State of Internet Freedom in Uganda 2015

Survey on Access, Privacy and Security Online

CIPESA ICT Policy Research Series 08/15

CIPESA

OpenNet Africa

Credits

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

The report presents the findings of a study on the threats to access, privacy and security online, as well as the knowledge, attitudes and practices of citizens on internet freedom in Uganda. Other country reports for Burundi, Kenya, Rwanda and Tanzania as well as regional State of Internet Freedom in East Africa 2015 report are also available.

The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa. CIPESA recognises the cotribution of Edris Kisambira and Esther Nakkazi in developing this report.

Design
Ish Designs
muwonge_issa@yahoo.com

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

Contents

1. INTRODUCTION

The internet and other digital technologies have become key platforms for Ugandan and East African citizens to enjoy their rights to expression and to associate with other citizens as well as to engage with leaders. However, like other countries in the region, Uganda is experiencing challenges to the advancement of privacy and freedom of expression online. These challenges are affecting the way ordinary citizens, the media, human rights defenders and political parties communicate over digital technologies.

As of June 2015, Uganda had an internet penetration rate of 37% and there were 64 telephone connections per 100 inhabitants.[1] With more Ugandans becoming users of the internet and associated technology, digital platforms were widely expected to become platforms for citizens to freely express themselves on issues of national concern, including politics. It is not in doubt that Information and Communication Technology (ICT) has helped to connect millions of ordinary citizens with other citizens and to access news and information more easily. Digital communications have also expanded the possibilities for citizens to connect to public officials and agencies (minimally though), and to express themselves.

However, there are challenges to citizens' enjoyment of internet freedom. 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. Uganda enacted its Regulation of Interception of Communications Act in 2010, but there is shortage of information on whether the country conducts communications monitoring in conformity with the law. The country appears to be intent on stepping up actions against social media users under the pretext of promoting public order and unity as well as preventing the spread of false information.[2] In December 2014, Uganda solicited citizens' inputs to a Data Protection and Privacy Bill that falls short of safeguarding privacy rights, but nine months later remained quiet on what it planned next with the bill.[3] Uganda conducts mandatory registration of phone users but it is unclear how this law is implemented or how data collected about citizens is used.

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

2. RESEARCH METHODOLOGY

The research presented in this report was conducted through a mixed methods approach which included policy and literature reviews, key informant interviews and stakeholder workshops.

The research targeted 60 key informants drawn from stakeholder groups that either affected internet freedom, those whose internet freedom was likely to be violated, and those deemed knowledgeable about the subject. The research also collected the views of a total of 37 human rights defenders, bloggers, journalists, editors, media rights organisations, sexual minorities and gender equality activists in Uganda who participated in digital safety and security training workshops during 2015.[4]

Media constituted 20% of the respondents, academia 19% followed by NGOs/CBOs at 14%. Tech/app developers and the private sector were 12% each. Regulatory authorities and Human Rights Defenders (HRDs) represented 7% of survey participants each while 5% were telecommunications companies. One respondent each was surveyed from law enforcement, security and political party. See annex 1 for a full list of organisations surveyed.

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

1 Uganda Communications Commissions (UCC), Status of Uganda's Communications Sector, October 2015, http://ucc.co.ug/files/downloads/Annual%20Market%20Industry%20Report%202014-15-%20October%2019-2015.pdf

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

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

CIPESA Conducts Digital Safety Training for Journalists and Activists in Tanzania and Uganda, http://www.cipesa.org/2015/04/cipesa-conducts-digital-safety-training-for-journalists-and-activists-in-tanzania-and-uganda/; and

World Press Freedom: Ugandan Journalists Convened for Digital Security Training, http://www.cipesa.org/2015/05/world-press-freedom-ugandan-journalists-convened-for-digital-security-training/

3. COUNTRY CONTEXT

3.1 ICT Access

There are 11.9 million internet users in Uganda, implying a 37% penetration rate. Telephone penetration stands at 64%.[5] The entry of Vodafone into the sector in the first half of the 2015 brought the total number of voice operators to seven.[6] The others include Airtel, Africell (formerly Orange), Uganda Telecom, MTN, Smart Telecom and K2 Mobile. Africell completed acquisition of Orange in November 2014.[7] Also, in November 2014, Liquid announced over the takeover of Infocom, an ISP.[8]

Through the national broadband Initiative, government has laid a total of 1,400 kms of fibre optic cable connecting major towns and government agencies.[9] A landlocked country, Uganda's major service providers are connected to high-speed submarine cables landing at the East African coast through Kenya and Tanzania.

