State of Internet Freedom in Tanzania 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 Tanzania. Other country reports for Burundi, Kenya, Rwanda and Uganda, 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 contribution of Jamii Media in developing this report.

Design
Ish Designs
muwonge_issa@yahoo.com

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

Contents

1. INTRODUCTION

Tanzania, located along Africa's east cost is composed of Mainland Tanzania and the Zanzibar archipelago. It is along this coast line that the Eastern Africa Submarine Cable System (EASSy) lands at Dar es Salam offering direct connectivity between east Africa, and Europe and North America. Other landing cables on the Tanzania coast line include The East African Marine System (TEAMS), the Sea Cable System (Seacom), and the Lower Indian Ocean Network 2 (LION2).

However, as of 2014, only 23% of the country's population had access to internet.[1] The government has worked to boost connectivity in country through the development of the National ICT Backbone which links the coastal cables with mainland infrastructure and that of neighbouring landlocked countries.[2] To date, 7, 560 kms of fiber option cable have been laid. Connectivity is further supported bytax exemptions on computer equipment prescribed in the Value Added Tax Act (2006).[3]

As more citizens have gone online, there have been a series of laws passed over the course of 2015 which threaten freedom of expression and access to information. The publishing of the Cybercrime Bill was met with apprehension due to its overt disregard for press freedom and freedom of expression, the excessive powers granted to police, and the limited protections afforded to ordinary citizen.[4] Additional laws such as the Access to Information Bill and the Statistics Act were both met with apprehension by civil society and the media due to their limitations on freedom of expression and access to information amongst other concerns.[5,6] Further, the country still relies on outdated laws such as the the Newspapers Act, 1976, the National Security Act, 1970, and the Public Leadership Code of Ethics Act, 1995 which continue to undermine these freedoms.[7]

This report therefore aims to generate an understanding on the state of internet freedom in Tanzania, 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 the country, and the effect of information controls on the online behaviours of citizens, journalists and human rights defenders. The findings of the study should serve 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: researchers based in Tanzania conducted policy and literature reviews plus interviews with key informants.

The research targeted 32 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. In addition, the research also collected the views of 17 bloggers, journalists (print, broadcast and online media), editors and content managers in Tanzania who participated in digital safety and security training workshops that were conducted during April 2015. The research mostly covered developments in the period between May 2014 and August 2015.[8] For a list of organisations that participated in the study, see Annex 1.

The media (38%) constituted the highest proportion of respondents followed by NGOs/ Community Based Organisations (16%) and human rights defenders (13%). One individual each was interviewed from academia, the national regulatory authority, government and tech innovation. Telecom companies/ISPs and political parties constituted 9% each of the key informants.

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 TCRA Quarterly Statistics, June 2015, http://www.tcra.go.tz/images/documents/telecommunication/telcomStatsJune15.pdf

2 Tanzania, National ICT Backbone, http://www.nictbb.co.tz/about.php?in=nictbb

3 Value Added Tax Act (2006), http://www.tra.go.tz/tax%20laws/The%20Value%20Added%20Tax%20Act,%201997.pdf

4 Tanzania Cyber Crime Bill Should Safeguard citizens rights on the Internet, http://www.cipesa.org/2015/04/tanzania-cyber-crime-bill-should-safeguard-citizens-rights-on-the-internet/

5 Article 19, Legal Analysis, Tanzania: Cybercrime Act 2015, https://www.article19.org/resources.php/resource/38058/en/tanzania:-cybercrime-act-2015

6 Twaweza, Rapid Analysis and Key Questions on Tanzania's Statistics Act, http://www.twaweza.org/go/stats-act-analysis

7 Access to Information in Tanzania: Laws, Policies and Practice, http://www.cipesa.org/2015/03/access-to-information-in-tanzania-laws-policies-and-practice/

8 CIPESA digital safety and security skills and awareness drive in Tanzania, http://www.cipesa.org/2015/04/cipesa-conducts-digital-safety-training-for-journalists-and-activists-in-tanzania-and-uganda/

3. COUNTRY CONTEXT

3.1 ICT Access

The government of Tanzania is developing a nationwide high-speed data connection through construction of optical fibre cable throughout the country. This, coupled with the increase of affordable smart phones in the country, has enabled internet use to increase at a rapid rate. Internet penetration has grown from 3.5 million users in 2008 to 11.3 million users in 2014 andas of June 2015, there are 34 million fixed and mobile telephone subscribers representing a telephone penetration rate of 71%.[9]

3.2 Governance Landscape and Legal Developments

Tanzania failed to complete the constitution review exercise ahead of the October 2015 elections.[10] The draft constitution proposed to raise the breadth of rights it offered and broadened the definition of the right to freedom of expression. Impasse over division of powers between mainland Tanzania and the semi-autonomous Zanzibar Island caused the deadlock. The October 2015 polls were thus held under the old constitution. The ruling Chama Cha Mapinduzi (CCM) has been in power since 1961 and in October 2015, Dr.Pombe Magufuli, the candidate of CCM won the presidential election. Following his election, the president has taken tough measure to fight corruption and improve governance in the country.

