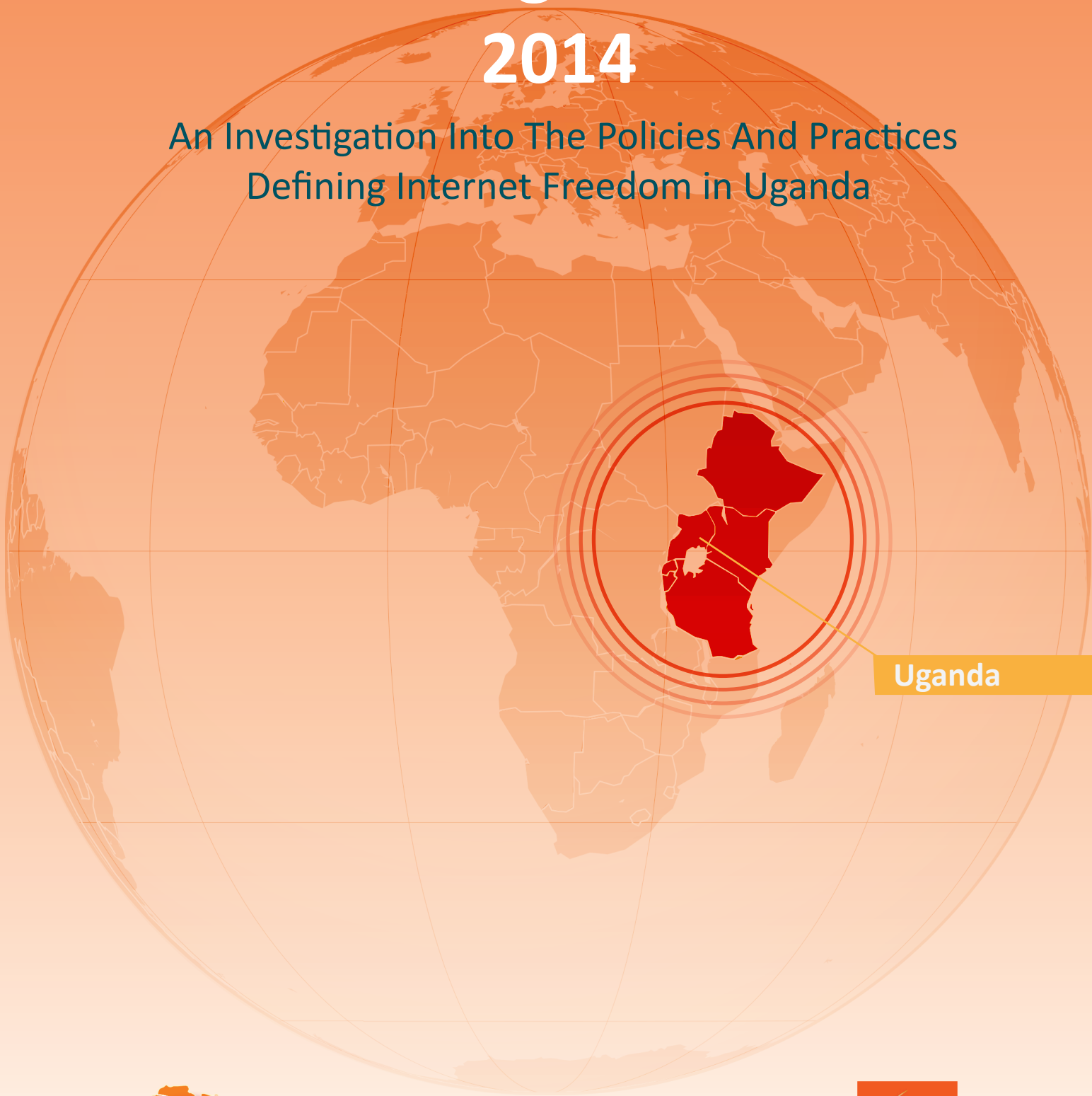
State of Internet Freedoms in Uganda 2014

An Investigation Into The Policies And Practices Defining Internet Freedom in Uganda



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 was produced as part of CIPESA's internet freedoms monitoring initiative, OpenNet Africa. Other country reports have been written for Burundi, Ethiopia, Kenya, Rwanda, Tanzania, and South Africa. The country reports, as well as a regional 'State of Internet Freedoms in East Africa' report, are available at www.opennetafrica.org.

State of Internet Freedoms in Uganda 2014
Published by CIPESA
May 2014

Content

Introduction

Uganda is a landlocked country with an estimated population of 36.3 million people[1] and a per capita income of US$ 506.[2] The country is run under a multi-party system with 38 registered political parties.[3] The National Resistance Movement (NRM) has been the ruling party since 1986 and in 2005 it orchestrated the removal of presidential term limits from the constitution. President Yoweri Museveni has been in power since 1986, and although elections are held regularly, the opposition often alleges that elections are rigged. Despite civil unrest experienced between the late 1970s and early 1990s, the country is largely stable today.

