State of Internet Freedoms in East Africa 2014

An Investigation Into The Policies And Practices Defining Internet Freedom in East Africa

OpenNet Africa

CIPESA

Credits

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) is grateful to our partners on this project, who offered technical and financial support. They include the Humanist Institute for Co-operation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

This report presents the findings of an exploratory study on the state of internet freedoms in East Africa. The research reviewed policy developments and actions related to internet freedoms over the period 2010 to April 2014. This report contains brief summaries of country reports but full-length reports have been written for Burundi, Ethiopia, Kenya, Rwanda, Tanzania, South Africa and Uganda. They are available at CIPESA's internet freedoms monitoring portal, OpenNet Africa (www.opennetafrica.org).

Research steering committee
Ashnah Kalemera, Lillian Nalwoga, Juliet Nanfuka, Wairagala Wakabi

Researchers and reviewers
Grace Githaiga, Christopher Gore, David Kezio-Musoke, Paul Kimumwe, Endalkachew Michael, Samuel-Paul Mugabi, Alain Ndikumana, Ansbert Ngurumo, Masashi Nishihata, Jean-Paul Nkurunziza

Design
Ish Designs
muwonge_issa@yahoo.com

State of Internet Freedoms in East Africa 2014
Published by CIPESA, www.cipesa.org
May 2014

Content

Introduction

Information and Communication Technologies (ICT) can offer easy access to information, swift communications, and flexible options of when and where citizens use them. As a result, ICT has become important for citizen participation in democratic processes, increased scrutiny of government actions, and improved management of public affairs. In East Africa, the internet and other digital technologies have become a key platform for citizens to enjoy their rights to expression and to associate with other citizens as well as with leaders.

Social network sites (SNS), such as Facebook, Youtube and Twitter, which are popular in East Africa, are helping to trigger non-institutionalised democratic participation by providing communication spaces through which individuals articulate “democratic ideas". Along with other digital technologies, SNS are providing a voice to those individuals[1] who were previously left out of traditional media. Consequently there has been an expansion in the breadth of opinion expressed in the public domain thereby contributing to building a democratic culture. However, many challenges stand in the way of East African citizens’ enjoyment of their right to seek, receive and impart information and ideas through digital technologies. These challenges include unfavourable legal regimes and affronts by both state and non-state actors, poor infrastructure and the high accessibility costs that have tended to create a wide digital divide. They also include irresponsible behaviour by internet users who are often unaware of online ethics or legal regimes that govern the internet and other non-traditional media.

The use of ICT in East Africa continues to grow steadily, with social media and mobile banking among the drivers of use. In Kenya, Tanzania, Uganda and Rwanda, mobile access rates have grown to beyond the 50% mark and internet access is also rising.

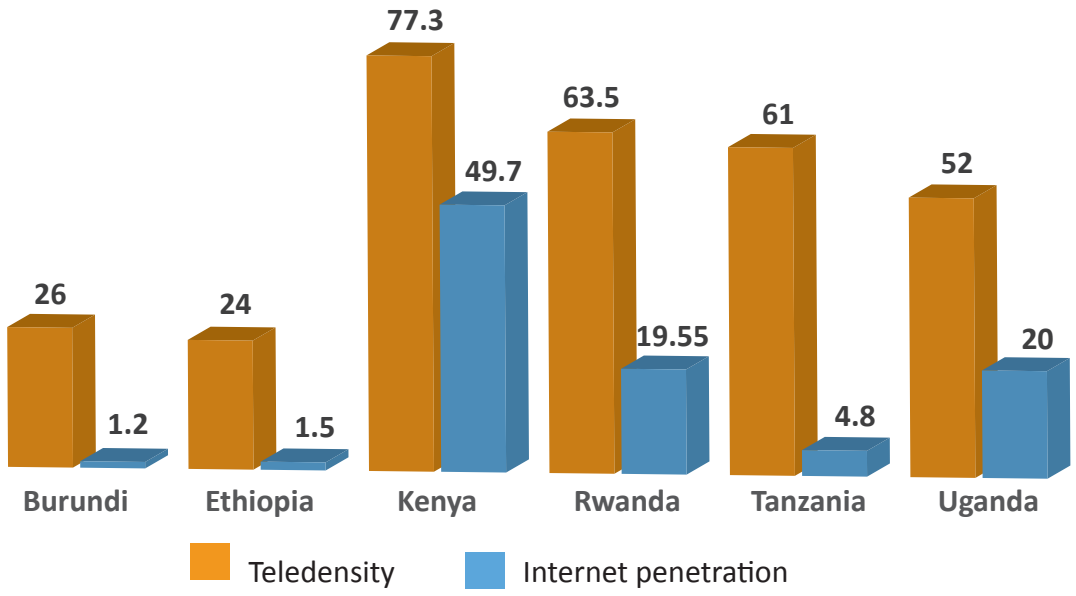

Figure : Telephone and Internet Penetration in East Africa (% of the population) [2]

1 Ndavula, J. and Mderia, H. (2012) Social Networking Sites in Kenya: Trigger for Non-Institutionalized Democratic Participation, http://www.ijbssnet.com/journals/Vol_3_No_13_July_2012/37.pdf

2 Data from the respective national communications regulators, see individual reports on the Open Net Africa website (www.opennetafrica.org).

However, as more East African citizens get online, governments are evidently taking a keener interest in what citizens are doing with their phones and on the internet. As this research reports, governments in East Africa are increasingly moving to place controls over the internet and associated technologies such as mobile phones. These caveats are framed from the angle of countering terrorism, fighting pornography, or guarding against cybercrime. However, often they are intended – or result into – curtails on legitimate opinion and affronts to the enjoyment of the right to freedom of expression. As examples from various countries in East Africa show, these caveats are often retrogressive and hamper citizens' right to seek, receive and impart information and ideas through digital technologies. They also appear to be mainly aimed at stifling critics of state actions and curtailing citizen organising rather than genuinely protecting the public good. Poor judicial oversight in surveillance and monitoring of citizens' communications was noted in some of the countries studied. Meanwhile, "distributed oversight," which could see both civil actors and state organs play a role in ensuring that monitoring and surveillance were in accordance with the law, was virtually non-existent.

This research found that in a number of countries, although national constitutions guaranteed numerous rights, various legislations curtailed the enjoyment of freedoms of expression and association online. It was also found that a plethora of laws related to citizens' online actions has been introduced between 2010 and 2014. However, in all countries studied, it appeared there was widespread lack of knowledge on what constitutes online freedoms, coupled with low levels of knowledge and skills about threats to online safety, including among bloggers, journalists and activists who regularly use the internet.

Notably, there are few conversations in East African countries on internet freedoms matters. Where they are taking place, they are often not informed by research, nor are they driven by an agenda that seeks to educate citizens and promote liberal regimes of online rights. Rather, these conversations are primarily framed by regulators (of communications, of media and of elections, for instance) and government departments who tend to slant the issues to favour heavy caveats on individuals' online expression and privacy. Moreover, there is a paucity of literature on internet freedoms in relation to most of the countries covered by this research. This further limits the role civil society, the media, legislators and regulators can play in promoting awareness and protection of internet freedoms.

This report aims to fill the deep gap in information on the state of online freedoms in East Africa and to form the basis for discussions, awareness and capacity development. It is a handy resource for media, academia, development actors and civil society in creating awareness and lobbying for the protection and promotion of internet freedoms in Africa.

The research presented in this report was conducted through a mix of methods: researchers based in the focus countries conducted policy and document reviews plus interviews with key informants. Between November and December 2013, technical audits were conducted on 1,413 websites (Uganda) and between July and August 2013, some 1,412 websites were tested (Ethiopia) using rTurtle software for evidence of blocking. Independent country-based experts reviewed the country research reports that form the basis of this regional report. The primary interest of the research was how policies and practices in each country were affecting internet freedoms, and it sought evidence of surveillance, interception, monitoring or blocking of access to digital communications and services. The research mostly covered developments between January 2010 and April 2014.

Country summaries

Burundi

With internet penetration at 1.2% and tele-density of 26 cell phones per 100 inhabitants, Burundi has one of the lowest ICT use rates in the region. During 2013, Burundi became one of the first countries in the region to pass laws that specifically provided for regulation of online media. The January 2013 amendments to the National Communications Council (CNC) law gave the regulatory body oversight over internet writings under Article 7, while Article 10 tasks the council, together with the communications ministry, with monitoring compliance to professional ethics by all online news agencies.

