GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

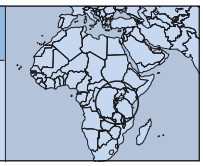
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

BURUNDI AND EAST AFRICA

Government surveillance in East Africa



Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
Lillian Nalwoga
www.cipesa.org

Introduction

Internet access and use of its related technologies continue to grow in East Africa. This can be partly attributed to the undersea cables that established landing sites along the Kenyan and Tanzanian coasts between 2009 and 2010,[1] consequently opening up the region to increased bandwidth and speeds. Other factors include a reduction in access costs and the proliferation of mobile phones.

Currently Kenya leads in internet access with 21.2 million users, or 52.3% of its total population,[2] compared to 8.67% in 2008,[3] while in Tanzania internet users were reported at 9.3 million at the end of 2013[4] compared to 4.9 million in 2010.[5] Meanwhile, internet usage also increased in landlocked Uganda, Rwanda and Burundi. By the end of 2013, Uganda's internet penetration stood at 20% compared to 12.5% in 2010, while that of Rwanda currently stands at 19.5%, having doubled from 2010. Meanwhile, Burundi and Ethiopia have the lowest proportion of internet users, at 1.32% and 1.5%[6] of the population, respectively.

Policy and political background

While East Africa has enjoyed relative stability, there have been cases of unrest in Burundi, Rwanda, Ethiopia, Uganda and Kenya in recent years. Tanzania continues to be the most peaceful country, while Kenya has recently been hit by terror attacks and earlier in 2007-2008, by election-based violence. The instability which the countries have experienced makes promoting national unity and national security, including fighting terrorism, pertinent concerns in the region. Despite this, the region has recognised that information and communications technologies (ICTs) can be used to advance governance and development. Governments in all these countries have enacted national ICT policies and other legal and regulatory frameworks to further facilitate and foster development in the digital age. Many of them have formed ICT Ministries – although they still make only negligible funding to these ministries and ICT development in general.

Between 2010 and 2014, various laws were introduced and have been criticised for curtailing online freedoms in these countries.[7] Often guised under the pretext of promoting national security and fighting cyber crime, these laws allow for interception of communications, censorship or the monitoring of online user activity. In many instances, the laws contradict the rights provided for in national constitutions.

All countries in East Africa have legal provisions, reinforced by state agencies, that enable the lawful surveillance and monitoring of communications. These include the Regulation of Interception of Communications Act, 2010 in Uganda; the Rwanda 2013 Interception of Communication Law and 2001 Law Governing Telecommunications; the Kenya Information and Communications (Amendment) Act 2013[8] and National Intelligence Service Act (Act No. 28 of 2012);[9] and the Prevention of Terrorism Act, 2002[10] in Tanzania. In Ethiopia, the Telecom Fraud Offence Proclamation No. 761/2012[11] allows for state moni-

1 Song, S. (2014, March). African Undersea Cables. *Many Possibilities*. https://manypossibilities.net/african-undersea-cables

2 Communications Commission of Kenya. (2013). Quarterly Sector Statistics Report: Second Quarter of the Financial Year 2013/14. www.ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q2%202013-14.pdf

3 www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

4 Tanzania Communications Regulatory Authority (2013). Telecom Statistics, www.tcra.go.tz/images/documents/telecommunication/telecomStatsDec13.pdf

5 www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

6 Ibid.

7 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

8 The Kenya Information and Communications Amendment Act 2013. www.cck.go.ke/regulations/downloads/KenyaInformationandCommunications_Amendment_Act2013_.pdf

9 Communication for Implementation of the Constitution. (2012). The National Intelligence Service Act, 2012. www.cickenya.org/index.php/legislation/acts/item/241-the-national-intelligence-service-act-2012

10 The Prevention of Terrorism Act, 2002. www.immigration.go.tz/downloads/Tanzania_Prevention%20of%20Terrorism%20Act%202002%20.pdf

11 Abyssinia Law. (2012). Telecom Fraud Offence Proclamation, No. 761/2012. www.abyssinialaw.com/uploads/761.pdf

toring of telecom subscriber information, and two agencies reconstituted in 2013 – the National Intelligence and Security Service (NISS) and Information Network Security Agency (INSA)[12] are actively involved in monitoring citizens' communications.