In recent years, Uganda has experienced several corruption scandals ranging from bribery to embezzlement of public and donor funds. Voices critical of government are often curtailed, including through contentious laws such as the Public Order Management Act, 2013, which some observers believe is meant to inhibit freedom of expression and assembly.[4]

Uganda has passed a number of laws to improve access to information, deal with cybercrime and regulate telecommunications. However, some of these laws negate citizens' online freedoms. The Regulation of Interception of Communications Act, 2010, which authorises lawful interception of communications, for instance, is unclear as to how data collected from citizens would be used and how citizens' privacy would be protected. The establishment under this law of a monitoring centre to collect users' data and government's plans to "monitor social media users who are bent to cause a security threat to the nation"[5] bode negatively for the right to freedom of expression and opinion. Lack of a data and privacy law means government agencies can mishandle and misuse telecom services users' data.

On a positive note, in January 2014 the information minister announced that drafting of a Data Protection and Privacy Bill was underway. The proposed law will aim to safeguard the rights of individuals during data collection and processing by government, public institutions and private entities.[6] However, Uganda is already overloaded with legislation that encumbers online freedoms – some of it enacted in 2014 - while those which promote these freedoms are hardly implemented.

1 *World Bank, Uganda country at a glance (2012), http://data.worldbank.org/country/uganda*
2 *World Bank (2014), Uganda Overview, http://www.worldbank.org/en/country/uganda/overview2013*
3 *Electoral Commission, Registered Political Parties; http://www.ec.or.ug/regdparty.php*
4 *The Act regulates public meetings and specifies the duties of the police as well as meeting organisers and participants. It has been criticised for restricting Uganda's right to freedom of expression. See for instance, FIDH, Uganda's Constitutional Court should repeal the Public Order Management Act as unconstitutional, http://www.fidh.org/en/africa/uganda/14422-uganda-s-constitutional-court-should-repeal-the-public-order-management*
5 *Emorut F., Gov't plans to monitor social media, The New Vision, May 31, 2013 http://www.newvision.co.ug/news/643403-gov-t-plans-to-monitor-social-media.html*
6 *Frederic Musisi, Cabinet approves Bill to protect phone records, The Daily Monitor, http://www.monitor.co.ug/News/National/Cabinet-approves-Bill-to-protect-phone-records/-/688334/2158008/-/159t075z/-/index.html, January 24 2014*

Background to ICT Usage

Since the liberalisation of the telecommunications sector in 1998, Uganda has registered notable growth with four major mobile telecom operators and more than 30 Internet Service Providers (ISPs).[7] Internet use stands at 20% of the population, while teledensity is 52 cellphones per 100 inhabitants.[8]

The Rural Communications Development Fund (RCDF) run by the Uganda Communications Commission (UCC) aims to ensure quality communications services are accessed at affordable prices in rural and under-served areas. The fund has financed the setup of 76 Internet Points of Presence, 106 internet cafes and 78 Multi-Purpose Community Tele-centres, 78 District web portals, 708 School ICT laboratories, and provided internet connectivity to over 300 projects across the country.[9] Meanwhile, the National Data Transmission Backbone Infrastructure and e-Government Project implemented by the National Information Technology Authority of Uganda (NITA-U) will connect all major towns to the optical fibre cable, and to the national data centre set up in Kampala. Implementation started in 2007 and as of May 2014, some 1400 kilometres of fibre optic cables have connected 22 district headquarters.[10]

However, ICT uptake is hampered by the poor spread of infrastructure, low literacy levels, high cost of access, and minimal local content online. The high cost of accessing internet in Uganda is partly because being landlocked, Uganda has to build or pay for backhauling costs through Kenya and Tanzania in order to access fibre cables at the Indian Ocean coast. The price averages UGX 500 (US$0.2) for 50MB of mobile broadband or UGX 1,000 (US$0.4) for 40 minutes of Internet use in internet cafes. These prices are still high considering that 24.5% of Ugandans live on less than US$2 a day.[11]

Local and international online content can be accessed in Uganda without restriction. Filtering tests conducted by the Citizen Lab and the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) in Uganda during 2013 on up to 1,413 websites hosted locally and internationally found no evidence of website blocking.

Ominously, the security minister said in May 2013 that government would start monitoring "social media users who are bent to cause a security threat to the nation."[12] "National security" is described by the Anti-Terrorism Act as matters relating to the existence, independence or safety of the State and constitutes one of the grounds for lawful interception of communications. According to Alexa.com, social networking sites such as Facebook, twitter, LinkedIn, Youtube and Blogspot are among the top 10 most visited websites in Uganda. The Uganda government has drafted social media guidelines to be followed by public bodies while communicating and engaging with citizens.[13]

7 *Uganda Communications Commission (UCC), Licensees in Uganda, http://www.ucc.co.ug/files/downloads/licensedProviders.pdf*
8 *UCC, Status of Uganda's Communications Sector, April 30, 2014*
9 *UCC, Rural Communication Development Fund Statistics, http://ucc.co.ug/data/smenu/25/1/About%20RCDF.html*
10 *NITA- U, NBI/EGI Project, http://www.nita.go.ug/index.php/projects/nbiegi-project*
11 *World Bank, Development Indicators, Uganda, http://data.worldbank.org/country/uganda*
12 *OpenNet Africa, Uganda's Assurances On Social Media Monitoring Ring Hollow, http://opennetafrica.org/ugandas-assurances-on-social-media-monitoring-ring-hollow/*
13 *NITA –U, NITA-U Develops Guidelines for Social Media, http://www.nita.go.ug/index.php/features/315-socialmediguide ; and OpenNet Africa, Q&A: Uganda Government Develops Social Media Guidelines, http://opennetafrica.org/qa-uganda-government-develops-social-media-guidelines/*

Relevant Agencies

The Uganda Communications Commission (UCC) was established in 1997 with the aim of developing a modern communications sector in Uganda. The Commission's mandate involves licensing and developing standards, spectrum management, tariff regulation, research and development; consumer empowerment, policy advice and implementation, rural communications and development.[14] The Commission has come under criticism over lack of independence from the ICT minister. The Uganda Communications Act, 2013 gives powers to the minister to appoint the commission's executive director and board members and to approve its budgets.