The Rural Communications Development Fund (RCDF) implemented by the Uganda Communications Commission (UCC) and funded by a 2% levy on licensed telecommunications operators' revenue, was established in 2003. It has since seen the establishment of numerous internet points of presence (POPs), internet cafes and ICT training centres, and the establishment of 1,000 ICT labs in schools and training of over 18,750 individuals in rural areas, 691 teachers and 486 head teachers in use of ICT.[10]

3.2 Governance Landscape and Legal Developments

Uganda has 29 registered political parties and to-date three general elections have been held since the reintroduction of multi-party politics in 2005. The next elections are scheduled for February 2016 with President Yoweri Museveni who has been in power for 29 years among the contestants. Allegations of voter intimidation and rigging have in past elections been cited by opposing parties. Uganda is also regularly criticised by human rights organisations for clamping on media freedom, witch-hunting the LGBTI community, and silencing critical civil society.[11]

On June 17, 2015, political tensions mounted when Amama Mbabazi, Uganda's former Prime Minister and secretary general of the ruling party, took to Youtube to officially announce his intention to run in the 2016 presidential elections.[12] In a rebuttal video to Mbabazi's announcement, Museveni linked Mbabazi aides to the Whatsapp audio recordings whose authors he had asked the police to arrest and to other "false" documents circulating on social media, which he said were tarnishing his government's image and inciting ethnic tensions.[13]

In 2015, Uganda proposed the Non-Governmental Organisations (NGO) Bill to replace the existing Act from 2006. The bill was drafted in response to the "rapid growth of Non-Governmental Organisations" which had led "to subversive methods of work and activities, which in turn undermine accountability and transparency in the sector."[14] Under the proposed law, NGOs will have to declare their sources of income and obtain permits from local authorities to operate. Furthermore, the NGO Board will be able to revoke permits if NGOs contravene their constitutions or the bill, or if "in the opinion of the board it is in the public interest to do so."[15]

5 UCC, Status of Uganda's Communications Sector, October 2015, http://ucc.co.ug/files/downloads/Annual%20Market%20Industry%20Report%202014-15-%20October%2019-2015.pdf

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

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

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

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

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

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

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

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

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

15 Alon Mwesigwa, Uganda: NGO bill aims to muzzle civil society, say activists, http://www.theguardian.com/global-development/2015/jun/24/uganda-ngo-bill-aims-muzzle-civil-society-say-activists

In late 2014, Uganda issued a draft Data Protection and Privacy Bill for public comment.[16] The Bill seeks to protect the individual privacy and personal data by regulating the collection and processing of personal information. It provides for the rights of persons whose data is collected and the obligations of data collectors and data processors; and regulates the use or disclosure of personal information. However, the bill falls short of its expectations, with numerous clauses undermining privacy.[17] Since the call for public comment, there has been no evidence of the bill's progression.

Meanwhile the Access to Information Act 2005 remained unimplemented until 2011 when the enabling regulations were enacted. To-date, proactive disclosure and citizens' requests for government-held information remain low.[18] In a landmark case, on February 6, 2015, a Chief Magistrate's Court in Kampala ruled that the reasons for which information is requested or the belief about how it will be used "are irrelevant considerations" in determining government's approval or denial of a request. The ruling came after the Hub for Investigative Media was denied access to information related to activities of the National Forestry Authority that were funded by the World Bank between 2009 and 2011. The landmark ruling set a precedent that could make it easier for journalists and citizens to exercise the right to information.[19]

The Regulation of Interception of Communications Act 2010 allows for the interception of communications. The law gives the ICT minister the powers to set up a monitoring centre connected to telecom service providers' systems. To date, there is no evidence that such a centre exists. Additionally, the Anti-Terrorism Act 2002 gives security officers the power to intercept the communications of a person suspected of terrorist activities and to keep suspected persons - including journalists who "promote terrorism - 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.

Meanwhile, the Anti-Pornography Act 2014 provides for the prohibition of the production, traffic in, publishing, broadcasting, procuring, importing, exporting and selling or abetting any form of pornography and punishment for those found to be in possession of any pornographic materials. Under section 17 (1), an Internet Service Provider (ISP) through whose service pornography is uploaded or downloaded is punishable with a fine of up to UGX 10 million (US$ 3,000) or five years imprisonment or both. Subsequent conviction of the ISP may lead to the suspension of their operating license.[20]

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

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

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

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

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

20

4. Survey Findings

4.1 Knowledge, Attitudes and Practices on Internet Freedom

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

Frequently Used Communication Technologies

The most frequently used communication technologies among respondents were mobile SMS, email, mobile or landline voice, WhatsApp, and Facebook. They were used either daily or 2-5 times a week by 92%, 91%, 90%, 86% and 84% of respondents respectively. Daily usage was highest for email (88%), voice over mobile or landline phone (86%), Whatsapp (78%) and Facebook (69%). Over 30% of respondents never used Blogger, Google Plus or Viber.