In Burundi, Article 29 of its 2013 Media Law makes it mandatory for news agencies, including online publications, to disclose certain information to the regulatory body, the National Communication Council (CNC). In Uganda, the Anti-Pornography Act, 2014 and Anti-Homosexuality Act, 2014 have been criticised for placing tough provisions on intermediaries regarding content hosted on their networks. Violators face hefty fines or even risk losing their licences.[13]

Ambiguous laws fuelling digital surveillance in East Africa

Internet rights violations in East Africa can be traced back as early as 2006 when the Ugandan government ordered the blocking of two websites. One of them, www.radiokatwe.com, a political news and commentary website, was accused of publishing anti-government gossip,[14] while the other, www.monitor.co.ug, the online version of the independent newspaper *Daily Monitor*, was temporarily blocked on the eve of the 2006 elections in a bid to stop it from publishing independent polling results.[15] Other governments have since then followed suit by frequently blocking or filtering website content deemed to be critical of their actions.

In Tanzania, at least five cases of website blocking and interference have been reported. In 2009, the www.zeutamu.com blog was shut down and its author was arrested for publishing allegedly doctored photos of the Tanzanian president, while in 2011 the Tanzanian government was reported to have tried to clone the website of jammiforums.com, a discussions group, in an attempt to control its content.[16] Earlier in 2008, the founders of Jammiforums, then called Jamboforums.com, were arrested and detained for one day, the website's computers were confiscated by the authorities, and their website was shut down for five days.[17] In October 2013, the Tanzanian newspaper *Mwananchi* was ordered to stop publishing online following a three-month ban over "seditious" content.[18]

Ethiopia has the most tightly controlled telecoms sector, and ranks lowest with regard to internet access. It, however, tops the list for having the most blocked websites in the region. These include the websites of human rights defenders, opposition parties, bloggers, news agencies – *Al Jazeera*, *Al Arabiya* and the *Washington Post* – and several social media platforms.[19]

In Rwanda, the government ordered the blocking of the website for the *Umuvugizi* newspaper in 2010.[20] It is also reported that several websites belonging to opposition members and other citizens deemed critical of the Rwandan government continued to be blocked between 2010 and 2013.[21] Burundi joined the league with one reported case involving the blocking of the comments section on www.iwacu-burundi.org, when the media regulator deemed some readers' comments to be a "threat to national security".[22]

State actors in some of these countries have made public announcements expressing their intention to monitor online users' communications. In Uganda, for instance, on 30 May 2013, the security minister announced plans to monitor "social media users who are bent to cause a threat to national security."[23] In the same year, Facebook reported that two requests were received from the Ugandan government regarding details of one its users.[24] Al-

12 chilot.files.wordpress.com/2013/10/national-intelligence-and-security-service-re-establishment-proclamation-english.pdf

13 APCNews (2014, May 19). New laws in Uganda make internet providers more vulnerable to liability and state intervention. *APCNews*. https://www.apc.org/en/news/new-laws-uganda-make-internet-providers-more-vulne; Nafuka, J. (2014, April 22). New laws in Uganda restrict citizens' rights. *CIPESA*. www.cipesa.org/2014/04/new-laws-in-uganda-restrict-citizens-rights

14 Privacy International. (2006). *Uganda: Privacy issues*. https://www.privacyinternational.org/reports/uganda/iii-privacy-issues

15 The Monitor (2006, February 26). Government jams Monitor radio, site. *UPC*. www.upcparty.net/memboard/election7_260206.htm

16 Allen, K. (2011, June 16). African jitters over blogs and social media. *BBC News*. www.bbc.co.uk/news/world-africa-13786143#story_continues_1

17 Balancing Act. (2008). Tanzanian Government detains two website editors. *Balancing Act*. www.balancingact-africa.com/news/en/issue-no-395/internet/tanzanian-government/en#sthash.AHUhqz7O.dpuf

18 The Citizen. (2013, October 1). Government now bans 'Mwananchi' website. *The Citizen*. www.thecitizen.co.tz/News/Government-now-bans--Mwananchi--website/-/1840392/2014814/-/item/0/-/ph66mgz/-/index.html