Some observers claim it is hard to access comprehensive and coherent information about the commission's operations. Furthermore, the leadership of the commission has been described as "overzealous" in "efforts to police and rein in operators, illustrating how the personal character of the regulatory authority's leadership can in large measure determine its activities and regulations." [15] The current Executive Director headed the Uganda Broadcasting Council from 1998 to 2010.[16]

The National Information Technology Authority – Uganda (NITA-U) is an autonomous statutory body established under the NITA-U Act, 2009[17] to coordinate and regulate information technology services in Uganda. Amongst its functions is the co-ordination and monitoring of the utilisation of information technology in the public and private sectors; set and regulate standards for information technology planning, acquisition, implementation, disposal, risk management, data protection, and security; and regulation of the electronic signature infrastructure and other related matters as used in electronic transactions in Uganda.

The Uganda Media Centre (UMC) is the government's official public relations department charged with disseminating "factual information" concerning the Government of Uganda.[18]

Uganda Internet Exchange Point (UIXP) provides high-speed Internet traffic (IP traffic) exchange facilities for Uganda and external entities. It aims to reduce operational costs for ISPs, spur competition among ISPs leading to a drop in prices for consumers, improve reliability and performance, leading to cost benefits to end users, and to create new local internet bandwidth in the local market. Currently, 14 ISPs are connected to the UIXP.

14 *Uganda Communications Commission (UCC), Overview and Mandate; http://ucc.co.ug/data/smenu/5/Overview-and-Mandate.html*
15 *Freedom House, Uganda Freedom on the Net 2013 Report, http://www.freedomhouse.org/report/freedom-net/2013/uganda#.Us6kI_vsV-Y*
16 *Godfrey Mutabazi | Executive Director; http://www.ucc.co.ug/data/cddetails/1/Mr-Godfrey-Mutabazi.html*
17 *National Information Technology Act of Uganda (2009), http://www.nita.go.ug/uploads/NITA-U%20Act%20(Act%20No.%204%20of%202009).pdf.*
18 *About Uganda Media Center, https://www.facebook.com/UgandaMediaCentre/info and http://www.gov.ug/media-center*

Policy and Regulatory Environment

Uganda has laws that provide for freedom of expression, right to access information and freedom of the press. Article 29 (1)(a) of the Constitution of Uganda 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 that "no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."[19] In 2011, Uganda enacted three cyber laws, namely the Electronic Signatures Act, 2011, the Electronic Transactions Act, 2011 and the Computer Misuse Act, 2011. These laws aim to promote online safety. A law on anti-pornography and another on anti-homosexuality, both enacted more recently in 2014, undermine internet freedoms. An analysis of how some of these laws impact freedom of expression and internet freedom is provided below.

Access to Information and Freedom of Expression

The Access to Information Act, 2005[20] provides for the right of access to information pursuant to Article 41 of the Constitution, which states that "every citizen has a right of access to information in the possession of the state or any other organ of the state except where the release of the information is likely to interfere with the security of the state or the right to the privacy of any other person". The Act prescribes the classes of information and the procedure for obtaining access to that information. It applies to information and records of government ministries, departments, local governments, statutory corporations and bodies, commissions and other government organs and agencies. However, cabinet records and those of its committees, as well as records of court proceedings before the conclusion of the case, are exempted.

In spite of having this law in place, obtaining information from government agencies is inhibited by Article 4 of the Official Secrecy Act of 1964, which prohibits public servants from disclosing information that comes to them by virtue of the offices they hold. Breach of the Act could earn a civil servant up to 14 years in prison.[21] Moreover, even with the passing of the access to information regulations in 2011, citizens are routinely denied access to information.[22] The Hub for Investigative Media (HIM)[23] reports that of the 21 information requests it made to government agencies in 2013, only 14% were granted. 28% were denied and 57% were still pending as of the end of 2013.[24] These limits to access to information negate freedom of expression as users cannot easily access and utilise government information to express their opinions online.