3.3 Legal Developments

During 2015, Tanzania enacted laws that shrink civic space, thwart online freedom of expression, and restrict the role of independent media in advancing greater transparency and access to information. The country passed the Cybercrimes Act, 2015[11] and the Statistics Act, 2015[12], and it attempted to rush through parliament the Media Services Bill and the Right to Information Bill without allowing any input from either citizens or stakeholders.

The Cybercrime Act 2015 was reportedly passed in the middle of the night[13] and has been criticised for disregarding press freedom and freedom of expression, granting excessive powers to police, and limited protections afforded to ordinary citizens.[14] It imposes tough fines and at least one year of jail time for sending unsolicited messages via computer, and prohibits publication of false, deceptive, misleading or inaccurate information. It penalises citizens who receive unauthorised computer data, regardless of whether content is received with intent or not. On the upside, this law imposes heavy penalties for cyber bullying and also proscribes production and dissemination of racist or xenophobic material and publication of material that incites or justifies genocide or crimes against humanity.

The stated objective of this law was to fight rising incidents of cybercrime such as bank fraud, mobile money theft, phishing attacks, website hacking and spoofing attacks – reportedly the common security threats in the country.[15] However, critics suggested that the timing and content of the law was intended “to control the media” ahead of the October 2015 elections. As stated by one activist: "We usually use various internet platforms to communicate our information—Twitter, Facebook, blogs, SMS, WhatsApp, etc. The use of all these forms will be rendered useless by the Act which in part criminalises transmission of any information deemed misleading, defamatory, false or inaccurate by the government.”[16]

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

10 SylivesterDomasa, TZ civil society concerned gov’t is mum on proposed new constitution, http://www.afrikareporter.com/tz-civil-society-concerned-govt-is-mum-on-proposed-new-constitution/

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

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

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

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

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

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

The Statistics Act 2015 violates the right to access information and has been criticised by Human rights groups for purportedly making it illegal for anyone to publish or communicate statistics that are unauthorised by the National Bureau of Statistics (NBS).[17] Violators of this law face a minimum fine of Tanzanian Shillings (TZS) 10 million (US$ 4,664) or imprisonment of up to a year, or both. However, the NBS defends the law, stating that it does not prohibit any person or agency such as research institutions, NGOs, and development agencies from producing and publishing their own statistics.[18] The bill was stringently opposed by opposition politicians and civil society actors who argued that introducing the law was a "desperate and calculated move by a draconian government keen on stamping out dissent and alternative views."[19]

The draft Access to Information Bill was introduced in 2015, nine years after the bill was initially published. The 2015 bill was critised for lacking detail in the procedures for requesting information and logding appeals against decisions on information requests.[20] The Bill imposes a 15 year prison term on any person who discloses exempt information withheld by a public authority. Nonetheless, the draft bill has been praised for its fairly broad scope, fairly narrow regime of exceptions, and for handing an oversight role to the independent Commission for Human Rights and Good Governance (CHRAGG).

Government also attempted to pass The Media Services Bill 2015 but shelved it following civil society protests about the lack of citizens' inputs and some restrictive clauses. The Bill under Section IV provides for the establishment of a Media Services Council (MSC) to regulate and monitor social media, print, radio and television content, among others.. A number of provisions in the Bill raise concern with regard to internet use, in particular, the licensing and monitoring of social media. Clause I (3) defines social media as online interactions among people in which they create, share, and exchange information and ideas in virtual communities, networks and their associated platform. Clause 5(b and h) of the Media Services Bill grants the MSC permission to monitor and license social media. However, the Bill does not provide clear measures on how social media licenses will be registered and monitored and whether every citizen creating a social media account should get a license.

Other proposals criticised under this Bill include professional fees, annual licencing, hefty fines for offenses, and a heavy government influence in choosing members of the media regulatory boards.