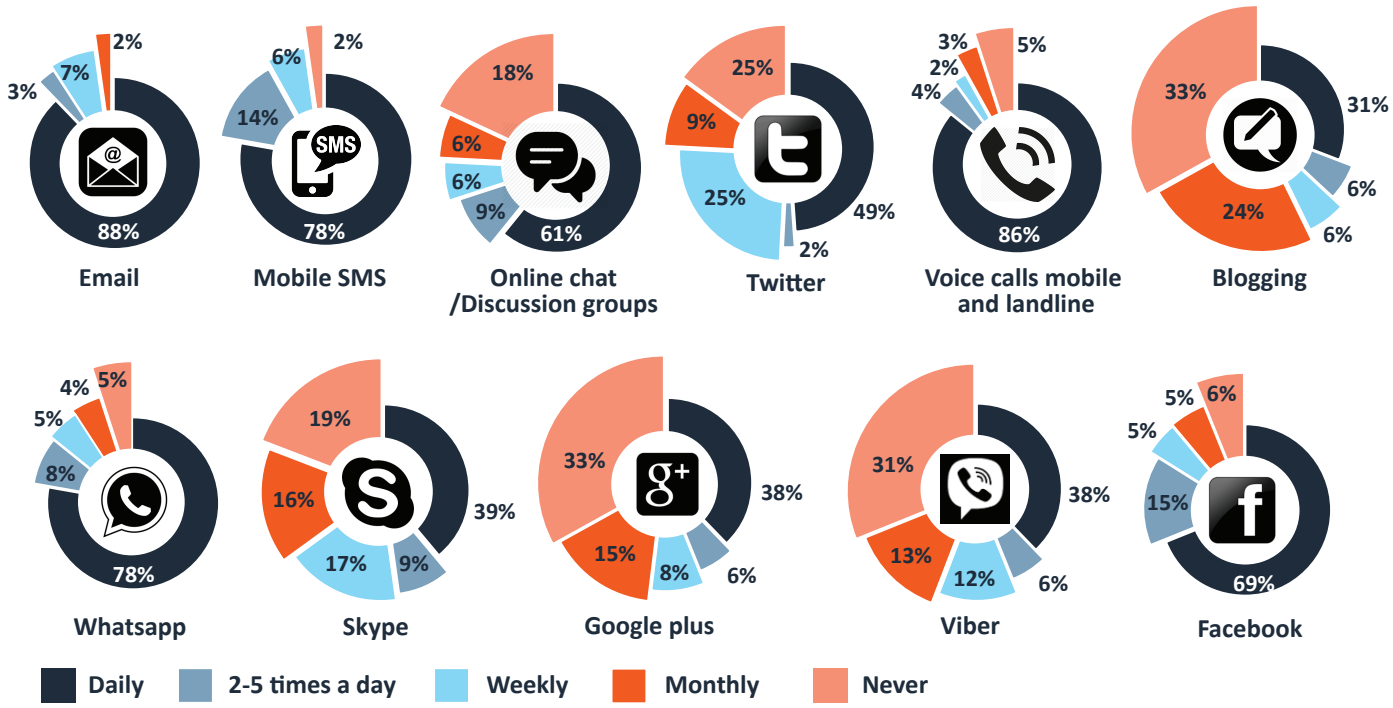

Figure 1: How regularly do you use these communication technologies?

Understanding of Internet Freedom

Most respondents understood internet freedom as the ability to use the internet and other digital communication technologies without commercial or state restrictions. There were varied descriptions of the elements that made up internet freedom, but recurrent themes included privacy and the right to access affordable and uncensored internet.

Notable quotes of understanding of internet freedom

"They are like any other rights, the right to free, easy access to the Internet."

"Free usage and access to the Internet"

"Free expression, affordable access, openness, freedom to innovate, and privacy"

"The ability to access my cyber space unrestricted"

"It's a form of freedom of speech and expression"

"The ability to communicate freely using communication technologies"

"Using the Internet freely without disturbing other people's peace"

"The ability to use the Internet uninterrupted by government restrictions"

"Unmonitored online, uncensored online browsing"

"The right to use the Internet which is a public domain"

Knowledge of Privacy and Security in Digital Communications

All respondents had some knowledge of privacy and security in digital communications. Of those surveyed, 17% rated themselves as having excellent knowledge, while 37% indicated their knowledge as good, with 33% as workable and 13% as poor. Those who indicated excellent knowledge were mainly academics and techies.