Meanwhile, the Press Law, also amended in 2013, proscribes dissemination of information – in print, broadcast and digital – that undermines national security, incites civil disobedience, serves as propaganda for enemies or insults the country's president. Article 29 of this law makes it a requirement for the owners of online publications and news agencies to disclose certain information to CNC or the public prosecutor's office. Amongst this information is the first edition of the publication, the full identity and address of the director of the publication, the editor's criminal record, the full address of the web host, the languages of publication and the constitution of the publishing agency.

On May 31, 2013, the online website of Iwacu newspaper was ordered by the CNC to block the comments section of its website[3] for 30 days, following readers' comments published on the site which the commission said contravened sections of the press law on "attacks on national unity, public order and security, inciting ethnic hatred, defending criminal activity and insulting the head of state." However, Iwacu said CNC never specified the comments it found in contravention of the law.

In justifying its actions, the CNC's chairperson Pierre Bambasi was quoted as saying, "We cannot have individuals or groups screaming abuse on the internet, stirring up ethnic hatred, talking of taking up arms and urging the people to rise up".[4] Three days before the ban, while responding to a May 28, 2013 warning from the CNC about the website comments, the Iwacu director explained in a letter to the regulator how they moderated improper readers' comments and were committed to improve filtering mechanisms within three weeks. He said of 400 comments received on May 28 and May 29 – the dates cited by the regulator – Iwacu had rejected 1 in 8 comments. As part of the website's user conditions, insults, defamation, racism and anti-Semitism speech are prohibited. Any posts infringing intellectual property rights are also not allowed. The publisher complied with the order from CNC, but rather than block only the comments section, Iwacu suspended publishing of articles on the whole website for the entire 30 days.

[3] *Iwacu newspaper online, http://www.iwacu-burundi.org/blogs/english/*
[4] *Burundi - Media regulator suspends comments on press group's website, http://www.trust.org/item/20130531164503-qium7/?source%20=%20hppartner*

Once the Iwacu website suspended its online publication, another website, www.ganira.com, was anonymously created where all of Iwacu's articles were posted and readers were able to comment on the articles. This website has since been shut down by its owners. In an interview in December 2013, Antoine Kaburahe, the Director of Iwacu Press Group, denied knowledge or association with the owners of Ganira.com, although he acknowledged that the new website continued with discussions that had started on the Iwacu website.[5] The Iwacu forum was re-instated on June 30, 2013 and remained fully accessible in Burundi as of April 2014. The fact that the Burundian government did not direct ISPs to block www.ganira.com was probably an indication that blocking was not taking place. On the other hand, the Ganira website episode showed that Burundians had the scope to anonymously run websites that could help them to access information and freely express themselves online.

Earlier in 2010, leading independent journalist Jean-Claude Kavumbagu was arrested over a report on his internet-based newsletter, Net Press, criticising the country's military, and he spent 10 months in prison. Mr. Kavumbagu, who had previously been arrested at least thrice over articles run by his online agency, was acquitted on the treason charge but found guilty of publishing an article "likely to discredit the state or economy".

Amendments to the media law drew criticism from the media and civil society and saw the lodging of an appeal. In January 2014, four Articles of the media law (Articles 61, 62, 67 and 69) were declared invalid by the country's constitutional court following a petition by the Burundi Union of Journalists. The union argued that articles such as those that stipulated fines for an initial offence before any warning, and vague definitions of "internet publications", were unconstitutional.[6] Before President Pierre Nkurunziza assented to this law, an online petition against it gathered 12,000 signatures.[7]

While Burundi's constitution guarantees citizens' privacy, freedom of expression and opinion, amendments made to the Code of Criminal Procedure in April 2013 provide for interception of communications, potentially including digital communications. The recent amendments to the law are likely to have a chilling effect on internet users, who might increase self-censorship in the knowledge that government is watching them and can take such action as that meted out on Iwacu and the Net Press editor. In January 2014, the communications regulator warned citizens against sending threatening SMS at a time the oppostion was mobilising for mass protests against proposed constitutional amendments, and reminded users that these messages could be traced to the sender.

This research did not find evidence of the Burundi government ordering internet service providers to block particular websites or SMS services, or the tapping of telephone conversations. However, failure to find such evidence was not proof that no such activity existed.

[5] *Nous sommes de nouveau là Communiqué du Groupe de PresseIwacu, http://www.arib.info/index.php?option=com_content&task=view&id=7350*
[6] *IFEX, Constitutional Court quashes several repressive provisions of Burundian media law, http://www.ifex.org/burundi/2014/01/08/articles_quashed/*
[7] *Radio Netherlands, 12 000 signatairescontre la loisur la presse au Burundi, http://www.rnw.nl/afrique/article/12-000-signataires-contre-la-loi-sur-la-presse-au-burundi*

Ethiopia

Although Ethiopia has some of the lowest ICT usage rates in Africa because of the tight control the government maintains over telecom services provision, more people are now getting access to mobile phones and the internet. In a country of 92 million people, mobile penetration stands at 24% while internet usage stands at 1.5%.[8] The national literacy rate is 30%. Although there has been an increase in mobile phone use and consequently internet access, the ease with which security services access users' data is worrying. This increasing technological ability of Ethiopians to communicate, express their views, and organise, is viewed less as a social benefit and more as a political threat for the ruling party, which depends upon invasive monitoring and surveillance to maintain control of its population, according to Human Rights Watch.[9] The country has since 1991 been under one party rule of the Ethiopian People's Revolutionary Democratic Front (EPRDF).

Citizens who use the internet to criticise the one party rule have been accused of promoting terrorism and their websites and blogs are blocked. At the end of April 2014, the government arrested six bloggers and three journalists, accusing them of working with foreign organisations and rights activists through "using social media to destabilise the country."[10] The bloggers are members of a group called Zone 9, which used blogs, Facebook and Twitter to discuss socio-political issues in the country.[11] With their website blocked in Ethiopia, they were mainly using Facebook and Twitter. In the months preceding the arrests, the group's website was inactive amid reports of fear and intimidation. The arrests came days after the group announced plans to rejuvenate its activism. At the time of this report, the bloggers and journalists had reportedly been denied legal counsel.[12]

Article 29 (2) of Ethiopia's constitution provides that "Everyone has the right to freedom of expression without any interference. This right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any media of his choice." These guarantees have been undermined by laws that detract from citizens' right to freedom of expression and privacy, as well as security agencies' flouting of judicial oversights in the process of monitoring citizens' communications. The 2008 Media Law, the 2009 Anti-Terrorism Law, the 2012 Telecom Fraud Law and most recently, the National Intelligence and Security Re-establishment Proclamation of 2013 have one after the other taken back the rights provided by the constitution.

[8] *International Telecommunications Union (ITU), ICT Facts and Figures, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*

[9] *Human Rights Watch, "They Know Everything We Do", Telecom and Internet Surveillance in Ethiopia, http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf*

[10] *Addis Standard, Ethiopia Files Charges Against a Group of Bloggers, Journalists Detained Over the Weekend, http://allafrica.com/stories/201404281454.html*

[11] *See http://zone9ethio.blogspot.com/*

[12] *Global Voices Online, Advocates Ask African Commission, UN Experts to Intervene in Zone 9 Bloggers Case, http://advocacy.globalvoicesonline.org/2014/05/03/advocates-ask-african-commission-un-experts-to-intervene-in-zone-9-bloggers-case/*

The Telecom Fraud Offence Proclamation No. 761/2012 proscribes the use of telecoms infrastructure other than that offered by Ethio Telecom. Activists believe that this section can be used against users of Skype and other VOIP services such as Google Talk, which are among the services monitored by the Ethiopian government and are also widely used by activists. In Section 15, the law provides that digital or electronic evidence; evidence gathered through interception or surveillance; and information obtained through interception conducted by foreign law enforcement bodies, are admissible as evidence in court. It also stipulates a 3 to 8 year prison sentence and a hefty fine for "whosoever uses or causes the use of any telecom network or apparatus to disseminate any terrorising message connected with a crime punishable under the Anti-Terrorism Proclamation" or an obscene message punishable under the Criminal Code. The Anti-Terrorism Proclamation of 2009 authorises interception of communication and a number of journalists, bloggers, and democracy activists have been charged and sentenced under this law.