The Broadcasting Services (Content) (The Political Party Elections Broadcasts) Code was gazetted in June 2015 and sought to regulate the elections of October in the same year. Section 10 of the 2015 code deals with "online content providers", defined as "any person or entity who develops files of content for the online users or on behalf of others to be made accessible online." It stipulates requirements on online content providers "residing within or outside Tanzania territory" who create "content intended for Tanzania mainland using Swahili or any other languages which have large audiences." These content providers have to register with the Tanzania Communications Regulatory Authority (TCRA); comply with Tanzania's laws and regulations governing the operations of electronic media; and ensure that information provided in blogs is accurate, fair, factual, and balanced to all parties and independent candidates in the elections.[21]

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

In February 2015, Tanzania enacted the Electronic Transactions Act.[22] Communications minister Makame Mbarawa, defended this law and the Cybercrimes Act, saying"There is a perception that the laws have been introduced to weaken people's freedom of opinion and expression, but they are aimed at protecting the people" from computer and cyber crimes.[23]

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

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

19 Tanzania passes draconian Bill that could hit publishers hard,

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

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

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

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

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

Tanzania has various laws that cater for lawful interception of communications. The most explicit is the Prevention of Terrorism Act, 2002[24], which states in Section 31 that subject to a police officer obtaining prior written consent from the Attorney-General, he may apply to court for an interception of communications order for the purposes of obtaining evidence of the commission of an offence of terrorism. The Court may make an order requiring a communications service provider to intercept and retain specified communications or it may authorise the police officer to enter any premises and to install any device for the interception and retention of communications.

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

In its 2014 Transparency report[25] , Vodafone a major operator in Tanzania noted that the EPOCA and its regulations can also be used for blocking URLs and IP addresses and performing service shutdown, the law does not provide for judicial review of the TCRA's use of its power. For its part, Vodafone stated that it has not implemented the technical requirements necessary to enable lawful interception and therefore did not receive any agency or authority demands for lawful interception assistance during 2014.[26]

Tanzania also maintains some archaic laws such as the Newspaper Act of 1976, which gives authorities powers to "exclude" any newspaper from operation in the "interest of the public." In 2013, government used this law to bar Mwananchi - the country's largest selling newspaper - from publishing both in print and on its website for 14 days after accusing the paper of publishing confidential government information and inciting Muslims.[27]

24 Prevention Of Terrorism Act, 2002, http://www.immigration.go.tz/downloads/Tanzania_Prevention%20of%20Terrorism%20Act%202002%20.pdf

25 Vodafone, Country-by-country disclosure of law enforcement assistance demands,
https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

26 Vodafone Law Enforcement Report, Legal Anne, June 2014,
http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf

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

4. Survey Findings

4.1 Knowledge, Attitudes and Practices on Internet Freedom

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

Frequently Used Communication Technologies

Mobile Short Message Service (SMS) was the most frequently used communication technology with all respondents indicating using it daily. Email and WhatsApp came in second with 90% of respondents using them daily. Viber and GooglePlus were among the least used technologies, with 46% and 41% of respondents respectively indicating having never used them.