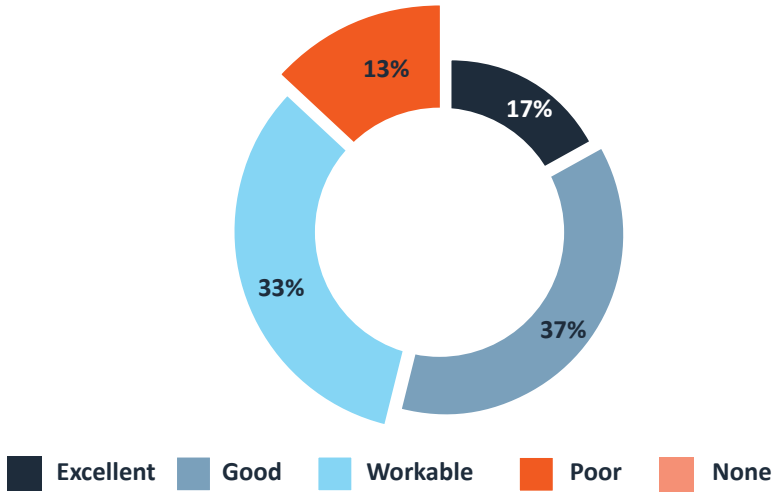

Figure 2: How would you rate your knowledge of privacy, security and unfettered access in digital communications?

Privacy and Security Concerns in Communications

The most common uses of communication technology in which security/privacy may be a concern were indicated as voice and SMS over mobile, email, social media platforms like Facebook, Twitter, online trading, online banking, online shopping and mobile money transactions

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

Use of Digital Safety and Security Tools

The majority of respondents (76%) had ever used technologies to protect their privacy and security online.

Figure 3: Do you use/ have you ever used tools and technologies intended to protect your privacy and security online?

The use of passwords was mentioned as a tool to protect information online but some respondents acknowledged that this alone did not guarantee safety. Others mentioned firewalls, password vaults, email encryption, identity management tools, virtual private networks (VPNs), and web proxies. Those who used anonymisation and circumvention tools sourced them from the internet on recommendation of organisations that work in the area of internet freedom or through recommendations from friends and colleagues. Some received the tools at digital safety training events or received them from their employers who needed to safeguard company and employee information.

Reasons for not using the tools included the belief by some respondents that they were careful not to compromise their security by not sharing more than they should. Some were just unaware of the security risks online and the tools to protect them. But for one private sector respondent, the apathetic attitude to online safety resulted from a belief that hackers could breach any security system. "I am not really assured that even if I used such technologies, the information will not be hacked especially if government agencies are interested in accessing the information in question," she said.

Perceptions of Government Monitoring and Surveillance

Just over three quarters of respondents (76%) thought that government agencies were monitoring and intercepting citizens' communications. Among those whose communications the respondents thought were being monitored were politicians opposed to President Museveni and the ruling party, critical journalists, the media, and NGOs engaged in political work.

Figure 4: Do you think government agencies in your country are monitoring and intercepting citizens' communications?

Ugandans with a significant presence on Facebook and Twitter particularly those who discussed or made posts on political issues, were also thought to be targets of monitoring. "The phone tapping [Interception of Communications] law gives Government the right to monitor anyone. I think all our conversations are monitored," said a respondent from academia. Without giving specifics, an official from the Uganda Communications Commission stated that the communications of suspected criminals were indeed monitored. "The communications monitored are for security of citizens. This is done world over," he said.

In terms of the Government departments that make these requests, respondents pointed out the Uganda Police, Internal Security Organisation, External Security Organisation, Uganda Communications Commission, Ministry of Information, the Judiciary and the Uganda Revenue Authority.

Respondents were not clear on the technologies and tactics used in monitoring, surveillance, filtering and censorship. However, some thought that the Police made requests to telecom companies for communications of suspects as part of criminal investigations and matters of national security. However, one respondent said the Government does not make requests; rather it instructs and orders the telcos to provide information. Another said they are not aware of such requests but that the regulator makes the requests on behalf of Government.

4.2 Threats to online access, privacy and security

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

Who is Likely to Violate Citizens' Internet Freedom?

Respondents were asked to rank the likelihood of various groups violating citizen's internet freedom with each group was ranked on its own and not in comparison to others. Regulators and law enforcement agencies were perceived as the likeliest violators of privacy and security online by 58% and 59% of respondents respectively. They were followed by intermediaries at 55% and adversaries at 53%. Those deemed least likely to violate user privacy and security were fellow citizens and journalists.