During 2013, Ethiopia revamped the Information Network Security Agency (INSA), which is said to be at the forefront of the government's internet control and censorship strategy. The proclamation revamping INSA stated that social media outlets, blogs and other internet related media had great capabilities to instigate dispute and war, to damage the country's image and create havoc in the economic atmosphere of the country.[13]

Meanwhile, the National Intelligence and Security Service (NISS) was re-established in 2013 with the status of a ministry and reports to the Prime Minister. It is mandated to carry out intelligence work inside and outside of the country, including on terrorism and extremism. It is heavily involved in surveillance and monitoring of citizens' online actions. Under Article 8 (7) of its proclamation law, the NISS is mandated to conduct surveillance, using a court warrant, "in order to protect national security and prevent threats to national security" and can do this "by entering into any place and by employing various mechanisms." Under Article 27, all persons have a duty to cooperate, if requested, in furnishing intelligence or evidence necessary for the work of the NISS. Those requested to provide assistance to the service are required to keep the request confidential.

Studies suggest that perhaps more than any other country in Africa, Ethiopia regularly blocks websites, undertakes surveillance of websites and social media, and charges journalists over content published offline and online.[14] Following the disputed elections of 2005, government blocked websites and access to social media in the face of protests by the opposition.[15][16] Since then, consistent affronts to online freedoms have continued into 2014. OpenNet Initiative (ONI) testing conducted in Ethiopia in September 2012 found that online political and news content continued to be blocked, including the blogs and websites of a number of individuals who had been recently convicted.[17] In May 2013, the Supreme Court upheld the conviction and 18-year prison sentence for journalist and blogger Eskeder Nega, who was sentenced in June 2012 for allegedly attempting to spark an Arab spring-style revolt in the country. That year, up to 150 websites were reportedly blocked in Ethiopia, including those owned by news

13 *DireTube, Information Network Security Agency (INSA) of Ethiopia is to be reestablished, http://www.diretube.com/article.php?keywords=The+Information+Network+Security+Agency+%28INSA%29&btn=Search*

14 *Tests by the Citizen lab have consistently found evidence of hundreds of websites that are blocked, as well as presence of surveillance software. Moreover, Freedom House ranks Ethiopia as 'Not free' in terms of online freedoms. See https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/*

15 *Barry Malone, "VOA Says Ethiopia Blocks Website as US Row Escalates," http://af.reuters.com/article/topNews/idAFJOE62S0KX20100329?rpc=401&feedType=RSS&feedName=topNews&rpc=401&sp=true.*

16 *Google Blocked in Ethiopia, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml*

17 *OpenNet Africa, Update on information controls in Ethiopia, https://opennet.net/blog/2012/11/update-information-controls-ethiopia*

organisations, political parties, bloggers, and international organisations such as Human Rights Watch and the Committee to Protect Journalists.[18]

Earlier in March 2013, Ethiopia was accused of blocking the Arabic and English language websites of Al Jazeera, after the network aired programmes on protests in Ethiopia.[19] In October 2012, Jemal Kedir, 32, was found guilty of "rumour-mongering" and handed a one-year jail term. Federal prosecutors charged that SMS messages he sent through his mobile phone were intended to foment dissension, arouse hatred against the government, or stir up acts of violence or political, racial or religious disturbances.[20]

Tests conducted by the Citizen Lab from July to August 2013 on Ethionet, and shared with the authors of this report, showed that 62 websites of a test list of 1,412 could not be accessed in Ethiopia.

Table: *Categorised blocked URLs and methods of blocking in Ethiopia (Source: Citizen Lab test lists)*[21]

Category	*Category Description*	*Total number tested*	*Number blocked*	*Blocking methods*
Political	Opposition, human rights, freedom of expression, minority rights and religious movements	1412	51	*The websites were blocked using methods difficult to distinguish from network problems including:* • Connection aborted as a result of an injected TCP reset (RST) packet • DNS Error – Resolution process failed • SSL Dropped – Client did not receive Server Hello response during SSL handshake • UNREQ SYN – Client did not receive response to initial SYN during TCP handshake
Social	Sexuality, gambling, illegal drugs and alcohol, and socially sensitive/offensive topics		3	
Conflict & Security	Armed conflicts, border disputes, separatist movements, and militant groups		2	
Internet tools	Web sites that provide e-mail, Internet hosting, search, translation, Voice -over Internet Protocol (VoIP), telephone service, and circumvention methods		6	
	Total	**1412**	62	

[18] *IMF.org and Economist.com Joined the Long List of Blocked Websites in Ethiopia, June 27, 2012, http://ethsat.com/2012/06/26/imf-org-and-economist-com-joined-the-long-list-of-blocked-website-in-ethiopia/*
[19] *Al Jazeera, Ethiopia 'blocks' Al Jazeera websites, http://www.aljazeera.com/news/africa/2013/03/201331793613725182.html*
[20] *LiyaTerefe, Ethiopian man jailed for one year for inciting public disorder using text messages, http://sodere.com/profiles/blogs/ethiopian-man-jailed-for-one-year-for-inciting-public-disorder*
[21] *Citizen Lab, Ethiopia 2013 Testing Results, https://citizenlab.org/2014/04/citizen-lab-collaborates-human-rights-watch-internet-censorship-testing-ethiopia/*

Similarly, an extensive study published by Human Rights Watch in 2014 showed that Ethiopian security officials could access the records of all phone calls made inside Ethiopia with few restrictions; and that users' emails and phone recordings had been tendered as evidence against perceived anti-government activists tried under the anti-terrorism law. The government was also using "some of the world's most advanced surveillance software to target key individuals in the Diaspora."

Earlier studies during May 2012 showed that the Tor Network anonymising tool was blocked in Ethiopia. Furthermore, internet scans conducted in 2013 by the Citizen Lab discovered the use of FinSpy surveillance malware using pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users.[22] In February 2014, an American citizen of Ethiopian origin living in Maryland sued the Ethiopian government for infecting his computer with secret spyware, wiretapping his private Skype calls, and monitoring his entire family's every use of the computer for months, as government agents allegedly attempted to gather information on members of the Ethiopian diaspora who criticised the ruling regime.[23]

[22] *The Citizen Lab, You Only Click Twice: Finfisher's Global Proliferation, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/*
[23] *Electronic Frontier Foundation, American Sues Ethiopian Government for Spyware Infection, https://www.eff.org/press/releases/american-sues-ethiopian-government-spyware-infection*

Kenya

Kenya's democratic credentials have been improving, with peaceful presidential elections in March 2013, supported by the country's steady implementation of wide-ranging governance reforms mandated by the 2010 constitution. The reforms include devolution of government, a cut to powers of the presidency, and greater transparency in public operations. Despite these progressive reforms, Kenya lacks an access to information law, although a bill was published in 2007. In 2013, Kenya amended two of her communications acts – the Kenya Communications and Information (Amendment) Act, 2013 and the Media Council Act 2013 - inserting retrogressive provisions that restrict media freedom and general freedom of expression. There were attempts to amend the Public Benefits Organisations Act, which would have greatly limited freedoms of association. The amendment bill was discarded after intense criticism from the public.

The country has some of the highest ICT usage rates in Africa, with 31.3 million mobile subscriptions, representing a mobile penetration of 77%. Internet access stands at 52% of the population and there are 26 million subscribers to the mobile money service.[24] The mobile phone is the preferred method of internet access and social media sites are among those accessed most. As of March 2014, the top websites accessed by Kenya's internet users were Google, followed by Facebook, Youtube and Twitter. Wikipedia, Blogspot were also among the top 10.[25]

An issue at the centre of the debate on internet freedoms in Kenya is hate speech. It became more prominent after the post-election violence of 2007-2008, in which up to 1,200 people were killed. The elections of 2013 not only saw increased usage of ICT for varying purposes, by citizens, civil society groups, and politicians, but also a surge in hate speech over the internet, particularly through social media.

There were regulatory measures prior to the elections to deter and to punish hate speech perpetrators. The National Cohesion and Integration Act of 2008, under section 13 states that a person who uses speech (including words, programs, images or plays) that is "threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behaviour commits an offence if such person intends thereby to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up."

