff88ea7193b551696bd26

[126] Association for Progressive Communications, Cases on women's experiences of technology-related VAW and their access justice, https://www.apc.org/en/pubs/cases-women%E2%80%99s-experiences-technology-related-vaw-a

[127] The Daily Monitor, Sex Tapes are Part of Pervasive Levels of Violence Against Women, http://www.monitor.co.ug/OpEd/Commentary/Sex-tapes-are-part-of-pervasive-levels-of-violence-against-women/-/689364/2618598/-/q4h7kiz/-/index.html

[128] Women of Uganda Network, Cyber Insecurity Impedes Fight Against Voilence on Women, http://wougnet.org/2015/02/cyber-insecurity-impedes-fight-against-violence-on-women/

[129] ibid

7. DISCUSSION

Evidently, there is a high belief amongst citizens that communications are being snooped on by governments as attested by 61% of respondents. Not surprisingly, half of the respondents in the survey had ever made the decision not to communicate because of a perceived security risk. This fear factor restricts the potential of the internet to be a democratising space where citizens have the ability to voice their opinions regardless of whether the government or other powerful actors disagree with their opinions.

The findings also show that there is widespread use of a diversity of communications tools in the region. Although voice over mobile and landline, and SMS remain the predominant means of communication amongst citizens, social media use is on the increase, as is the use of other tools such as free video and messaging services. However, considering that majority of the surveyed respondents were frequent users of the internet and were drawn from sections deemed more knowledgeable than the average citizen about the need for securing digital communication, it is worrying that only a small portion had good or excellent digital safety knowledge. Only 10% of the respondents indicated having excellent knowledge of privacy, security and unfettered access in digital communications.

The upside is that a notable number of respondents would become bolder in their digital communications if they were given access to digital safety tools and the skills to use them. This high belief in the ability of technology tools to offer anonymity and security to critical bloggers, journalists, LGBTI groups and other HRDs, brings to the fore the need to expand usage of these tools so as to advance internet freedom in East Africa.

Despite the increased access to and use of internet in the region, more than half (52%) of the respondents had never used tools/ technologies to secure their privacy online. This is a very large number, considering that the threshold of what constituted 'tools and technologies' included low level measures such as privacy settings on social media.

Meanwhile, although findings indicate that there are high perceptions that surveillance is taking place in the region, the extent of surveillance is not known. But even without evidence, these perceptions have created fear within the region, with a large number of citizens practicing self-censorship, or choosing to remain silent in online platforms for fear of reprisals.

Telecom companies and ISPs are likely to come under more pressure to release users' private information to government bodies. Without strong data protection and privacy laws, it will be difficult in the future for these service providers to resist requests for users' data, including those that may be made outside of established procedures.

Several challenges were noted by respondents with regard to internet freedom in East Africa. Emerging internet freedom issues such as online violence against women and girls and child online protection were mentioned. The magnitude of online VAW is unknown since most victims rarely come out to report cases to authorities. Besides, in some countries there are no specific laws that cover these crimes.

Overall, respondents were concerned about government security agencies intercepting their communications, and protection of their data by telecoms service providers. Ultimately, the call to telecom and internet services providers is clear: Take firm measures to protect the privacy of subscribers' data, play a role in educating citizens about digital safety, and publish regular transparency reports. But the findings show that internet users are not only concerned about their privacy and security with perceived government surveillance, but also threats from fellow citizens, hackers and fraudsters.

Besides the challenges specifically mentioned by the respondents, many other challenges are apparent from the overall research. These include general lack of capacity by law enforcement agencies in addressing internet freedom cases, regressive legislations, and increasing digital attacks on human rights activists. Clearly, numerous challenges exist and measures are needed to address these challenges for the status of internet freedom in the region to be lifted.