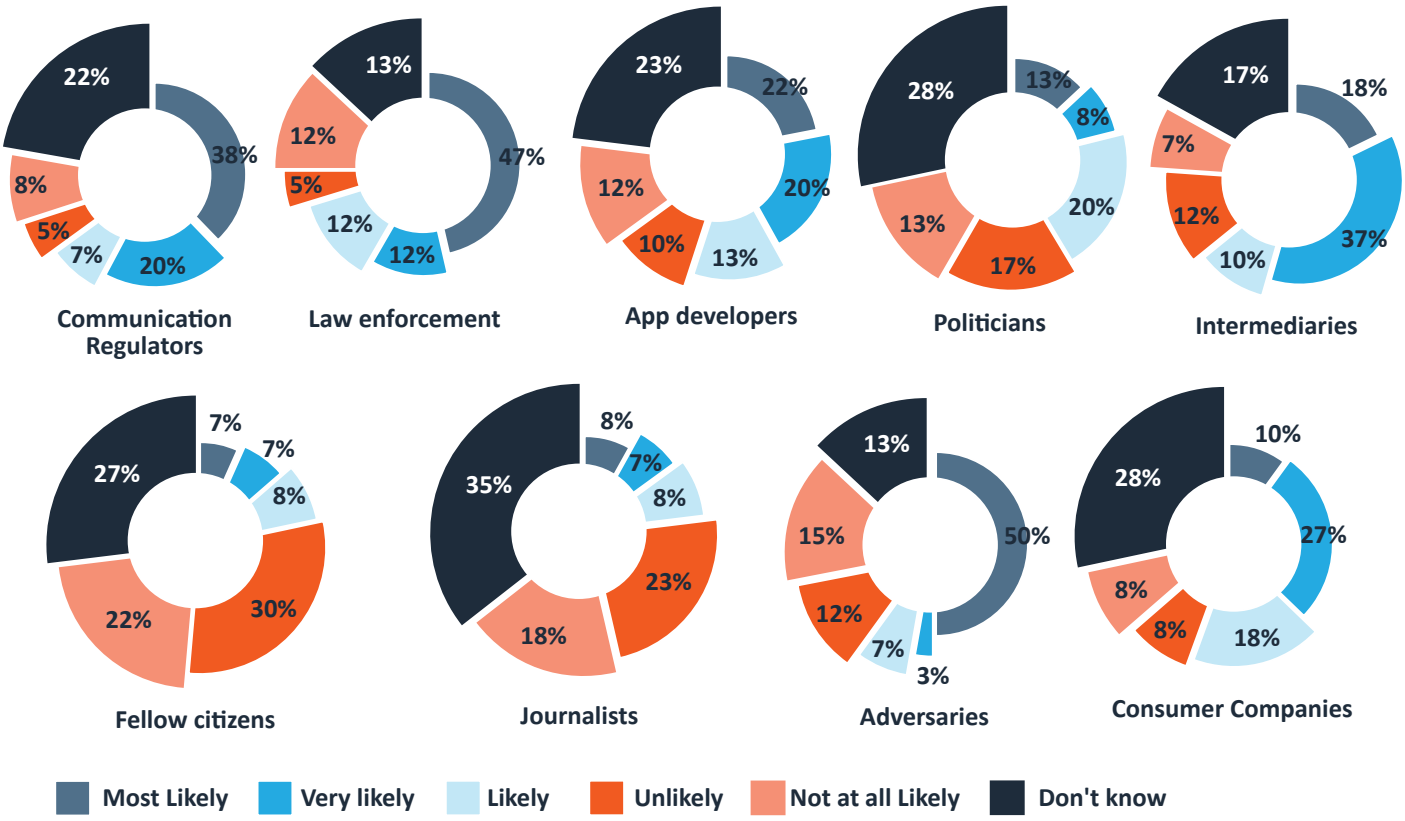

Figure 5: Who are the most likely to violate privacy and security of citizens' and organisations' communications?

Major Causes of Privacy and Security Vulnerabilities

Ignorance among internet users and governments alike was pointed out as amajor cause of security/privacy vulnerabilities in Uganda. The government lacked the will to secure citizens' digital information while most citizens did not consider privacy and security as important issues.

Others causes of vulnerabilities mentioned were:

- Weak consumer protection laws
- Weak internet laws that take long to evolve and are poorly implemented
- Lack of security tools
- The growing threat of hackers and online fraudsters
- Emerging threats to internet freedoms like terrorism
- A general lack of use of up-to-date anti-virus software
- Poor government enforcement of ICT related policies

Among the challenges to internet freedoms cited were website hacking, limited mechanisms of child online protection, online fraud, cyber stalking and bullying, and – more recently, online violence against women.