The Communications Amendment Act 2009 also criminalises the sending of messages that are "grossly offensive or of an indecent, obscene or menacing character". In March of 2011, the National Integration Cohesion Commission (NCIC) announced it would monitor hate speech on the internet in the lead-up to the 2013 polls. Dr. Mzalendo Kibunja, the head of the Commission, stated: "Facebook, twitter and such networks will be our main focus and I can tell you most of the hate speech comes from the Diaspora not internally."[26] This was

[24] *Communications Commission of Kenya (CCK), Quarterly Sector Statistics report: Second Quarter of the Financial year 2013/14, April 16, 2014; http://www.cck.go.ke/resc/downloads/Sector_Statistics_Report_Q2_201314.pdf*
[25] *Alexa, Top Sites in Kenya, http://www.alexa.com/topsites/countries/KE*
[26] *MoreenMajiwa, NCIC Monitoring Social Media for Hate Speech, March 26, 2011; http://www.mzalendo.com/blog/2011/03/26/ncic-monitoring-social-media-for-hate-speech/*

followed by regulations issued by the then communications regulator, the Communications Commission of Kenya (now Communications Authority of Kenya) on sending political bulk SMS. The regulations required service providers to vet content before rejecting or sending it.

However, although these measures reduced the negative role that SMS played during the 2007-2008 post-election violence, they did not dissipate the role of social media in spreading hate speech during the 2013 elections. As one study noted, hate speech appeared to have largely migrated from SMS and found a new home on the web, particularly on social media.[27] During the 2013 elections period, telecommunications service provider Safaricom, which enjoyed a 65% share of the voice market and 75% of the internet market, rejected at least 18 bulk message transmission requests for reasons such as failing to submit a copy of ID, or specifying who was signing off the message. These requests were sent back to the clients for amendment and five of them were never returned to Safaricom.[28]

According to the Umati project that monitored hate speech online in the run up to the 2013 elections, bloggers and other social media users were the main perpetrators of hate speech. During March of 2013, some 405 incidents of offensive speech online were recorded, as were 358 incidents of moderately dangerous speech, and 321 incidents of extremely dangerous speech.[29]

Meanwhile, in March 2013, Kenyan authorities were reported to be tracking down 14 bloggers accused of posting hate messages on the internet. Six of them had already been identified, and one had been charged with posting "annoying" statements on Twitter and Facebook.[30] Among those that were investigated was well-known blogger Dennis Itumbi, whom the NCIC accused of "posting threatening messages" on a Facebook account, which were "intended to cause ethnic hatred among various communities." He denied the allegations.[31]

However, the lack of equipment and skills by the police and the NCIC made it hard to investigate and prosecute suspects, with accused persons often set free because of lack of sufficient evidence to prove that they owned social media accounts used to propagate hate speech. The NCIC stated that one of the barriers to prosecuting those who posted material online was that, without permission from the interior ministry, the commission did not have the power to launch an investigation on its own. The commission also needed to receive a complaint before carrying out investigations.

Also, ahead of the 2013 elections, the Communications Commission had blocked access to the web portal Mashada.com, accusing it of failing to moderate hate speech.[32] There were also actions against specific individuals such as in 2012, when blogger Robert Alai was arrested over a tweet that suggested a government spokesperson had ordered the murder of two

[27] *Institute for Human Rights and Business, Corporate responses to Hate Speech in the 2013 Kenya Presidential Elections: Case Study Safaricom. November 2013*
[28] *Ibid*
[29] *OpenNet Africa, Monitoring Dangerous Online Speech in Kenya, http://opennetafrica.org/wp-content/uploads/researchandpubs/Monitoring%20Dangerous%20Online%20Speech%20in%20Kenya.pdf*
[30] *Kenya: 14 bloggers linked to hate messages http://www.nation.co.ke/News/14-bloggers-linked-to-hate-messages/-/1056/1732288/-/cut5kvz/-/index.html*
[31] *Judie Kaberia and NzauMasau, Kenyan Authorities in the Dock Over Hate Speech, http://iwpr.net/report-news/kenyan-authorities-dock-over-hate-speech; Bernard Koech, Tackling Online Hate Speech in Kenya, http://iwpr.net/report-news/tackling-online-hate-speech-kenya*
[32] *Was The Government Justified In Shutting Down Mashada.com?' http://jameni.com/was-the-government-justified-in-shutting-down-mashada-com/*

human rights activists. He was held for two days then released on bond. His arrest was effected in terms of Section 29 of the Information and Communication Act.[33] In April 2012, blogger Itumbi sued blogger Robert Alai for defamation via malicious tweets.[34] Alai was arrested again in April 2013 over an "offensive tweet" and charged under Article 29(b) of the 2009 Kenya Information and Communications Act.[35] He was acquitted. Further, in the first half of 2013, Kenya made a request to Google to remove content from Blogger, arising out of a court order in a defamation case. The request was rejected.[36]

Legal experts warned that tracking web traffic could be an invasion of privacy since Article 31 of Kenya's constitution granted all citizens the right to privacy, including in the sphere of online communications.[37] Moreover, Brice Rambaud, programme director of the media consultancy Internews, said NCIC seemed to be targeting well-known bloggers and social media activists, yet "most of the dangerous speech witnessed on social media came from ordinary citizens."[38]

Kenya's National Intelligence Service Act, 2012 gives security agencies the powers to monitor communications as well as to "search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing." It describes the term 'monitor' as the "means to intercept, listen to, record or copy using any device." Under Article 45, a member of the intelligence service needs to obtain a warrant for authorisation to do monitoring. The law does not state in detail what kinds of communications may be monitored.[39]

[33] *Gareth van Zyl, Blogger's arrest shines light on Kenya's internets freedom, IT Web, http://www.itwebafrica.com/ict-and-governance/256-kenya/229859-bloggers-arrest-poses-questions-about-kenyas-internet-freedom*
[34] *Dennis Itumbi, "Why I am moving to court against a blogger," DennisItumbi.com (blog), March 18, 2012, http://www.dennisitumbi.com/?p=297.*
[35] *Jambonewspot.com, Robert Alai arrested for alleged "libelous" twitter post, http://www.jambonewspot.com/robert-alai-arrested-for-alleged-libelous-twitter-post/*
[36] *CIPESA, Online Freedoms Under Siege as African Countries Seek Social Media Users' Information, September 2013, http://www.cipesa.org/2013/09/online-freedoms-under-siege-as-african-countries-seek-social-media-users-information/#more-1623*
[37] *Institute of War and Peace Reporting (IWPR), Tackling Online Hate Speech in Kenya, http://iwpr.net/report-news/tackling-online-hate-speech-kenya*
[38] *Jude Kaberia, Kenya: Too Little Action on Hate Speech?, http://iwpr.net/report-news/kenya-too-little-action-hate-speech*
[39] *The National Intelligence Service Act, 2012, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/NationalIntelligenceServiceAct2012.PDF*

Rwanda

Rwanda has a population of 10.5 million with mobile penetration at 63% and internet penetration of 19.55% in December 2013.[40] The country has put ICT at the forefront of its development agenda with initiatives such as the National Information Communication Technology Literacy and Awareness Campaign and Vision 2020, which aim to improve governance, access and build ICT skill.[41] However, this progress in the access to and use of ICT by citizens and the government remains hampered by regressive laws.

Rwanda has a history of tough control over the media, particularly after some media houses fuelled ethnic tensions during the 1994 genocide. In recent years, numerous journalists have been harassed or charged in courts of law for such reasons as criticising government institutions and leaders or "promoting the genocide ideology". Human rights watchdogs often accuse the government of stifling the political opposition and curtailing the activities of civil society actors.

This repressive control has been creeping into the online sphere: as recently as April 2014, state agencies intruded into citizens' communications and took action against online publishers. In a strong indication that Rwanda monitors citizens' communications, in April 2014 during the terrorism and treason trial of popular musician Kizito Mihigo and radio journalist Cassien Ntamuhanga, prosecutors displayed messages the singer shared over the phone, Whatsapp and Skype. The musician said the messages were genuine but denied he intended to join a group intent on overthrowing the government.[42] Records of emails, phone calls and text messages belonging to opposition activists have been tendered as evidence in previous trials. Also in April 2014, there were reports that the editors of Umusingi newspaper, Isimbi newspaper and the www.ireme.net news website were on the run fearing arrest.[43]

Notably, Article 33 of Rwanda's Constitution guarantees freedom of thought, opinion, conscience, religion and worship. Article 34 provides for freedom of information and freedom of the press. Similarly, the Rwanda Media Law No. 02/2013 gives journalists the right to freedom of opinion and expression, including the "right to seek, receive, give and broadcast information and ideas through media". Section 3, Article 19 of this law is dedicated to internet-based media and states: "Every person has the right to receive, disseminate or send information through internet. He/she is entitled to the right of creating a website through which he/she disseminates the information to many people. Posting or sending information through the internet does not require the user to be a professional journalist."