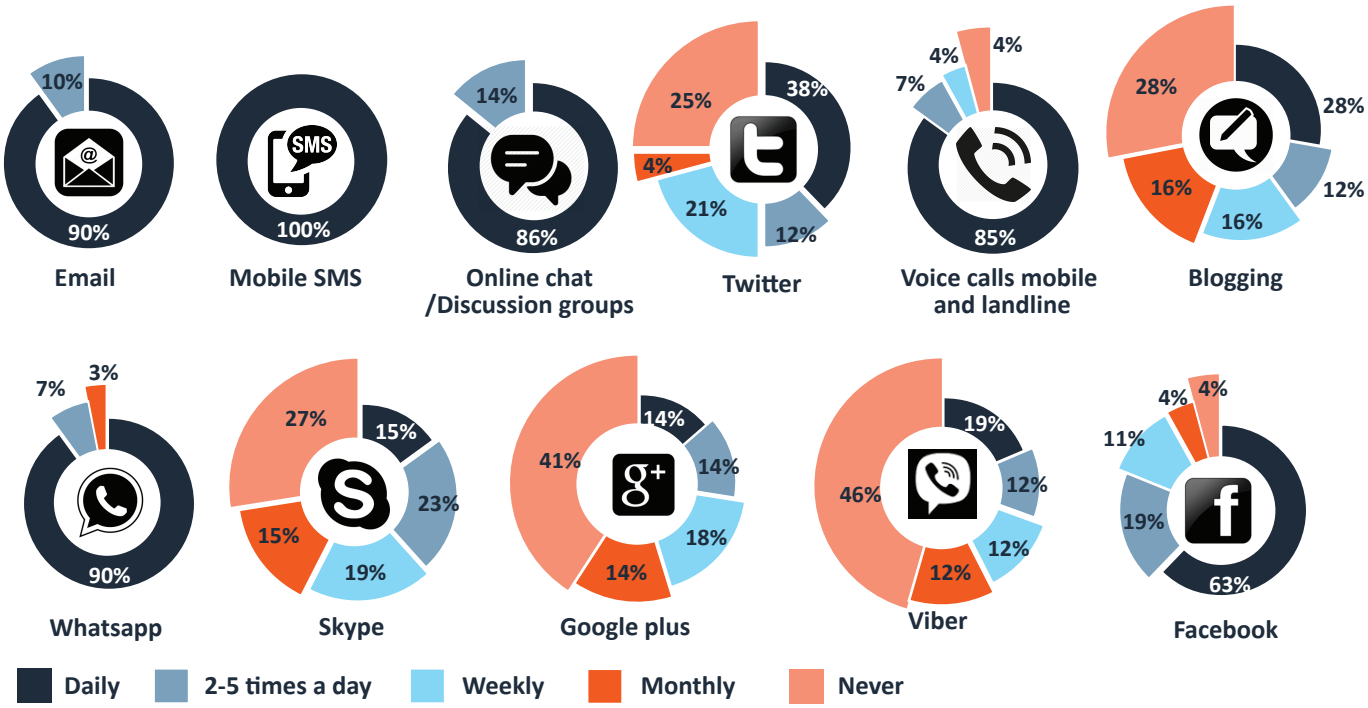

Figure 1: How regularly do you use these communication technologies?

Understanding of Internet Freedom

In response to the question of what is understood by the term 'internet freedom', many respondents provided a description which included aspects of use of the internet free of interference or censorship by the government and telecoms service providers.

Notable quotes of understanding of internet freedom

"Being able to access, share and upload things on the internet freely with no hindrance from any authoritative figure" – Journalist

"To access and utilise the internet as part of my human rights as stipulated in the constitution of Tanzania of 1977" – Activist

"The use of internet without any external interference" – Journalist

"The act of engaging on different online platforms without any kind of censorship" – Journalist

"Internet freedom is where people use the internet without interference from third parties" – Tech/app developer

"A situation that allows people to use internet as a platform to learn and socialise without restriction except in cases of insults or disrespect." – Telecom/ISP Rep

"The ability to use the internet freely for all members in the society without government- imposed obstacles or without obstacles from anywhere." – NGO rep

Knowledge of Privacy and Security in Digital Communications

None of the respondents indicated having no knowledge of privacy and security in digital communications at all. Nonetheless, knowledge was low, with only 10% rating themselves as having excellent knowledge, while 56% indicated having a good level of knowledge on privacy and security in digital communications. These were mainly techies and human rights defenders. Over a quarter of the respondents thought their knowledge on the subject was workable or poor, with academics dominating this group.

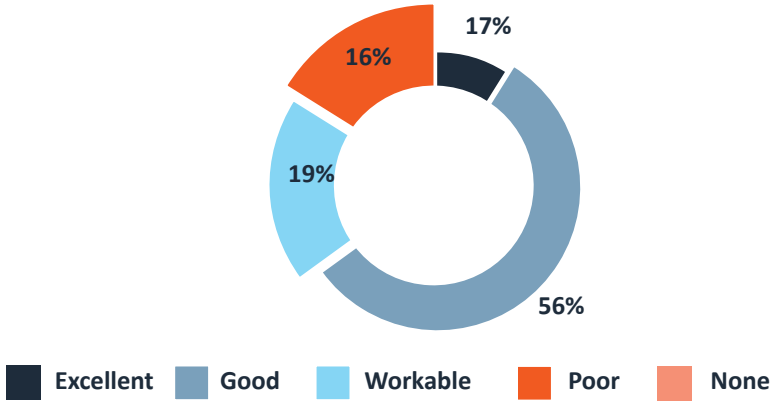

Figure 2: How would you rate your knowledge of privacy, security and unfettered access to digital communications?