Government security agencies tapping citizens' communications, the loss of data and information resulting from theft of devices were highlighted too. The lack of user awareness regarding safe and responsible use of the internet was another challenge. "Releasing of uncensored content on the internet due to the absence of regulation on social media networks is a challenge to internet freedoms," said one respondent.

Adequacy of Measures to Protect Citizens From Illegal Monitoring of Communications

Majority of respondents (75%) said measures to protect citizens from illegal monitoring of their communications were not adequate and urged the enactment of laws to govern privacy of communications and user data.

Figure 6: Are there adequate measures to protect citizens in your country from illegal monitoring of communications?

However, a respondent from the communications regulatory authority noted that government had put in place a number of regulations to protect the end-users. While other respondents expressed confidence in the proposed Data Protection Bill, 2014, which is still to be passed. They also mentioned the Computer Misuse Act, which allows aggrieved parties to go to court in case their rights and freedoms have been infringed, and the registration of all mobile phone users and regulating all mobile operators.

4.3 Effect of Information Controls on Communication Behaviour

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

To Communicate or Not to Communicate Because of Security Risks

Over half of the respondents (58%) indicated an instance of opting not to communicate or share information because of a perceived security risk. The decision not to communicate was informed by various reasons. Some noted increased concerns especially over personal information which they rarely shared on social media.

Further, the fear of personal information being used against them was also cited as a concern that led to limited sharing of information. An apps developer who was fearful of revenge pornography stated, "I don't share personal pictures on social media and Whatsapp because it can be abused."

And yet for some, the decision not to share information was taken so as not to endanger its recipients. A human rights defender working with sexual minorities stated that at the time when the anti-gay law was passed, "I had to withhold information in order not to endanger others." In early 2014, Uganda enacted the Anti-Homosexuality Act that prohibited any form of sexual relations between persons of the same sex and promotion of homosexual relations. Although the law was subsequently nullified by court, members of the local LGBTI community have reported ongoing malicious attacks on their email and social media accounts, theft of devices and blackmail, among others.[21]

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

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

Some of the respondents whose communications had never been deterred by perceived security risks felt confident that they could secure their communications, while some said they had not felt the need to secure their communications. “Everything we do a lot of times has risks but we don’t stop to live our lives, do we?” one respondent wondered. “My entire existence is dependent on the internet. When my data runs out its worse than when there is a power cut so I cannot think of not using the internet, communicating online, or sharing things online,” said another.

How Access to Safety Tools Would Affect Individuals’ Communication Practices

Respondents were asked how their communication behaviour would be affected if they were provided with anonymisation and circumvention tools. Some respondents thought that anonymisation or circumvention tools would boost their confidence to communicate freely because their identities would remain unknown thus enabling them to raise concerns which they would otherwise not have raised if their identities were revealed.

Opposing this view were respondents who worked with Government agencies and regulatory authorities, who believed provision of such tools to citizens could promote irresponsible behaviour, such as the perpetration of hate speech, defamation and cyber crime.

However, the delicate balance between security and privacy was also highlighted in light of growing threats such as terrorism. A political leader said promoting anonymity would not be ideal in a scenario like the April 2015 terrorist attacks on Garissa University College in Kenya in which more than 150 students were killed by al Shabaab militants. “If such information [about an impending attack] is available, it is the duty of the person with this information to pass it on to the relevant authorities so that lives are not lost and as such anonymity and circumvention should not always prevail,” he said.

5. INCIDENTS OF INTERNET FREEDOM VIOLATIONS

In February 2015, the Uganda Communications Commission reportedly threatened to "shut down social media sites over their misuse by the public. This came in the wake of concerns over the use of social media to leak and share pornographic content.[22] In the same month, authorities arrested Robert Shaka, accusing him of being behind the pseudonym Tom Voltaire Okwalinga (TVO), whose Facebook account was allegedly used to disclose supposed government secrets. Police ransacked Shaka's home without a search warrant, and confiscated his personal electronic devices including an iPad, laptop, mobile phone and flash disks.[23]

In June 2015, Robert Shaka was again arrested under Section 25 of the Computer Misuse Act for using computers and other electronic devices to issue "offensive communication". Section 25 of the Computer Misuse Act states, "Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor." A conviction attracts a fine not exceeding UGX 480,000 (US$140), imprisonment not exceeding one year, or both. The charges of making "offensive communications" related to Facebook posts by TVO on President Museveni's health status. It was alleged that between 2011 and 2015, Shaka had "wilfully and repeatedly using a computer with no purpose of legitimate communication disturbed the right of privacy" of President Museveni "by posting statements as regards his health condition on social media." However, there has been no evidence that Shaka is responsible for posting content under the TVO pseudonym. He was released on bail a week after arrest. There are unconfirmed reports of user information requests to Facebook by the Uganda government of accounts related to the TVO.