19 CIPESA. (2014). *State of Internet Freedoms in Ethiopia 2014*. opennetafrica.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Ethiopia%202014.pdf

20 Reporters Without Borders. (2010, June 11). Persecution of independent newspapers extended to online versions. *Reporters Without Borders*. en.rsf.org/rwanda-persecution-of-independent-11-06-2010,37718.html

21 Freedom House. (2013). *Freedom on the Net 2013*. http://freedomhouse.org/report/freedom-net/2013/rwanda#.U9KP9rH8uoM

22 Reporters Without Borders. (2013, May 31). Burundi - Media regulator suspends comments on press group's website. *Thomson Reuters Foundation*. www.trust.org/item/20130531164503-qium7/?source%20=%20hppartner

23 CIPESA. (2013, June 10). Uganda's assurances on social media monitoring ring hollow. *CIPESA*. www.cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow

24 https://govtrequests.facebook.com/country/Uganda/2013-H2

though both requests were rejected by Facebook, the state-owned newspaper *Sunday Vision* reported that a former head of political intelligence in the president's office was arrested on suspicion of being the owner of the Facebook account "Tom Voltaire Okwalinga", which is strongly critical of the government.[25]

In Burundi, Ethiopia and Rwanda, online users are constantly intimidated and arrested over content posted online, often cited as threatening national security or inciting violence among the public. Ethiopia has been faulted by many digital rights defenders and to date tops the list of African countries that are constantly intimidating, monitoring, intercepting communications and issuing criminal sanctions against users who post content online.[26] In April 2014, six members of the blogging group "Zone9" and three freelance journalists associated with the group were arrested following accusations of working with foreign organisations and rights activists through "using social media to destabilise the country."[27] Rwanda is also reported to actively intercept communications, as was seen in 2012 when records of emails, phone calls and text messages of opposition activists were produced in court as evidence.[28] Another incident was recorded in April 2014, when private messages exchanged via WhatsApp and Skype between a local journalist and musician were produced as evidence in court during a treason trial.[29]

According to research conducted by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), in Kenya, Tanzania, Burundi and Rwanda, governments' interest in citizens' social media activity has also been motivated by the need to combat online hate speech. Although hate speech is a genuine concern, measures taken to combat it are often said to violate online user privacy and freedom of expression.[30] Kenya is reported to have blocked access to one website, www.mashada.com, for its failure to moderate hate speech ahead of the 2013 elections.[31] In 2013, the Kenyan government was also looking for 14 bloggers for allegedly posting hate speech messages, with one arrested and charged under Section 29(b) of the Kenya Information and Communications Act, 2013, for posting an "offensive tweet".[32]

Kenya, Tanzania and Uganda have each been reported to have made requests to internet intermediaries to release information on particular users' details. In 2012, Google listed Kenya among the eight African countries which had requested particulars about its users. The Kenyan request, which was rejected, involved the removal of content from a blogger site following a court order in a defamation case.[33] Similarly, in the last quarter of 2013, Kenya topped the list of African countries that made requests to the search company. A total of eight requests were made, with Google fully or partially complying with 63% of these.[34]

Telecom giant Vodafone, in its first Law Enforcement Disclosure Report released in June 2014, revealed that the governments of Kenya and Tanzania actively monitored its subscribers' communications by issuing data requests to the telecom companies.[35] Tanzania was reported to have made the highest number of requests in all of the African countries for which Vodafone provided statistics – 98,785 requests. Statistics about requests made in Kenya could not be revealed due to legal restrictions in the country.[36] Lawful interception of communications is provided for in Tanzania under Section 9 of the Electronic and Postal Communications Act 2010 and Section 31 of the Prevention of Terrorism Act, 2002; and in Kenya under the National Intelligence Service Act, 2012, and Section 27 of the Kenya Information and Communications (Amendment) Act 2013. However, Vodafone also noted that it had

25 CIPESA. (2014). *State of Internet Freedoms in Uganda 2014*. opennetafrica.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Uganda%202014.pdf

26 CIPESA. (2014). *State of Internet Freedoms in Ethiopia 2014*. opennetafrica.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Ethiopia%202014.pdf