8. RECOMMENDATIONS

Government

- Telecommunications regulators should initiate collaborative measures with service providers to ensure robust protection of users' data and communications.
- Investigations and prosecution of offences related to online criminal activities should be undertaken in conformity with the provisions of the law, as opposed to adopting practices that undermine free speech and critical opinion.
- Rising online violence against women and girls should be urgently addressed through governments enacting laws that criminalise these acts and specify stringent penalties for perpetrators.
- Desist from using mass surveillance tools that would expose citizens to illegal or unwarranted surveillance and affronts on their rights.
- Support capacity building for law enforcement agencies in technical and non-technical measures to address violations of internet freedom.
- Speed up the enactment of Data Protection laws that guarantee privacy of citizens' information and offer legal recourse to citizens when their data is illegally accessed or compromised.
- Frivolous charges made against bloggers and the media using broad clauses and words such as "misuse of a licensed communication platform to cause anxiety", "publishing false information" and "offensive communication" further limit engagement on issues such as government corruption. Laws with such clauses should be repealed to ensure that societal concerns can be reported and addressed without fear of reprisals.

Civil Society Organisations

- Increase advocacy for the enactment of laws with specific focus on the protection of vulnerable groups including children, LGBTI groups, women and girls online. This should also be supported by public awareness campaigns and initiatives which promote and protect internet rights for all.
- Deliberate efforts should be taken to create awareness and build practical skills in online safety for media, activists, and civil society; and provide them with digital safety tools to ensure secure communication and data protection.
- Build the capacity of the media to uphold journalistic ethics both online and offline.

Telecom and ISPs

- Service providers should ensure that as part of their core service offering to users, there are mechanisms to safeguard users' data from fraudulent activity and privacy breaches.
- Telecoms and internet service providers should initiate campaigns to cultivate general online safety practices amongst subscribers and also make public their policies and procedures in handling subscriber information.
- Government requests for subscriber information should be made public through consistent disclosure reports detailing the number and nature of requests, as well as compliance rates.

ANNEX 1

List of survey respondents in each country including key informants, focus group discussants and stakeholder workshop participants

Burundi

Association pour la Protection des Droits Humains et des Personnes détenues (APRODH)
Ligue ITEKA
Commission Nationale Indépendante des Droits de l'Homme (CNUDH)
Association Burundaise des Consommateurs (ABUCO)
LEO-ECONET
Office National des Télécommunications, division Mobile (ONAMOB)
Le Centre Burundais d'Internet (CBINET)
USAN BURUNDI
Afriregister Burundi
Internet Society, Burundian chapter (ISOC BURUNDI)
Computer Applications Limited Burundi (CAL)
Independent Web Developer
INITELEMATIQUE
Radio Publique Africaine (RPA)
Radio ISANGANIRO
IWACU
REMA FM
NET PRESS
Union Burundaise des Journalistes (Burundi Union of Journalists -UBJ)
Agence de Régulation et de Control des Télécommunications (ARCT)
Secrétariat Exécutif des Technologies de l'Information et de la Communication (SETIC)
Conseil National de la Communication (CNC -Media Regulatory Authority)
Ministry in charge of ICTs (DG TICs)
Burundi Police
An Opposition party leader

Kenya

Airtel
Afrihackathon
Kenya National Commission on Human Rights
Makadara law courts
Kenya Central police station
ICT Authority
Communications Authority Kenya
Nation Media Group
Standard Media group
Royal Media
Faces of Peace
People Daily
Kenya Broadcasting Cooperation
Code for Africa
International Commission of Jurists (ICJ) Kenya
Milimani law courts
Kenya Institute of Security and Criminal Justice
University of Nairobi
Kenya Apps
Housing Finance
Magazine Reel
CNBC Africa
Moi University
Mount Kenya University
Kenya Education Network
Interactive Media Services
Riara University
Blogger Association of Kenya (BAKE)
iHub
Internet Society (ISOC) Kenya chapter
K.A.P
Destiny Africa
Rock ‘n’ Roll Film Festival Kenya (ROFFEKE)
People Daily
CELEB
Kreative Generations
Xchange Perspectives
Otto Benecke Development Foundation
Kenya Broadcasting Cooperation
Worldpress.org
Uwezo Pamoja
Royal Media