The arrest of Shaka came shortly after President Museveni expressed disdain for "sectarian and abusive" audio recordings that were widely shared on the popular mobile messaging platform WhatsApp. The audios featured an exchange of words between unidentified individuals, supposedly from the Bahima and Bakiga ethnic groups of Western Uganda, ridiculing each other. Museveni, who hails from the former group, called for the immediate arrest of the people involved in the recordings. He accused them of using sectarianism to achieve political advantage.

In July 2015, reports emerged that the Uganda Police and the Office of the Presidency were in advanced stages of acquiring hi-tech surveillance software from Israel and Italy to begin large-scale spying in Uganda.[24] Information released by Wikileaks shows email exchanges between the between the Italian surveillance malware vendor Hacking Team and its local vendor Zakiruddin Chowdhury, who seemed to have strong contacts with senior Uganda government officials.[25] Wikileaks also revealed that Kenya's government was in the process of acquiring surveillance software from Hacking Team.[26] In Uganda's case, it was suggested that the LGBTI community could be among the key targets of surveillance.[27] Earlier, in April 2014 after the after the Anti-Homosexuality Bill was signed into law, the LGBTI community in Uganda was reportedly targeted by Zeus, a spyware which steals confidential information from computers.[28] Human rights defenders interviewed by OpenNet Africa for this research reported incidents of office break-ins and hacking of websites belonging to organisations working on LGBTI issues.

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

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

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

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

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

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

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

In December 2014, popular Facebook page, "Ugandans at Heart" was reportedly shut down by Facebook due to violation of the company's terms of service including promoting hate speech, hatred and obscenity.[29] A presidential aide commended Facebook's actions stating that "It's good that the action is known to have been the work of Facebook management as opposed to those disdainfully attributing it to NRM/President Museveni."[30] The page was eventually restored.

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

On June 22, 2015, authorities announced that a cybercrime unit had been established and a head appointed. This came in response to the president's warnings on the misuse of cyberspace to incite hatred and sectarianism. Although this unit will fight cyber crime in general (including cyber fraud, cyber terrorism, cyber stalking and other electronic crimes), its timing and set up are curious, given that in 2013, a national Computer Emergency Response Team (CERT) was set up for similar purposes.

6. CYBERCRIME

According to the Uganda Police Annual Crime and Road Safety report 2012, a total of 62 cybercrime cases were reported and investigated in which Uganda shillings (UGX) 1.5 billion (US$ 410,000) was lost through hacking victims' emails, phishing, mobile money and ATM fraud. In 2013, 45 cases were reported but these resulted into UGX 18.1 billion (US$ 4.9 million) losses. Between the months of August and November 2014, mobile money fraud caused a loss of over UGX 207 million (US$ 56,000) to the users.[31]

6.1 Online Violence Against Women

The extent of online violence against women (VAW) in Africa remains unknown. However, there are anecdotal indications that it is becoming more rampant, fuelled by increased access to ICT and the lack of laws to punish those who commit cyber VAW.[32] Incidents of revenge porn targeting women have been registered in Uganda as in other East African countries. The region has witnessed an increase in incidents where women's private information, including pictures and videos, are published on social media without their consent.[33] In Uganda, the victims who have included musician Desire Luzinda and television personalities Anita Fabiola and Sanyu Mweruka, were further subjected to threats of prosecution.[34]

29 Ugandans at Heart, Write To Facebook And Ask Them Why They Closed UAH, http://ugandansatheart.org/2014/12/, UAH Closure was a Shock to me too such that I have lost my faith in Facebook!, http://semuwemba.com/2014/12/04/uah-closure-was-a-shock-to-me-too-such-that-i-have-lost-my-faith-in-facebook/

30 Ugandans At Heart, President Museveni cannot shut down UAH, http://ugandansatheart.blogspot.ug/2014/12/uah-president-museveni-cannot-shut-down.html

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

32 Association for Progressive Communications (2015), Cases on women's experiences of technology-related VAW and their access justice, https://www.apc.org/en/pubs/cases-women%E2%80%99s-experiences-technology-related-vaw-a

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

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

Ibid

7. Discussion

The findings from the survey show that many of the respondents had a good understanding of what constituted internet freedom. However, a big number thought the term referred to having free (not paid for) access to the internet. Respondents from academia, politicians, human rights organisations and people who work in the Information Technology (IT) space were more aware of the meaning of internet freedom and the implications associated with regulating the use of the internet.

It is noteworthy that most respondents who noted internet freedom to mean free usage and access to the internet considered this to be a human right. Majority of the respondents believed that the telecommunications regulator and law enforcement agencies were the major perpetrators of surveillance and posed the biggest threat to people's privacy, security and access to the internet.