[40] *Rwanda Utilities Regulatory Authority (RURA), "Statistics and Tariff Information in Telecom Sector as of December 2013," http://www.rura.rw/fileadmin/docs/statistics/Telecom_Statistics_Report_December_2013.pdf*
[41] *The Republic of Rwanda, Ministry of Youth and ICT, ICT Sector Profile, 2012, http://admin.theiguides.org/Media/Documents/Rwanda-ICT-Profile-2012.pdf*
[42] *Phone evidence used in terror, treason case; The EastAfrican, April 26, 2014, http://www.theeastafrican.co.ke/news/Phone-evidence-used-in-terror/-/2558/2294196/-/klwpvi/-/index.html*
[43] *Great Lakes Voice, Three senior Journalists flee Rwanda, April 21, 2014; http://greatlakesvoice.com/breaking-four-senior-journalists-flee-rwanda/*

In August 2013, Rwanda amended the 2008 law on interception of Communications.[44] In the new law, national security services can apply for issue of an interception warrant to monitor citizens' voice and data communications on grounds of national security. Article 4 of the interception law "strictly" prohibits the interception of communications of the president. Government authorities of "the relevant security organs" are authorised to apply for an interception warrant. Warrants are issued by a national prosecutor who is appointed by the justice minister. In urgent security matters, a warrant may be issued verbally, "but the written warrant shall be completed in a period not exceeding twenty four hours". A warrant shall be valid for three months.

Whereas Article 7 of the 2013 law requires service providers to ensure that their systems "are technically capable of supporting interceptions at all times, security organs have powers to intercept communications using equipment that is not facilitated by communication service providers." Article 10 states that authorities can apply for a warrant "without recourse" to the communication service providers. The law relating to arms governs the equipment used for such interception and the president has the powers to determine which organ is in charge of such equipment. Article 12 provides for the appointment of "inspectors" to ensure that authorised interceptions are enforced in accordance with the law. However, the independence of these inspectors may be called into question given that they are appointed by the president.

In addition, the 2001 Law Governing Telecommunications states that court can authorise the interception or recording of communications in the interests of national security and the prevention, investigation, detection and prosecution of criminal offences. An application to the court, supported by evidence "which clearly demonstrates that the interception of communications is necessary" may be made by the regulatory board or the ministries of justice, defence, or commerce. This law gives government powers to "do all such things as are necessary concerning telecommunications networks and telecommunications services as it ensures the preservations of the national integrity," such as interrupting private communications which "appear" dangerous to national integrity, contrary to the law, public order or public morals". Meanwhile, the penal code, and legislations on discrimination, sectarianism and genocide ideology broadly restrict freedom of expression. The penal code forbids defamation of the head of state or other public officials.

On the progressive front, following international criticism [45] of Rwanda's freedom of expression record, the government has taken positive steps to amend the genocide law. In July 2013, the Senate approved amendments to the law to include a less ambiguous definition of offenses and a requirement to prove criminal intent of a suspect. Sanctions were reduced from 25 years imprisonment to 9 years. As of March 2014, the president was yet to assent to the new law.[46]

Additionally, the 2013 Law Regulating Media[47] established the Rwanda Media Commission (RMC) as the media industry's self-regulatory body with the mandate to promote ethical

[44] *Law No.60/2013 Regulating the Interception of Communications, http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf*
[45] *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*
[46] *Draft Law on Genocide Ideology heads to State, http://www.newtimes.co.rw/news/index.php?a=68728&i=15421 and Senate Approve Genocide Law, http://www.africareview.com/News/Rwandan-senate-approves-amended-anti-genocide-law/-/979180/1932950/-/ddevp9z/-/index.html*
[47] *Law No.2/2013, http://www.rura.rw/fileadmin/laws/Media_Law_Official_Gazette_no_10_of_11_03_2013.pdf*

journalistic practices and defend media freedom. The commission has powers to enforce the journalistic code of ethics and to act as the primary and highest adjudicator of complaints against the media."[48] But in a move that sent mixed signals, in March 2014 the commission's head dismissed reports that there was no freedom of the press in Rwanda.[49]

In 2013 Rwanda enacted the Law Relating to Access to Information of 2013,[50] which outlines procedures and modalities for requests, receipt, copy and use of information in the possession of authorities. Information requests can be made in "writing, telephone, internet and other means of communication." However, the law has no provisions for response times to information requests. Article 11 states that an information officer takes a decision "according to priorities".

Nevertheless, internet users in Rwanda are reported to have become more vocal in criticising government agencies, particularly through social media. The country's president, Paul Kagame, is also an avid user of Twitter and has a following of over 300,000 users.[51] He often uses the platform to engage with users on governance issues. In 2012, Rwandans used Twitter to protest a decision by the Kigali City Council to close down a local entertainment venue. In the same year, in response to a United Nations report implicating Rwanda in the armed conflict in neighbouring Congo, Rwandans used the social media platform to circulate a petition against development aid cuts.[52]

However, some actions appear to negate the government's publically declared intentions on using ICT for development. From April 2012, the Media High Council (HMC)[53] reportedly started "systematic" monitoring of online media during the genocide period with the aim of "highlighting the civic contribution of the media during the commemoration period and discerning the extent to which media abide by legal and professional standards while covering genocide related issues."[54]

Some critical news websites that were previously blocked in 2010-2011 were intermittently inaccessible throughout 2012 and early 2013 and a number of critical blogs were unavailable altogether. Freedom House reports that it was unclear whether their unavailability was due to direct government interference or technical issues. There were reports that online news websites, Umusingi and Umurabyo, had been contacted by authorities to delete content related to local political affairs and ethnic relations. Umusingi and Inyereri – also an online news site - were reportedly blocked on some ISPs. The former was first blocked in 2011 but its content remained available via its Facebook page. The content of other websites that had been blocked over the years was accessible through their associated blogs.

[48] *http://igihe.com/IMG/pdf/rmc_tor_background.pdf*
[49] *James Karuhanga, Regulatory commission rebuts state of media report, The New Times, March 25, 2014; http://www.newtimes.co.rw/news/index.php?i=15672&a=75569*
[50] *Law No.4/2013, Relating to Access to Information, http://www.rura.rw/fileadmin/laws/Media_Law_Official_Gazette_no_10_of_11_03_2013.pdf*
[51] *Paul Kagame, https://twitter.com/PaulKagame*
[52] *The New Times, Twitter: 2012 was a very interesting year for 'RwOT", http://newtimes.co.rw/news/views/article_print.php?&a=13541&week=52&icon=Print*
[53] *The Media High Council, http://www.mhc.gov.rw/general-information/home.html was set up to advocate for media freedom, build capacity, participate in initiating and implementing policies and strategies to develop the media sector, and assist in creating an enabling environment for the development of the sector.*
[54] *Freedom House, Freedom on the Net and Freedom of the Press Annual Reports, http://www.freedomhouse.org*

Tanzania

Internet penetration continues to grow in Tanzania with the regulatory body reporting an increase in users from 7.5 million in 2012 to 9.3 million in 2013. With a teledensity of 61 phones per 100 inhabitants, mobile subscriptions stood at 27.6 million while fixed lines were at 607,822 as of December 2013.[55] However, many of the laws governing Tanzania's media and communications are outdated and woefully retrogressive. Moreover, while Tanzania has traditionally enjoyed more political stability than its East African neighbours and also been fairly more tolerant to the media, it has recently seen a steady decline in tolerance for press freedom and civic activists. Online media has not been spared.