Uganda

Ministry of ICT
SMS Media
Freelance IT Consultants
Independent Media Analysts
Uganda Police
Freelance app developers
Freelance journalists
Staff and Students - Makerere University Department of Journalism
Uganda Communications Commission (UCC)
Consumer Rights Association
Independent Social Media Consultant & trainer
Bloggers
Opposition Politician with Uganda People’s Congress (UPC)
Uganda ICT Association
Management Sciences for Health
Uganda Technology and Management University (UTAMU)
Hive Colab
MTN Uganda
Lubega and Ochieng company advocates
Staff and students - Makerere University Business School
Staff and students - Makarere University Faculty of IT
Staff and Students – Makarere University Faculty of Engineering

Staff and students - Ndejje University
Super FM
Radio Uganda
New Vision
Monitor publications
Parliament of Uganda staff
Public Relations Association of Uganda (PRAU)
Cyber School
Information Network (I-Network)
PC Tech Group Ltd
Sexual Minorities Uganda
Vertus Radio
The Patriot Magazine
Bukedde newspaper
Radio one FM
Voice Media Group
Capital FM
Women of Uganda Network
Freedom and Roam Uganda (FORAG)
Bukedde Television
Kawowo news
TopTV
Metro FM
Sanyu FM
The Independent newspaper
Daily Nation Newspaper
Uganda Journalist Union
The Observer
Arua One Radio
Kigezi News Online
Kiira FM Radio
Elgon FM
The East African newspaper
ifreedom Uganda
East and Horn of African Human Rights Defenders Project (EHARDP)
Safety For All Ugandans Online (SAFAUO)

Rwanda

National Human Rights Commission
Association of Youth for Human Rights and Development (AJPRODHO-JIJUKIRWA)
Umbrella body of Rwanda human rights organizations (CLADHO)
National Commission for Children
Transparency International Rwanda
Haguruka.
Broadband Systems Cooperation
Liquid Telecom
4G Networks
4 net Africa Rwanda
MTN Rwanda
Airtel Rwanda
Tigo Rwanda
Rwanda Utility Regulatory Agency
Rwanda Standards Board
Rwanda High Media Council
Higher Education Council.
The New Times
Izuba Rirashe
Rwanda Today
Imvaho Nshya- weekly
City Radio
Flash FM
Contact FM
Isango Star FM
Rwanda Correctional Services
National Identification Development Agency
Ministry of Education
Ministry of Sports and Culture
Ministry of Youth and ICT
Ministry of Local Government
Rwanda Energy Group
WASAC
Private Sector Federation
Intersec Security Company
TOPSEC International
Agespro Security Company

Tanzania

Tanzania Communications Regulatory Authority (TCRA)
Ministry of Information, Youth, Culture and Sports
Vodacom Tanzania
Zantel Tanzania
Smile Tanzania
Jamhuri Media Communications
Start TV
IPP Media
New Habari Cooperation
Tanzania Daima
Mini Buzz TV
University of Dar es Salaam
Masoko Tanzania
Tanzania Information Technology Association
Legal and Human Rights Centre
Change Tanzania
Tanzania Human Rights Defenders Coalition (THRDC)
Union of Tanzania Press Clubs
Chama Cha Mapinduzi (CCM)
Chama cha Demokrasia na Maendeleo (Chadema)
Alliance for Change and Transparency (ACT)
The Habari.com
FikraPevu.com
8020fashions.com
mpekuzihuri.com
bloguyawananchi.com
isaamichuzi.com
Muhimbili National Hospital
Jamii Forums
Business Times
Lenzi ya Michezo
dewjiblog.com
Uhuru Publications

This report was produced by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) under the Open Net Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedom in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania and Uganda.

The production of this report was supported by the Humanist Institute for Co-operation with Developing Countries (Hivos) and the Open Technology Fund (OTF).

OPEN TECHNOLOGY FUND

Hivos
people unlimited

CIPESA

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
Facebook: facebook.com/cipesaug
www.cipesa.org