Although a fairly big number (42%) had never decided not to communicate online due to a perceived security risk, those who knew the risks involved, such as the LGBTI community and human rights defenders regularly protected their privacy or security while communicating online.

Most journalists especially political reporters opt to communicate offline if the information they are receiving or relaying was perceived sensitive. This often translates in withholding by-lines from stories and not naming their sources. The journalism fraternity, however, unlike the LGBTI community, does not have access to digital safety tools. Although some journalists changed passwords and email addresses frequently, they have not been able to access the tools as those used by the LGBTI groups, which would offer them more security.

While many respondents wished to use anonymisation and circumvention tools so as to gain greater trust in communicating online, regulators cautioned that this could lead to a rise in criminal behaviour on digital platforms.

African governments including Uganda were criticised for passing legislation that aim at restricting access to information and threaten security and people's privacy online. A common view was that such legislation should have well outlined checks and balances to prevent abuse or excesses by government authorities. There was also low awareness of the provisions of existing laws such as the Computer Misuse Act, Regulation of Interception of Communications and Access to Information across all stakeholder groups.

Respondents also expressed a widespread need for telecom companies to guarantee the privacy of their clients and also cultivate trust in their systems. Service providers were further faulted for not doing enough in terms of protecting and educating their subscribers about digital safety.

Media scholars and practitioners pointed out that the same 'high-handed' restrictions that have traditionally applied to freedom of speech and access to information in Uganda are increasingly being applied to internet freedom. This was evidenced in restrictions stipulated in such laws as the Regulation of interception of communications 2010, and the Anti-pornography Act 2014.

8. Recommendations

There is a need for intermediaries to support internet freedom, particularly by upholding user privacy through safeguarding clients' information and not sharing it with third parties unless legally obliged to do so. In the instances where disclosure of clients' information is necessary, telecom companies should adhere to due processes and only disclose information on the basis of a court order or otherwise as clearly required by the relevant laws of Uganda.

- Government, civil society organisation, the media, development partners and other actors should step up education and awareness campaigns on internet rights. Observing Internet Freedom day (January 18) could be one of the ways of raising awareness.

- Training and capacity building in the use of online safety and security tools particularly for groups that are most at-risk such as journalists, the LGBTI community, and human rights defenders who work on areas the government considers could undermine national security or social cohesion.

- Capacity building across all sections of internet users in responsible and ethical conduct online should be encouraged so as to curb emerging issues such as child pornography, violence against women online and hate speech.

- A call for the immediate enactment of a data protection and privacy law by government. The provisions of this law should be anchored in regional and international treaties regarding privacy online. Further, the process of enacting this law should involve robust stakeholder consultations.

- Need to enact and enforce laws and regulations on vices like hate speech, online violence against women, and child online protection.

- Government transparency in communications surveillance and investigations into online crimes should be observed.

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

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

75 Government now bans 'Mwananchi' website, http://www.opennetafrica.org/government-now-bans-mwananchi-website/

9. ANNEX 1 (List of Survey Respondents including key informants and participants in stakeholder workshops)

Ministry of ICT
SMS Media
Freelance IT Consultants
Independent Media Analysts
Uganda Police
Freelance app developers
Freelance journalists
Staff and Students - Makerere University Department of Journalism
Uganda Communications Commission (UCC)
Consumer Rights Association
Independent Social Media Consultant & trainer
Bloggers
Opposition Politician with Uganda People's Congress (UPC)
Uganda ICT Association
Management Sciences for Health
Uganda Technology and Management University (UTAMU)
Hive Colab
MTN Uganda
Lubega and Ochieng company advocates
Staff and students - Makerere University Business School
Staff and students - Makarere University Faculty of IT
Staff and Students – Makarere University Faculty of Engineering
Staff and students - Ndejje University
Super FM
Radio Uganda
New Vision
Monitor publications
Parliament of Uganda staff
Public Relations Association of Uganda (PRAU)
Cyber School
Information Network (I-Network)
PC Tech Group Ltd
Sexual Minorities Uganda
Vertus Radio
The Patriot Magazine
Bukedde newspaper
Radio one FM
Voice Media Group
Capital FM
Women of Uganda Network
Freedom and Roam Uganda (FORAG)
Bukedde Television
Kawowo news
TopTV
Metro FM
Sanyu FM
The Independent newspaper
Daily Nation Newspaper
Uganda Journalist Union
The Observer
Arua One Radio
Kigezi News Online
Kiira FM Radio
Elgon FM
The East African newspaper
iFreedoms Uganda

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

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

OPEN TECHNOLOGY FUND

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
156-158 Mutesa II Road, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org