In September 2013, two newspapers were shut down, with orders to stop publishing online. Mwananchi and Mtanzania were closed for two weeks and three months respectively on allegations of "publishing seditious stories that were allegedly aimed to provoke discontent between the government and public."[56] Mtanzania was sanctioned for writing stories that accused the government of not doing enough to prevent a recent spate of acid attacks in Zanzibar. One of Mwananchi's stories was about government salaries, based on leaked information, while another alleged that police had beefed up security at local mosques. The government felt this story was insulting to Tanzanian Muslims.[57] Tanzania's Director of Information, Assah Mwambene, said Mwananchi's stories intended to influence "citizens to lose confidence in state organisations."[58] While Mwananchi planned to continue publishing its online edition, it was told to stop the online edition as well under threat of further sanctions.[59]

Earlier in July, 2012, government indefinitely banned MwanaHalisi for allegedly publishing two seditious stories alleging that state intelligence officers were involved in the kidnap and torture of the Medical Association of Tanzania head, who had led a nationwide doctors' strike. The ban was cited under section 25 (1) of The 1976 Newspaper Act.[60] The online version of Mwanahalisi (http://www.mwanahalisi.co.tz/) remained accessible but was last updated in 2012. Human rights activists called for the amendment of the Act.[61]

In 2011, the Tanzania government was accused of cloning the JamiiForums website in an attempt to control content produced on that website, although the government refuted these allegations.[62] In February, 2009, the government had shut down one blog (www.zeutamu.com) for posting an allegedly doctored photo of the president and blackmailing prominent people. The blog owner, Malecela Peter Lusinde, was arrested and

55 *Tanzania Communications Regulatory Authority (TCRA), 2013 Telecom Statistics, http://www.tcra.go.tz/images/documents/telecommunication/telecomStatsDec13.pdf,*
56 *Media Council of Tanzania, "Press Release: Media Council condemns closure of two major newspapers;" http://www.mct.or.tz/index.php/component/content/artcle/62-press-release/257-media-council-condemns-closure-of-two-major-newspapers*
57 *Chris Oke, Tanzanian government bans nation's largest newspaper; http://speakjhr.com/2013/10/tanzanian-government-bans-nations-largest-newspaper/*
58 *Ibid 15*
59 *The Citizen, "Government now bans 'Mwananchi' website," october 02, 2013 http://www.thecitizen.co.tz/News/Government-now-bans--Mwananchi--website/-/1840392/2014814/-/item/0/-/ph66mgz/-/index.html*
60 *CPJ, 'Tanzanian authorities ban weekly indefinitely,' http://www.cpj.org/2012/07/tanzanian-authorities-ban-weekly-indefinitely.php, July 30, 21012*
61 *East African Horn of Human Rights Defenders, 'Civil society concern at ban of newspaper in Tanzania, http://www.defenddefenders.org/2012/08/civil-society-concern-at-ban-of-newspaper-in-tanzania/,*
62 *Karen Allen, 'African jitters over blogs and social media,' www.bbc.co.uk/news/world-africa-13786143#story_continues_1*

charged in Tanzania, although it was not clear under what law he was charged.[63] As of April 2014, the website was still accessible but its content was unrelated to the original content posted by Lusinde.

Earlier in February 2008, Maxence Mello and Mike Mushi, editors of Jambo Forums, a public discussion site with more than 2,000 members and 6 million hits, were detained and interrogated for 24 hours in Dar es Salaam, in what observers said was a politically motivated attempt to shut down their site. Although they were released after one day, police confiscated three computers used to host their website, shutting down the site for five days while the equipment remained under police custody.[64]

Like Kenya, Tanzania has been battling hate speech via ICT. In August 2013, the regulator, Tanzania Communications Regulatory Authority (TCRA), launched a social media campaign to curb hate speech and to promote "positive use" of ICT in the country. The campaign called "Futa Delete Kabisa" (Delete all hate messages) is aimed at reducing incitements through use of mobile phones, social media, radio, televisions and other channels of communication which the Authority said were threatening the country's peace. The campaign further "aims to promote self-regulation" and "discourage hate messages in all communication platforms."[65] According to the TCRA director general, Prof John Nkoma, even though the regulatory body "licenses internet service providers" it did not have regulations for bloggers.[66]

Article 18 of the Tanzanian Constitution[67] and Article 18 of semi-autonomous Zanzibar[68] guarantee the right to freedom of opinion and expression and the rights to seek, receive and impart information. However, in the absence of an access to information law, the National Security Act of 1970 is used to define what should be disclosed or withheld from the public.[69] The Act makes it a punishable offence to investigate, obtain, possess, comment on, pass on or publish any document or information the government considers to be classified. It also limits what public servants can reveal to the public and gives the minister responsible for information powers to prohibit the publication of any newspaper in the "public interest or in the interest of peace and good order." It further prohibits publishing of seditious content and publication of false news likely to cause fear and alarm to the public and incitement to violence.[70]

While the Act is meant for print media, it may apply to online media as many newspapers have digital versions. Critics consider this law to be needlessly restrictive and contradictory to the spirit of press freedom and freedom of expression. The minister's sweeping powers to ban newspapers on the pretext of protecting undefined "public interest" is another issue of concern.[71]

[63] *J. Nambiza Tungaraza (2009); 'Tanzania: Blogger arrested for publishing manipulated images of the president' Global Voices Online, http://globalvoicesonline.org/2009/06/19/tanzania-blogger-arrested-for-publishing-manipulated-images-of-the-president/*
[64] *Balancing Act (2009); Tanzanian Government detains two website editors; Issue no 395, http://www.balancingact-africa.com/news/en/issue-no-395/internet/tanzanian-government/en#sthash.AHUhqz7O.dpuf*
[65] *See https://www.facebook.com/pages/Futa-Delete-Kabisa/159279144263159?id=159279144263159&sk=info*
[66] *Anne Robi, TCRA Decries Bad Language in Networks, Daily News, August 1, 2013; http://archive.dailynews.co.tz/index.php/local-news/20614-tcra-decries-bad-language-in-networks*
[67] *The Constitution Of The United Republic Of Tanzania(Cap. 2), http://www.judiciary.go.tz/downloads/constitution.pdf.*
[68] *The Constitution of Zanzibar, http://www.wipo.int/edocs/lexdocs/laws/en/tz/tz028en.pdf*
[69] *Tanzania first introduced an Access to Information Bill in 2006 but it met fierce opposition from media activists who proposed an alternative bill. In 2013, deputy information minister Amos Makalla announced that more consultations were necessary before the Bill could be presented again. See: Kaijage, "Govt shatters hope on Right to Information Bill," February 02, 2013, http://www.ippmedia.com/frontend/index.php?l=50772*
[70] *See Section 36 (1) and Section 37*
[71] *The East and Horn of Africa Human Rights Defenders Project(2012); "Civil society concern at ban of newspaper in Tanzania," http://www.defenddefenders.org/2012/08/civil-society-concern-at-ban-of-newspaper-in-tanzania/*

The Electronic and Postal Communications Act (EPOCA) Consumer Protection Regulations 2010 and EPOCA Licensing Regulations, 2011 provide for mandatory registration of SIM cards. The afore-mentioned Consumer Protection Regulations and the Electronic[72] and Postal Communications (Computer Emergency Response Team) Regulations, 2011 criminalise unlawful disclosure of consumer data by service providers or their agents. However, the[73] Tanzania Evidence Act, 2007 provides for admissibility of electronic evidence in criminal cases.

Tanzania is going through a constitutional review process with the draft constitution now being debated by the Constituent Assembly. Section 29 regarding freedom of expression and 30 regarding freedom of information and the media, if passed in their current form, would extend the breadth of rights guaranteed to citizens. Also, government's announcement in April 2014 of plans to enact a Cyber Security Act, Data Protection Act and the Electronic Transacting Act by end of 2014 is a positive step for online users' security.[74]

With general elections set for late 2015 and the growing online political activism for electoral and other reforms by the country's growing online community, it can be expected that Tanzanian authorities will increasingly monitor what citizens do online and attempt to curtail independent and critical online voices. Watchdogs say a rise in attacks on the press is already sowing self-censorship among Tanzanian journalists.

[72] *TCRA (2011); "Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011," http://www.tcra.go.tz/images/documents/regulations/cert.pdf*
[73] *Evidence Act, 2007; http://www.tanzania.go.tz/egov_uploads/documents/EVIDENCE%20ACT.pdf*
[74] *IPP Media (2014); Data Protection and cyber laws ready by year-end, http://www.ippmedia.com/frontend/?l=67133, 21st April 2014*

Uganda

With seven mobile telecom operators and more than 30 Internet Service Providers, Ugandan ICT users have a variety of providers to choose from. Internet use stands at 20% of the population, while teledensity is 52 cellphones per 100 inhabitants.[75] Similar to Kenya, social media platforms such as Facebook, Youtube, Twitter and Blogspot are among the top ten most visited sites in Uganda. The country is run under a multi-party system with 38 registered political parties. President Yoweri Museveni's National Resistance Movement (NRM) has been in power since 1986, and in 2005, it orchestrated the removal of presidential term limits from the constitution.