Meanwhile, the Anti-Homosexuality Act 2014,[25] assented to by President Museveni on February 20, 2014, 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

19 *Freedom of Expression in Uganda, http://www.ulii.org/files/ug/judgment/constitutional-court/2005/6/6_0.pdf*
20 *Access to Information Act, 2005, http://www.freedominfo.org/documents/uganda_ati_act_2005.pdf*
21 *Official Secrecy Act of Uganda, 1964, http://www.ulii.org/ug/legislation/consolidated-act/302*
22 *World Resources Institute, Improving Freedom of Information in Uganda, http://www.wri.org/blog/improving-freedom-information-uganda*
23 *Hub for Investigative Media (HIM) is an organization that was conceived to promote investigative media toward good governance and accountability in Uganda, www.him.or.ug; and Mobile Monday Kampala (MoMoKla), Slides – Open Data - Pioneers Tell Their Stories, Putting ATIA to the Test - Experiences from an Investigative Reporter, http://momokla.ug/downloads/Putting%20ATIA%20to%20the%20Test%20-%20Experiences%20from%20an%20Investigative%20Reporter%20by%20Edward%20Sekyewa.pdf*
24 *HIM, Information Requests, http://www.him.or.ug/information-request*
25 *Anti-Homosexuality Act, 2014, http://cryptome.org/2014/02/uganda-anti-gay.pdf*

devices which include internet, films, and mobile phones for purposes of homosexuality or promoting homosexuality." The penalty is UGX100 Million (US$ 40,000) or minimum five years and maximum seven year jail sentence. Where the offender is a corporate body, association or NGO, on conviction its certificate of registration shall be 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, they argue that this clause limits the ability of adult consenting homosexuals to use mobile phones freely as, by implication, "it criminalises even flirting or making dates."[26]

The Uganda Communications Act 2013[27] consolidates the Uganda Communications Act of 2000 and the Electronic Media Act of 1996. It merged the Uganda Communications Commission and the Broadcasting Council into one body known as the Uganda Communications Commission. Among the body's functions are the monitoring, inspecting, licencing and regulation of communication services.

Under Section 86 subsection 1 (a), the Act gives power to the commission to "direct any operator to operate a network in a specified manner in order to alleviate the state of emergency."

As explained in the internet freedom violations section below, in the past the regulator used these powers to issue directives to service providers to temporarily block access to certain services such as Facebook and Twitter and to filter content. Recently, there has been an increase in the number of directives by the regulator ordering radio broadcasters not to air programmes deemed to host 'abusive' political commentators.[28] The law provides for the creation of the Uganda Communications Tribunal, which has "jurisdiction to hear and determine all matters relating to communications services arising from decisions made by the Commission or the Minister."[29] The tribunal has powers equivalent to those of the High Court. However as of May 2014, the tribunal had not been created.

Unlike recent laws in countries such as Rwanda and Burundi that explicitly define ICT and the internet or web technologies, Uganda's new communications law does not. Instead, a general term "telecommunications" caters for all ICT related technologies.

Privacy and Data Protection

Sections 79 and 80 of the Communications Commission Act, 2013 criminalise infringing privacy and provide for the punishment of unlawful interception and disclosure of communication by a service provider. The Computer Misuse Act, 2011[30] also upholds individuals' right to privacy of communications. It provides for the safety and security of electronic transactions and information systems, and criminalises unauthorised access to computer systems and data.

[26] *GenderIT, Uganda's Anti-Homosexuality Bill – a great blow to internet freedom, http://www.genderit.org/feminist-talk/uganda-s-anti-homosexuality-bill-great-blow-internet-freedom*
[27] *Uganda Communications Act, 2013, http://www.ucc.co.ug/files/downloads/UCC%20Act%202013.pdf*
[28] *Daily Monitor Uganda, UCC suspends two radio talk shows, http://www.monitor.co.ug/News/National/UCC-suspends-two-radio-talk-shows/-/688334/1659788/-/kkpm7xz/-/index.html*
[29] *UCC Act (2013); Section 64 (1)*
[30] *The Computer Misuse Act, 2011, http://www.nita.go.ug/uploads/Computer%20Misuse%20Act%20%28Act%20No.%202%20of%202011%29.pdf*

Section 18 of the Computer Misuse Act protects user privacy by specifying circumstances under which unauthorised disclosure of information (defined as "data, text, images, sounds, codes, computer programs, software and databases") is punishable. Sub-section 1 states: "Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access." An offense under this section is punishable upon conviction with a fine not exceeding UGX 4 million (US$1,600), imprisonment not exceeding 10 years or both.

However, Section 28 subsection 5 (c) gives powers to an authorised officer executing a search warrant to "compel a service provider, within its existing technical capability - (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorities in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system."

The Regulation of Interception of Communications Act, 2010[31] commonly known as the 'phone tapping law' provides for lawful interception and monitoring of communications in the course of their transmission through telecommunications, postal or any other related services or systems in Uganda. The law was hurriedly passed by parliament following the terrorist attacks by Al Shabaab militants in Kampala in July 2010.[32] Under Section 3, it gives the ICT minister the powers "to set up a monitoring centre, equip, operate and maintain the centre, acquire, install and maintain connections between telecommunication systems and the Monitoring Centre; and administer the Monitoring Centre at the expense of the state." The law requires the ICT minister to appoint officers to run the centre. The persons allowed to apply for lawful interception are the Chief of Defence Forces, the Director General of the External and Internal security agencies, and the Inspector General of Police.

Under Section 5 subsection (1) (c) (d) &(e), lawful interception is granted after issuance of a warrant by a judge if "there is an actual threat to national security or to any national economic interest, a potential threat to public safety, national security or any national economic interest, or if there is a threat to the national interest involving the State's international relations or obligations." Whereas the Act defines 'national security of Uganda' to include matters relating to the existence, independence or safety of the State, it does not define what 'national economic interests' are.