27 Addis Standard. (2014, April 28). Ethiopia files charges against a group of bloggers, journalists detained over the weekend. *AllAfrica*. allafrica.com/stories/201404281454.html

28 Freedom House. (2013). Op. cit.

29 The East African. (2014, April 26). Phone evidence used in terror, treason case. *The East African*. www.theeastafrican.co.ke/news/Phone-evidence-used-in-terror/-/2558/2294196/-/klwpvi/-/index.html

30 CIPESA. (2014). State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa. www.cipesa.org/?wpfb_dl=76

31 Diaspora Messenger. (2013, January 30). Kenya's popular forum Mashada.com shut down in hate speech Crackdown. *Diaspora Messenger*. diasporamessenger.com/kenyas-popular-forum-mashada-com-shut-down-in-hate-speech-crackdown

32 Jambo. (2013, May 15). Robert Alai arrested for alleged "libelous" twitter post. *Jambonewspot.com*. www.jambonewspot.com/robert-alai-arrested-for-alleged-libelous-twitter-post/

33 CIPESA. (2013, September 9). Online freedoms under siege as African countries seek social media users' information. *CIPESA*. www.cipesa.org/2013/09/online-freedoms-under-siege-as-african-countries-seek-social-media-users-information/#more-1623

34 Google. (2013). Google Transparent Report – Kenya. http://www.google.com/transparencyreport/userdatarequests/KE/

35 Vodafone. (2014). Law Enforcement Report. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

36 Kalemera, A., & Nanfuka, J. (2014, July 2). Vodafone reveals government requests for subscriber information. OpenNet Africa. opennetafrica.org/vodafone-reveals-government-requests-for-subscriber-information

not received any demands for technical assistance to enable interception of communications in these countries.[37]

Conclusions

The increase in internet access speed, reduction in internet costs and proliferation of easy-to-use digital tools have led to a shift in the way citizens and governments engage with each other and share information in East Africa. However, this is being threatened by clauses in legal and regulatory frameworks in these countries.

Although there is indeed cause for governments to protect national security and fight cyber crime, creating a balance between promoting national security and protecting internet rights, including the rights to information, freedom of expression, privacy and data protection, is becoming controversial in many respects. As seen in the cited violations, legal frameworks are being used to arrest, intimidate, monitor and intercept communications of sometimes innocent online users expressing legitimate opinions. Moreover, the legal frameworks often curtail constitutionally guaranteed rights. It is also feared that these laws and their associated violations are triggering self-censorship, a practice that may limit internet growth and have a chilling effect on freedom of association, even in the offline world, in these countries.[38]

In all the six focus countries, data protection and privacy laws do not exist, despite mandatory user registration exercises for voice and data communications and lawful interception of communications. This is coupled with a general lack of knowledge on what constitutes internet freedoms and limited capacity and skills by both state and non-state actors to safeguard internet freedoms.[39]

Action steps

An urgent call to advocate for the amendment of laws and regulations that curtail freedom of expression online, user privacy and the right to information needs to be made in all these countries. Countries should commit to the implementation of progressive laws that allow for the enjoyment of internet rights. There needs to be a push for meaningful multi-stakeholder participation in policy-making processes to deter the passage of regressive laws.

Capacity building for both state and non-state actors needs to be undertaken to empower them with the necessary knowledge and skills on internet rights. This will allow state actors to understand what constitutes internet rights so that they are better placed to handle cases arising from perceived violations. Non-state actors including human rights activists, digital rights defenders, bloggers and journalists need capacity development in the area of digital safety. Among other things, they need skills to better understand legal provisions so that they do not fall on the wrong side of the law.

There is a need for more openness from all actors – including state agencies, telecom companies and content hosts – in disclosing information about online freedom violations. State agencies should become more transparent by sharing findings from investigations and prosecutions of digital offences with the public. All telecom companies should take Vodafone's lead by revealing all government requests for intercepting, monitoring or censoring communications. This will serve as a best practice and also create more awareness about state surveillance.

37 Vodafone. (2014). Country-by-country disclosure of law enforcement assistance demands. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

38 CIPESA. (2014). State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa. www.cipesa.org/?wpfb_dl=76

39 Ibid.