Article 29(1)(a) of the country's constitution states that, "every person shall have the right to freedom of expression and speech which includes freedom of the press and other media". Meanwhile, Article 27 (2) of the constitution, states: "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

However, there are numerous laws passed between 2010 and 2014 that constrain freedom of expression on the internet as well as offline. In 2010, Uganda's parliament hurriedly passed the Regulation of Interception of Communications Act[76] following the terrorist attacks in Kampala in July of that year.[77] The law gives the ICT minister the powers to set up a monitoring centre which maintains connections with telecommunication systems.

Section 8 of the Act requires service providers to assistance in intercepting communication by ensuring that their telecommunication systems are technically capable of supporting lawful interception at all times. They are required to install software and hardware, ensure their services are capable of rendering real time and full time monitoring facilities, provide all call-related information in real time or as soon as possible upon call termination; and provide for more than one interface from which the intercepted communication shall be transmitted to the monitoring centre. Non-compliance is punishable by a fine not exceeding UGX 2,240,000 (US$960) or imprisonment for up to five years or both. Non-compliance could also lead to cancellation of an operator's license.

The Anti-Terrorism Act (2002)[78] gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance. 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. Under the anti-terrorism law, journalists who "promote terrorism" can be liable to capital punishment.

[75] *UCC, Status of Uganda's Communications Sector, April 30, 2014*
[76] *Regulation of Interception of Communications Act, 2010, http://www.ulii.org/content/regulation-interception-communications-act-2010*
[77] *The New Vision (2010), Over 40 die in Kampala bomb blasts; http://www.newvision.co.ug/D/8/12/725545, January 09, 2014*
[78] *"The Anti-terrorism Act No.14 of 2002, "http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf*

In February 2014, President Museveni assented to the Anti-Homosexuality Act, 2014 which prohibits any form of sexual relations between persons of the same sex. Section 13 outlaws the promotion of homosexuality, including by the use of "electronic devices which include internet, films, and mobile phones for purposes of homosexuality or promoting homosexuality." The penalty is UGX 100 million (US$ 40,000) or prison sentence of 5-7 years. Where the offender is a corporate body, association or NGO, on conviction its certificate of registration is cancelled and its directors and promoters are punishable by seven years imprisonment. This clause, according to some activists, may be used to crack down on organisational websites that work with sexual minorities in Uganda, as well as gay and lesbian websites. Furthermore, it is argued that this clause limits the ability of adult consenting homosexuals to use mobile phones freely as it criminalises even flirting or making dates.[79]

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. The Act calls for the setting up of a Pornography Control Committee whose functions include to "expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography."

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 service providers are obliged to take measures recommended by the Pornography Control Committee, including installing software to detect and censor pornography.

Uganda's ICT fraternity has criticised this law, arguing that service providers should be liable for removing illegal content hosted on their networks but not for content that merely flows through their networks. They also argue that best practice requires that in order to avoid infringing internet users' rights to freedom of expression and right to privacy, ISPs should only implement restrictions to these rights after judicial intervention. The law is also criticised for infringing on some principles of the internet, namely openness and privacy.[80] The liability, according to some, needs to only be placed on internet content developers, publishers or broadcasters who allow pornography, specifically child pornography, to be published to the public.

The anti-pornography law seems to contradict the Electronic Transactions Act, 2011, whose Section 39 provides that a service provider can be exempt from liability if they are "not directly involved in the making, publication, dissemination or distribution of the material or a statement made in the material." Furthermore, service providers are not required to monitor stored or transmitted data nor "actively seek for facts or circumstances indicating an unlawful activity."[81]

[79] *GenterIT.org, Uganda's Anti-Homosexuality Bill – a great blow to internet freedom, March 5, 2014. http://www.genderit.org/feminist-talk/uganda-s-anti-homosexuality-bill-great-blow-internet-freedom*
[80] *Wire. J (2014): "Brace yourselves Ugandan Internet Users," The New Vision, February 24, 2014 http://www.newvision.co.ug/news/293-blogger-brace-yourselves-ugandan-internet-users.aspx*
[81] *See Section 32 subsection (1) of the Act*

Uganda's Access to Information Act (2005) provides for the right of access to information as provided for in the constitution. However, even with the passing of the regulations for this Act - in 2011 - this law remains largely unimplemented due to lack of capacity and influence of accountability institutions, especially the civil society organisations and the media, to hold public bodies accountable. Retrogressive laws such as the Official Secrets Act have also practically barred public officials from proactive disclosure of public information due to fears associated with being held criminally liable for violating this Act.

While remaining averse to information openness, Uganda is taking a keen and manifestly negative interest in what its citizens are doing online. On May 30, 2013, the Uganda government announced that it would form a social media monitoring centre "to weed out those who use this media to damage the government and people's reputations" and also target those "bent to cause a security threat to the nation."[82]

Twice in 2011, the regulator, Uganda Communications Commission (UCC), ordered filtering of SMS content and a temporary shutdown of social media, the first time during a national election, the second during opposition protests.[83] Uganda is also among six African countries that asked Facebook to disclose users' details, according to the organisation's transparency report for the first half of 2013. Uganda made a second request in the second half of 2013. Both requests were denied.[84] Meanwhile, one journalist is on trial over an article published online in 2010 which suggested that the government may have had a hand in two bomb attacks that killed 76 people in the Ugandan capital in July of 2010.[85] These developments, along with recently passed laws and temporary closure of newspapers and radio stations, have prompted wide-scale self-censorship online by the media and citizens.

[82] CIPESA (2013); Uganda's Assurances on Social Media Monitoring Ring Hollow, http://www.cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow/
[83] CIPESA/ APC, Intermediary Liability in Uganda, April 2012, http://www.cipesa.org/?wpfb_dl=58
[84] Facebook Government request report (2013); Uganda, https://govtrequests.facebook.com/country/Uganda/2013-H2/
[85] The Daily Monitor, Journalist Timothy Kalyegira Arrested, http://www.monitor.co.ug/News/National/-/688334/1172464/-/c0wx5jz/-/index.html, May 31, 2011

Key internet freedom issues in East Africa

Flood of internet-related laws

In a number of countries, there are laws that curtail the enjoyment of freedoms of expression and association online. Governments in East Africa have, since 2009, enacted laws that provide for the interception of communications, place responsibility on internet intermediaries to monitor users and to block or take down content. These laws introduce or extend the reach of the law in regulating online content and activity. Many of the laws have been enacted in the last three years. The need to fight terrorism, cybercrime, and hate speech, has often been cited as motivating the enactment of these laws. However, evidence from the incidents where these laws have been invoked suggests that often the primary interest of authorities lies much closer to stifling legitimate expression than fighting terrorism and hate speech. Plans announced in 2013 to form a social media monitoring centre in Uganda, increased monitoring of internet users in Kenya during the election period; the regulation of political SMS in Kenya, new laws enacted in Burundi and Rwanda in 2013 that specifically regulate online content by journalists and bloggers; revamping of institutions with the mandate to monitor online communications in Ethiopia, and growing harassment of journalists in Tanzania, all point to increased action related to internet freedoms in East Africa. All five member countries of the East African Community (EAC) have completed registering SIM card owners, which could make monitoring and interception of telephone communications easier. Although registration of phone users is becoming a global trend, in East Africa it is a cause for worry due to the absence of data protection and privacy laws and given limited oversight in accessing users' data and instituting surveillance. As part of the registration exercises, personal user information including name, address and ID details were collected.

Interception of Communications

Lawful interception of communications is allowed in the countries studied, for purposes such as protecting national security, countering terrorism or fighting cybercrime. Uganda enacted its interception of communications law in 2010, Ethiopia in 2009, Rwanda in 2013, while in Burundi, the amended Code of Criminal Procedure 2013 provides for interception of communications. Kenya's Intelligence Service Act of 2012 provides for interception. In Ethiopia, the National Intelligence and Security Service (NISS) re-established in 2013 is heavily involved in surveillance and monitoring of citizens' online actions. The institution is mandated to conduct surveillance, using a court warrant, "in order to protect national security and prevent threats to national security" and can do this "by entering into any place and by employing various mechanisms." In Tanzania, communications can be intercepted under The Electronic and Postal Communications Act 2010, Section 91, which requires the TCRA to monitor and supervise all subscriber information. Although the various laws lay down the procedures for government interception of communications, evidence suggests that authorities sometimes take actions that do not follow the law. In Rwanda, interceptions for undefined "urgent" security matters can be conducted prior to the issuance of a written warrant.