Section 8 of this Act requires service providers to provide assistance in intercepting communication by ensuring that their telecommunication systems are technically capable of supporting lawful interception at all times.[33] Non-compliance by service providers is punishable by a fine not exceeding UGX2.24 million (US$896) or imprisonment for a period not exceeding five years or both. Non-compliance could also lead to cancellation of an operator's license.

31 *Regulation of Interception of Communications Act, 2010, http://www.ulii.org/content/regulation-interception-communications-act-2010*
32 *The New Vision, Over 40 die in Kampala bomb blasts; http://www.newvision.co.ug/D/8/12/725545*
33 *Article 18 requires service providers to install software and hardware facilities and devices, 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 for termination; provide for more than one interface to from which the intercepted communication shall be transmitted to the monitoring centre; and to ensure intercepted communication are transmitted to the monitoring center via fixed or switched connection. Service providers are also required to provide access to all interception subjects operating temporarily or permanently within their communications systems and where possible provide the capacity to implement simultaneous interceptions.*

To facilitate the enforcement of the Act, the personal information of subscribers has to be registered. This includes the subscriber's full name, residential address, business address, postal address and identity number. Failure to disclose the required information is an offence punishable by a fine of UGX 2.4 million (US$960) or imprisonment for a period not exceeding five years, or both.

The mandatory registration of all SIM card holders kicked off in March 2012 and concluded in August 2013 with 92% of SIM cards reported as registered.[34] This exercise attracted criticisms from human rights defenders who claimed it could curtail freedom of expression and the right to privacy, and violated Article 27 of the Constitution which guarantees the right to privacy.[35] Although a human rights group filed a suit against the mandatory registration on the grounds that it violated constitutional guarantees on privacy, court dismissed the challenge.[36]

The Regulation of Interception of Communications Act was enacted to effectuate the Anti-Terrorism Act No.14 of 2002.[37] The anti-terrorism law 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. Section 19 of the Anti-Terrorism Act lists purposes for which interception or surveillance may be conducted as: safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism.

Failure to comply with interception and surveillance under this Act is an offence. A person who knowingly obstructs an authorised officer in the carrying out of his or her functions commits an offence and is liable, on conviction, to imprisonment not exceeding two years or a fine not exceeding UGX2 million (US$800) or both as per Section 20.

The "broad and undefined basis for interception of communication" under the law on interception has been criticised "for possible intrusion into communications of individuals and professionals – such as journalists, human rights defenders and political dissidents engaged in legitimate activities and exercising their human rights."[38]

In July 2012, a ministerial policy statement released by the Office of the Presidency for the financial year 2012/2013 stated that the government was looking for UGX205 billion (US$ 82million) for the purchase of equipment to establish systems for the interception of communication.[39] The said funds would be channelled through the Internal Security Organisation, which would work closely with the Office of the President to implement the surveillance. However, the statement did not give details of the nature or type of equipment to be purchased or a breakdown of how the money would be spent.[40] The National Budget

34 *UCC wins SIM card registration case, http://ucc.co.ug/data/dnews/3/UCC-wins-SIM-card-registration-case.html*
35 *IFEX News, Law requiring registration of SIM cards in Uganda a threat to privacy, http://www.ifex.org/uganda/2012/09/24/sim_card_registration/*
36 *IFEX News, Ugandan court declines to hear SIM card registration case, http://www.ifex.org/uganda/2013/12/19/case_closes/*
37 *The Anti-terrorism Act No.14 of 2002, http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf*
38 *ARTICLE 19's Submission to the UN Universal Periodic Review; www.article19.org/pdfs/submissions/uganda-upr-submission.pdf*
39 *Government of Uganda, Office of the Presidency , MPS 2012-2013 Presidential Final - Office of the President, http://www.officeofthepresident.go.ug/index.php/2012-08-15-07-42-08/doc_download/15-mps-2012-2013-presidential-final-with-preliminaries-2012-2013*
40 *Phone tapping: Govt seeks 200bn, The Observer, http://www.observer.ug/index.php?option=com_content&view=article&id=19818:phone-tapping-govt-seeks-200bn*

Framework Paper for Financial Year 2014 / 15 – 2018/19 released by the Ministry of Finance, Planning and Economic Development in March 2014 is still requesting for UGX 200bn (US$ 80million) to "acquire specialised communication equipment" that would enable lawful interception.[41]

A recent unconfirmed report claimed service providers were facing pressure from government agencies to release print outs of their subscribers' information without court orders, and that this information had been used as evidence in courts of laws to justify arrests of individuals opposing government.[42] The allegations were refuted by the security minister, who in March 2014, insisted that tapping of phones was done in compliance with the law and upon issuance of a court order, and for criminal activity investigative purposes only.[43] He also stated that phone tapping did not apply to the most senior government officials – that is the President, Vice President, the Prime Minister, the Speaker of Parliament, and the Chief Justice. This was on the assumption that these individuals were "beyond subversion."

Intermediary Liability

The Electronic Transactions Act, 2011, regulates electronic communications and transactions. It defines an 'intermediary' as "a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message." On the other hand, it describes a service provider as "any public or private entity that provides to the users of its service the ability to communicate by means of a computer system" and "any other entity that processes or stores computer data on behalf of such communication service or users of such service."