There are wide variations in terms of actual monitoring, surveillance and filtering. Some countries, notably Ethiopia, have widespread, blatant and advanced monitoring, surveillance and filtering of content. Others, such as Tanzania and Uganda, do not appear to

be doing any filtering of content or active monitoring of what users do online. Burundi and Rwanda appear to be actively monitoring and, in the latter's case, intercepting communications considering recent actions against online publishers and instances of treason suspects whose digital communications were produced in court as evidence.

Access to Information: denied

The right to seek, receive and impart information and ideas, as well as freedom of the press and the right to information are enshrined in the constitutions of all the countries studied. However, as has been observed, there are various laws that negate these constitutional guarantees. Moreover, countries such as Kenya and Tanzania, both of which published access to information bills over seven years ago that would conceivably expand the breadth of citizens' right to information and freedom of expression, have dragged their feet on passing them. Ethiopia, Rwanda and Uganda have right to information laws but have not been enthusiastic in implementing them. In Uganda, even with the passing of the access to information regulations in 2011, citizens are routinely denied access to information.[86] Similarly, in Rwanda, the 2013 access to information law has no provisions for response times to information requests as an information officer is required to take a decision "according to priorities". Furthermore, some countries, such as Uganda and Tanzania, have laws dating to the colonial era, such as Official Secrets Acts and the Newspaper Act of 1976 (in Tanzania's case), which prohibit public officials from disclosing information that comes to them by virtue of the offices they hold.

Inadequate knowledge and skills on online safety

During workshops and online discussions conducted on the sidelines of this research, knowledge and skills about threats to online safety appeared to be widely lacking, including amongst bloggers, journalists and activists that regularly used the internet.[87] Many online users are prone to attacks and hacks into their private communication due to the lack of requisite skills to secure their communication and information. Similarly, there seemed to be a general lack of knowledge on what constituted online freedoms and what was needed to protect and to promote them.[88] This partly explained why there were few conversations on internet freedoms in the East Africa region. A final plank in the deficiency in knowledge and skills was related to online ethics among internet users.[89]

Lack of data protection and privacy laws

With the mandatory registration of phone users in all the six countries studied, it was noteworthy that none of them have data protection and privacy laws. Although governments in these countries were using the SIM card registration process under the pretext of enhancing national security, the absence of laws to safeguard user data and privacy could mean that government agencies could easily mishandle and misuse telecom services users' data. Besides, with the increase in the numbers of critical voices getting online and given the low levels of knowledge and skills on online safety and online ethics, it is likely that they could fall on the wrong side of the law. Some countries, notably Burundi, Kenya, Uganda and Tanzania have announced plans to draft privacy laws. However, none has made clear indications on the schedule for consultations, tabling and eventual passing of these laws.

[86] *Veit.P, et.l (2013), Improving Freedom of Information in Uganda, Veit.P, et.l (2013), http://www.wri.org/blog/improving-freedom-information-uganda;*
[87] *CIPESA (2013); Internet Rights in Uganda: Challenges and Prospects, http://www.cipesa.org/2013/12/internet-rights-in-uganda-challenges-and-prospects-workshop-report/*
[88] *CIPESA (2013): Exploring the State of Internet Freedom in Africa, http://www.cipesa.org/2014/03/exploring-the-state-of-internet-freedom-in-africa/*
[89] *Ibid. 96*

Emerging ambiguous regional regulatory frameworks

The African Union Convention on Cybersecurity and Personal Data Protection establishes a framework for cyber security in Africa "through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime." Civil society and academia have raised concerns about some of the articles in the convention, which was adopted on May 15, 2014 by African Union Justice ministers. An example of clauses that threaten internet freedoms is Article III – 34. It states that AU member states have to "take necessary legislative or regulatory measures to set up as a penal offense the fact of creating, downloading, disseminating or circulating in whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using a computer system." Some observers deem this clause to be problematic as it requires a measure of truth, which would be hard to legislate or determine owing to the relativity of truth.[90] Whereas the six countries included in this research are yet to make public declarations about the convention, it remains to be seen how individual states will implement it.

[90] *CIPESA, Report on African Union Cybersecurity Convention, http://www.cipesa.org/?wpfb_dl=71*

Recommendations

Amendments to laws and regulations

Governments should amend laws and regulations, particularly provisions that violate peoples' rights to freedom of expression and access to information across all media platforms. For instance, **Burundi** needs to remove heavy sanctions that are stipulated by the 2013 media law while **Rwanda** needs to amend the 2013 Rwanda Media Law to provide for a clear distinction between professional journalists and citizen journalists, including the rights and penalties applicable to the two kinds of journalists.

Ethiopia should amend The Anti-Terrorism Law 2009 [for example Sections 6 and 14], The Telecom Fraud Law 2012 [Sections4, 5, 6, 9, 15] and the NISS Re-establishment Proclamation 2013 [Article 27, Article 8 (7)] as they all detract from **the rights of citizens and contradict the constitution**. The revisions should extend the space for free expression by citizens without fear of reprisals from state authorities or non-state actors. Amendments should lower the powers of state organs in monitoring and investigating journalists and bloggers and also **lower the penalties**. Further the Telecom Fraud law in Ethiopia should be amended to allow free use of services such as VOIP.

The Interception of Communications laws in Uganda, Ethiopia and Rwanda should be revised to outline the modalities and procedures of interception, particularly when a telecommunications service provider does not facilitate it. Amendments should also include key provisions for **greater judicial and legislative oversights** over surveillance, including guidelines to be used in accessing individuals' data and monitoring communications, and circumstances under which courts of law can reject evidence gathered under conditions that flout laid-down regulations.

For all countries, the circumstances and laws under which individuals can be charged over their online activities need to be explicitly defined in the national legislation. Broad definitions of 'national security', 'terrorism', 'divisiveness', 'hate speech' and 'annoying messages' should not be acceptable grounds for taking action against citizens, journalists and bloggers that are expressing legitimate opinion both offline and online.

Laws and regulations must provide clear **delineation of the liability of intermediaries** and other parties in relation to filtering, removing and blocking content in all six countries. The steps to be followed in handling such content as well as appeal processes where there is an attempt to filter, remove or block a site or content also need to be clearly articulated in the legislation.

Tanzania, Kenya, and Burundi need to expedite the **enactment of access to information laws** to allow citizens' right of access to information and the free flow of information online. Ethiopia, Rwanda and Uganda need to **commit to the full implementation** of their access to information laws by encouraging proactive disclosure of information and putting in place structures and offices with competent information officers to facilitate free flow of information including online.

The Ethiopian **telecommunications sector should be liberalised** to promote pluralism and diversity so that users have increased options and better services. Having a single provider also bodes negatively for users' privacy since a centralised backbone and internet exchange makes it easier for the state to filter, monitor, and block internet access.

Tanzania should enact laws and regulations that **mirror the rapidly changing telecommunications technology.** Many of its laws related to communications are outdated (dating back to the 1970s) and retrogressive. Data and privacy protection, computer related fraud and crimes, access to information, security and privacy of e-transactions, all need to be addressed in new, progressive laws.

Respect privacy and data protection of online users: Whereas the privacy of communications is guaranteed by national constitutions, the absence of privacy and data protection laws calls for immediate enactment of laws that safeguard online users' privacy and data.

Skills building/ awareness raising

Widespread skills and knowledge development amongst users, activists, media and human rights defenders in staying secure online and in responsible user behaviour online (code of conduct and responsible journalism – both for citizen and professional journalists). While there is a need for the constant monitoring of violations, this should be countered with the **initiation and encouragement of conversations** amongst civil society, private sector, the media, religious organisations and government departments on what constitutes free speech and the distinction between blind control and respect for online free speech.

Build the capacity building for state organs and enforcement agencies to understand online freedoms so as to **investigate violation cases with a profound respect for users' freedoms.**

Strong advocacy for protection of users' digital rights and freedom of expression both online and offline needs to be undertaken by both civil society, media activists and ISPs.

Increased openness by state agencies

East African Governments should seek to meaningfully involve citizens, media and civil society organisations in the policymaking processes by holding **consultative meetings** with all stakeholders to get insightful inputs into these laws.

State agencies should **make public the findings of their investigations and prosecutions** into offences and crimes committed via digital technologies, as well as orders that may be issued to block websites or web content.

Notes

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) under the Open Net Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa. As part of the project, we are documenting internet rights violations, reviewing cyber security policies and how they affect internet freedoms, promoting information availability and conducting awareness-raising.

The production of this report was supported by the Humanist Institute for Co-operation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

Collaboration on International ICT Policy in 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