Section 29 delineates the liability of service providers and intermediaries. It states that "a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access." The service provider is only 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; or the infringement of any rights subsisting in or in relation to the material."[44]

Providing access in relation to material of a third-party (a subscriber to a service) is defined as "providing the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access."[45]

Section 30 states that service providers are not liable for infringement for referring or linking to a "data message or infringing activity" if the service provider: "does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user; is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; does not receive a financial benefit directly attributable to the infringing activity; or removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user."

41 *National Budget Framework Paper for Financial Year (FY) 2014 / 15 – FY 2018/19 p.833; and www.budget.go.ug/budget/sites/default/files/National Budget docs/National Budget Framework Paper 14_15.pdf*
42 *Unwanted Witness Uganda, The Internet: They Are Coming For It Too, https://www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf*
43 *Muruli Mukasa: I replace Sejusa, The Observer, http://www.observer.ug/index.php?option=com_content&view=article&id=30889:-muruli-mukasa-i-replaced-sejusa&catid=53:interview&Itemid=67*
44 *See Section 29 subsection (1) (a) (b)*
45 *See Section 29 Subsection (3)*

Under Section 31, persons with complaints about a data message or related activity are required to notify the service provider or their designated agent in writing, giving details of the right allegedly infringed and remedial action required to be taken by the service provider in respect of the complaint.[46] If a service provider fails to act on a complaint, the complainant can appeal to NITA-U, under regulations issued in 2013.[47] However, the Act and its regulations are silent on the appeal mechanisms the party accused of infringement may take. Also, the regulations do not state the steps that NITA–U will take to investigate the complaint raised.

Besides, service providers are not required to monitor stored or transmitted data nor "actively seek for facts or circumstances indicating an unlawful activity."[48] However, it should be noted that other laws such as the Regulation of Interception of Communications, the Computer Misuse Act, and the 2013 communications regulatory authority law, require service providers to install hardware and software to allow for the lawful interception of communications.[49]

The recently passed Anti-Pornography Act, 2014, makes service providers liable for content hosted on their networks. The Act prohibits the production, traffic in, publishing, broadcasting, procuring, importing, exporting and selling or abetting any form of pornography. Under, Section 17 (1), internet service providers (ISPs) whose systems are used to upload or download pornography can be imprisoned for five years and fined UGX 10 million (US$4,000). Subsequent conviction of the ISP may lead to the suspension of their operating license. Under Section 7 (f), the Act provides for establishment 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." Service providers are obliged to take measures recommended by the Pornography Control Committee, including installing software to detect and censor pornography.

These provisions have drawn criticism from several ICT bodies in the country, who argue that the Act infringes on some principles of the internet, namely openness and privacy.[50] They claim that ISPs should not be held liable for content hosted on their systems. It is also suggested that the law should only require service providers to detect and suppress child pornography and that adults who consume adult pornography in private should not be proscribed as is the case with the law.

In addition, it has been argued that filtering content may be in violation of the principle of net neutrality, which requires internet service providers and governments to treat all data on the internet equally, not discriminating or charging differently by user, content, site, platform, application, type of attached equipment, and modes of communication.[51] In particular, the Principle on the integrity of communications and systems, states that "In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes."

46 *Section 31 calls for the person whose rights have been infringed to notify the ISPs or their agents in written form stating their name and address, the alleged infringed right, description of the material or activity which is alleged to be the subject of infringing activity, proposed remedial action required to be taken by the service provider in respect of the complaint, a declaration that the person complaining is acting in good faith, and a declaration that the information in the notification is correct to his or her knowledge. Persons found to be reporting false information are liable to the service provider for the loss or damage suffered by the service provider.*

47 *The Electronic Transactions Regulations, 2013, under Regulation 18*

48 *See Section 32 subsection (1) of the Act*

49 *The Regulation of Interception of Communications Act, 2010 (Section 11); Computer Misuse Act, 2011 Section 28 Subsection 5 (c), and the Uganda Communications Act, 2013, Section 29 (a)*

50 *Brace yourselves Ugandan Internet Users, The New Vision, http://www.newvision.co.ug/news/293-blogger-brace-yourselves-ugandan-internet-users.aspx*

51 *International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org/text*

Internet Freedoms Violations

In the first six months of 2013, Uganda was among the five African countries that requested administrators of the social networking site Facebook for details on one of its users.[52] A government spokesman said the request was related to "cybercrime" but he provided no details.[53] Facebook, which follows its own criteria and not Ugandan law in handling such requests, turned down Uganda's request. In the second half of 2013, Uganda made a similar request to Facebook related to the particulars of an unnamed user, which was similarly turned down.[54] In September 2013, the government-owned Sunday Vision newspaper reported that a former head of political intelligence in the president's office had been arrested on suspicion of being the operator of the Facebook account 'Tom Voltaire Okwalinga', a strong critic of the government.[55] He denied being arrested and being the operator of the said account.[56] These requests by the Uganda government could make citizens cautious of what they communicate over social networking sites.

The government announced on May 30, 2013 its intention to set up a social media monitoring centre to monitor social media users and "to weed out those who use it to damage the government and people's reputations." Security minister Muruli Mukasa was quoted as saying some social media users were "bent to cause a security threat to the nation" but said any action against social media users would be backed by a court order.[57]

As of April 2014, it was not clear if the government had formed the centre the minister referred to, or if it was indeed monitoring social media. However, a report released in January 2014 by a local civil society group claimed Uganda had set up a "counter intelligence desk" under the leadership of an army captain to "monitor social media and the Internet."[58] There was no independent verification of these claims.

Uganda has not been spared from international hacking. Government websites have been hacked into by actors based outside the country a number of times. In August 2012, the international hacker group "Anonymous" hacked into the Office of the Prime Minister's website in protest against the Anti-Homosexuality Bill. The following year, in May 2013, a number of government websites were hacked into by the hack group "Islamic Ghosts Team." However, reasons behind this hacking were not provided.[59] While in January 2014, reports emerged that the intelligence agencies – the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) - hacked into the network of one of Uganda's phone companies, Uganda Telecom, and used it to remotely access data and conversations of the Ecuadorian Embassy's staff in London where Wikileaks founder Julian Assange had sought refuge.[60] [61]

52 *Facebook, Global Government Requests Report FAQs, https://www.facebook.com/about/government_requests*
53 *Facebook rejects Ugandan request for user information, Africa Review, http://www.africareview.com/News/Facebook-rejects-Ugandan-govt-request-for-user-record/-/979180/1972348/-/29i5xpz/-/index.html*
54 *Facebook Government request report, Uganda, https://govtrequests.facebook.com/country/Uganda/2013-H2/*
55 *Sunday Vision, Rwomushana's Night in Jail, September 15, 2013*
56 *Rwomushana Denies Arrest In Okwalinga Facebook Firestorm, http://chimpreports.com/index.php/special-reports/crime-investigation/12847-rwomushana-denies-arrest-in-okwalinga-facebook-firestorm.html*
57 *Government to create Social Media Monitoring Centre, http://www.cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow/*
58 *Unwanted Witness Uganda, The Internet: They Are Coming For It Too, https://www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf, Pg.37*
59 *Over 40 Uganda Government Websites Hacked By Islamic Ghosts Team, PC Tech Magazine, http://pctechmag.com/2013/05/over-40-uganda-government-websites-hacked-by-islamic-ghosts-team/*
60 *UK, US hacked into Uganda's phone network, http://www.newvision.co.ug/news/651180-uk-us-hacked-into-uganda-s-phone-network.html*
61 *How the NSA hacks PCs, phones, routers, hard disks 'at speed of light': Spy tech catalog leaks- It's not as bad as you thought - it's much worse, http://www.theregister.co.uk/Print/2013/12/31/nsa_weapons_catalogue_promises_pwnage_at_the_speed_of_light/*

In early 2013, Freedom House reported a case where an unnamed LBGT rights group uncovered a case in which an email attachment sent among a private group of individuals was possibly intercepted by an unknown actor.[62] According to Freedom House, the information in the email attachment was later published in a local tabloid. Details of this account could not be verified.

On April 14, 2011, UCC instructed ISPs to temporarily block access to Facebook and Twitter for 24 hours "to eliminate the connection and sharing of information that incites the public." The order came in the heat of the 'walk to work' protests in various towns over rising fuel and food prices. The regulator's letter stated that the order had been prompted by "a request from the security agencies that there is need to minimise the use of the media that may escalate violence to the public in respect of the on-going situation due to the demonstration relating to 'Walk to Work', mainly by the opposition." At the time, UCC Executive Director Godfrey Mutabazi told Reporters Without Borders that he would again order that access to Facebook and Twitter be cut off if it was in the interest of public safety. He stated: "The freedom to live is more important than the freedom to express oneself." He further explained that that he was only appealing to Ugandans to take care not to use social networks to issue calls for hatred or violence. Some ISPs said they did not comply with the order, having received it after the 24-hour period during which the regulator had ordered them to block access. This could not be independently verified.[63]

Earlier in February 2011, UCC issued a directive to telecom companies to block and regulate text messages that could instigate hatred, violence and unrest during the presidential election period. The Commission issued 18 words and names, which mobile phone short message service (SMS) providers were instructed to flag if they were contained in any text message. These words included 'Tunisia', 'Egypt', 'Ben Ali', 'Mubarak', 'dictator', 'teargas', 'kafu' (it is dead), 'yakabbadda' (he/she cried long time ago), 'emuudu/emundu' (gun), 'gasiya' (rubbish), 'army/ police/UPDF', 'people power', and 'gun/bullet'. Two UCC spokesmen confirmed the directive to local media, saying the aim was "to ensure free, fair and peaceful elections."[64] The head of the regulatory body was at that time quoted to have said that "messages containing such words when encountered by the network of facility owner or operator, should be scrutinised and if deemed to be controversial or advanced to incite the public should be stopped or blocked."[65] A report of all blocked messages would then be prepared and submitted to UCC in 48 hours. However, it is not known whether any such reports were submitted.[66]

In July 2010, Timothy Kalyegira, editor of the online newspaper Uganda Record (http://www.ugandarecord.co.ug), was arrested and charged with publishing material online "with intent to defame the person of the president". The prosecution alleged that on July 12 and 16, 2010, he unlawfully published defamatory matter on the Uganda Record suggesting that government was behind the two bomb attacks on July 11, 2010 that killed at least 76 Ugandans in the capital Kampala. Security agencies also confiscated the journalist's laptop and mobile phone. Shortly after his arrest, the site http://www.ugandarecord.co.ug went down and remained inaccessible as of April 2014. It was not clear whether this resulted from

62 *Freedom House, Freedom on the Net, Uganda 2013 Report*
63 *Open Net Initiative, Government blocks Facebook, Twitter, https://opennet.net/blog/2011/04/ugandan-government-asks-isps-block-facebook-twitter*
64 *Uganda bans SMS texting of key words during poll, http://www.reuters.com/article/2011/02/17/ozatp-uganda-election-telecoms-idAFJOE71G0M520110217*
65 *Ibid 63*
66 *Intermediary Liability in Uganda, Intermediary Liability Africa Research Papers 5, Association for Progressive Communications, http://www.apc.org/en/system/files/Intermediary_Liability_in_Uganda.pdf.*

pressure on the hosts or it was a decision taken by the publisher. Uganda Record's Facebook and Twitter pages remained accessible in 2014 but had not been updated since 2011 and 2010 respectively. The media analyst organisation ACME stated that the most significant aspect of the charging of the Uganda Record journalist was that the government was becoming interested in what Ugandans were writing online and was doing something about it.[67]

Perhaps the earliest recoded case was in 2006, when government ordered ISPs to block access to radiokatwe.com, a website that published anti-government stories.[68] Authorities alleged that the website was publishing "malicious and false information against the ruling party NRM and its presidential candidate."[69] One of the service providers, MTN, issued a statement quoted by The Daily Monitor, defending the decision to block the site, saying that Ugandan law "empowers the commission to direct any telecoms operator to operate networks in such a manner that is appropriate to national and public interest."[70] At the time, users accessed the website using proxy websites. As of April 2014, information posted on the website could be accessed on their blog site at http://radiokatwenews.blogspot.com/. However, the content had last been updated in 2006. The domain radiokatwe.com was available but appeared to be under new ownership and published commercial information not related to Uganda.

Another early incident was in February 2006, when the government reportedly blocked access to the privately owned radio station 93.3 KFM and the website of its sister newspaper Daily Monitor (www.monitor.co.ug) because they were publishing independently tallied presidential election results. The paper's managing director said the internal affairs minister had explained to him the cause of the blocking but promised to end it within two days.[71] The website became accessible before the end of this period, by which time the elections commission had announced results from almost all over the country.

To-date, the media continues to bear much of the wrath from state organs who are hostile to criticism or to what they perceive as negative reporting. In May 2013, police shut down the Red Pepper, the Daily Monitor and its two radio stations KFM and Dembe FM, for publishing and broadcasting a classified internal government letter, which contained alleged succession plans of the Uganda presidency.[72] Journalists and media activists widely used social media to condemn and lobby for the re-opening of the affected houses. They were re-opened after 11 days.[73] Facebook and twitter hashtags #Monitorsiege, #RedPepperSiege were widely used to question the government's closure of the media houses rather than dealing with the author of the letter and the issues he raised.[74] Throughout the closure period, the websites of the affected media houses remained accessible but with limited content updates. The temporary closure of the media houses, which mirrored the September 2009 closure by the now defunct Broadcasting Council of four radio stations[75] accused of fanning ethnic tensions, have contributed to an increase in self-censorship by journalists on all media platforms as well as by ordinary citizens who use digital technologies.

67 *ACME, Be afraid, the government is nosing around online, http://www.acmeug.org/component/k2/item/26-be-afraid-the-government-is-nosing-around-online*
68 *Privacy International, Initial case of Internet freedoms invasion in Uganda, https://www.privacyinternational.org/reports/uganda/iii-privacy-issues*
69 *CPJ/IFEX, Critical website Radio Katwe blocked on eve of presidential election, http://www.ifex.org/uganda/2006/02/23/critical_website_radio_katwe_blocked/*
70 *Ibid. 43*
71 *Government Jams Monitor Radio, Site, http://www.upcparty.net/memboard/election7_260206.htm*
72 *Uganda's Daily Monitor raided over Museveni 'plot', http://www.bbc.com/news/world-africa-22599347*
73 *Media Literacy Project, Social Media Provides Outlet for Seized Ugandan Press and Media Activists, http://medialiteracyproject.org/news/pressroom/social-media-provides-outlet-seized-ugandan-press-and-media-activists*
74 *Redpepper Facebook page, https://www.facebook.com/REDPEPPERUG/posts/611371998880743?stream_ref=5*
75 *Government temporarily closes radio stations, http://humanrightshouse.org/Articles/11722.html*

Recommendations

- There is a need to sensitise citizens on what constitutes internet freedoms. Also, awareness should be created about the country's cyber laws so that users know how these laws affect their enjoyment of internet freedom.

- Government should clearly indicate how it intends to protect users' online privacy. For instance, the Regulations on Interception of Communications Act, 2010 explains how government intends to intercept communications but is silent on how the collected data will be protected.

- A law should be enacted to safeguard users' data and online privacy. The proposed Data Protection Bill should be drafted in consultation with all stakeholders including the media, CSOs, academia, service providers amongst others.

- Given the confusing and contradictory regulatory provisions in the different laws, government and civil society should prioritise understanding the interaction between all the laws and clarifying contradictions particularly with the constitutions. This should be with a view to amending the contradictory and retrogressive sections of these laws.

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