Privacy and Security Concerns in Communications

Respondents were most concerned about their security and privacy in communication conducted over email, mobile (voice and SMS), and social media (Facebook, Twitter, Whatsapp, Viber and Instagram). Those who shared this were direct victims of privacy invasion on Whatsapp, Facebook and Twitter, hence their concerns over these particular platforms. Some of these respondents gave examples of instances where their voice calls were recorded without their knowledge and "used negatively." In other cases cited, screenshots of private messages were shared with non-intended recipients. The circumstances under which the recordings and screenshots were taken were not political but social, relating to friends, acquaintances and family.

For some, privacy and security concerns prevailed for all communication between security organs and individuals, between politicians and the media, and between security institutions. One respondent noted that security and privacy concerns were common for any communication involving "negative issues that may trigger violence in the community". He cited the example of messages intended to trigger religious hatred.

Use of Digital Safety and Security Tools

Majority of respondents (65%) had used tools and technologies to help protect their privacy and security online whilst 35% had not. The use of tools was common among respondents from telecom companies, internet service providers, and non-government organisations. Only a few journalists used the tools – primarily those who have been exposed to the tools through online security workshops or had been introduced to the tools by colleagues who had benefited from such training. The tools utilised were sourced through online purchases, IT personnel at places of work and online security trainings. Other tools used were as a result of factory pre-installations on devices or as part of software packages.

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

Among the most commonly used tools were: Cyberoam, Hotspot Shield, LastPass, Anti Virus softwares, Firewalls, TOR browser, and Text Secure. Password security was used through the application of "complex passwords" and two-factor authentication. Other tools mentioned were Wired Equivalent Privacy (WEP) and Telegram.

"Telegram is an excellent application for privacy," said one respondent.

Among those who did not use any privacy and security tools, a lack of knowledge and trust were the hindering factors, "I don't trust any technological tool for my privacy and security online," said one respondent, while another stated, "I know very little about stuff like Virtual Private Networks (VPN) or TextSecure. Using them takes time and makes processes slow." One human rights defender was not sure if digital safety and security tools were in place at his organisation. He said, "Maybe our IT staff use some form of tools to generally protect office data, I have no idea." He stated that he personally did not use any.

Notable quotes

"Apart from passwords for my emails and other social media accounts, on my phone and laptop, I really haven't used any kind of online protection." – Private sector respondent.

"I use Facebook privacy settings. It keeps away people who want to tag me in nude photos." – Journalist.

Perceptions of Government Monitoring and Surveillance

Over three quarters (80%) of respondents believed that Tanzanian government agencies were monitoring and intercepting citizens' communications while only 20 % thought otherwise.

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

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

Technologies and Tactics Employed in Online Monitoring, Surveillance, Filtering and Censorship

State monitoring was believed to be achieved through orders from the police orders and the communications regulatory authority. "Government gives orders to get what information they want through giving directives to police," said one respondent. "Ministry of internal affairs and TCRA are the ones who control telecom companies, internet service providers and electronic media and they request information of all activities as required," stated another respondent.

The registration of SIM card holders in the country was cited as a means to enable surveillance of citizens' communications. The EPOCA Consumer Protection Regulations 2011 and EPOCA Licensing Regulations, 2011 provide for the registration of SIM cards. Service providers are required to collect subscriber information including full name, identity card number and the physical residential or business address of a potential subscriber. However, the country has no data protection and privacy law hence making users' data vulnerable to state abuse.

A respondent from an NGO alluded to the importation of "some machines" for monitoring and the training of government officials in their use, but he was unable to clarify what kind of machines they were and when they were imported. Two respondents mentioned the use of "special software" and the monitoring of IP addresses for online activities. Again, it was not possible to establish what this software was, or whether Tanzanian government authorities possess surveillance software.

One respondent mentioned government "intimidating the owners" of some sites with critical content or those of organisations which defend human rights. Indeed, a media activist admitted having been summoned by authorities "several times" to answer questions relating to content on online discussion forums regarding his stance on internet freedom in Tanzania.

4.2 Threats to online access, privacy and security

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

Who is Likely to Violate Citizens' Internet Freedom?

Law enforcement agencies such as the national police and intelligences services were indicated by 47% of respondents as the most likely to be involved in violation of internet freedom.Specifically, the national police and intelligence services were mentioned. Politicians and intermediaries followed, both were mentioned by 25% of respondents. Fellow citizens were perceived by 22% of respondents as highly likely to violate other users privacy and security, while application developers were perceived to be least likely to violate user rights by 28% of respondents.

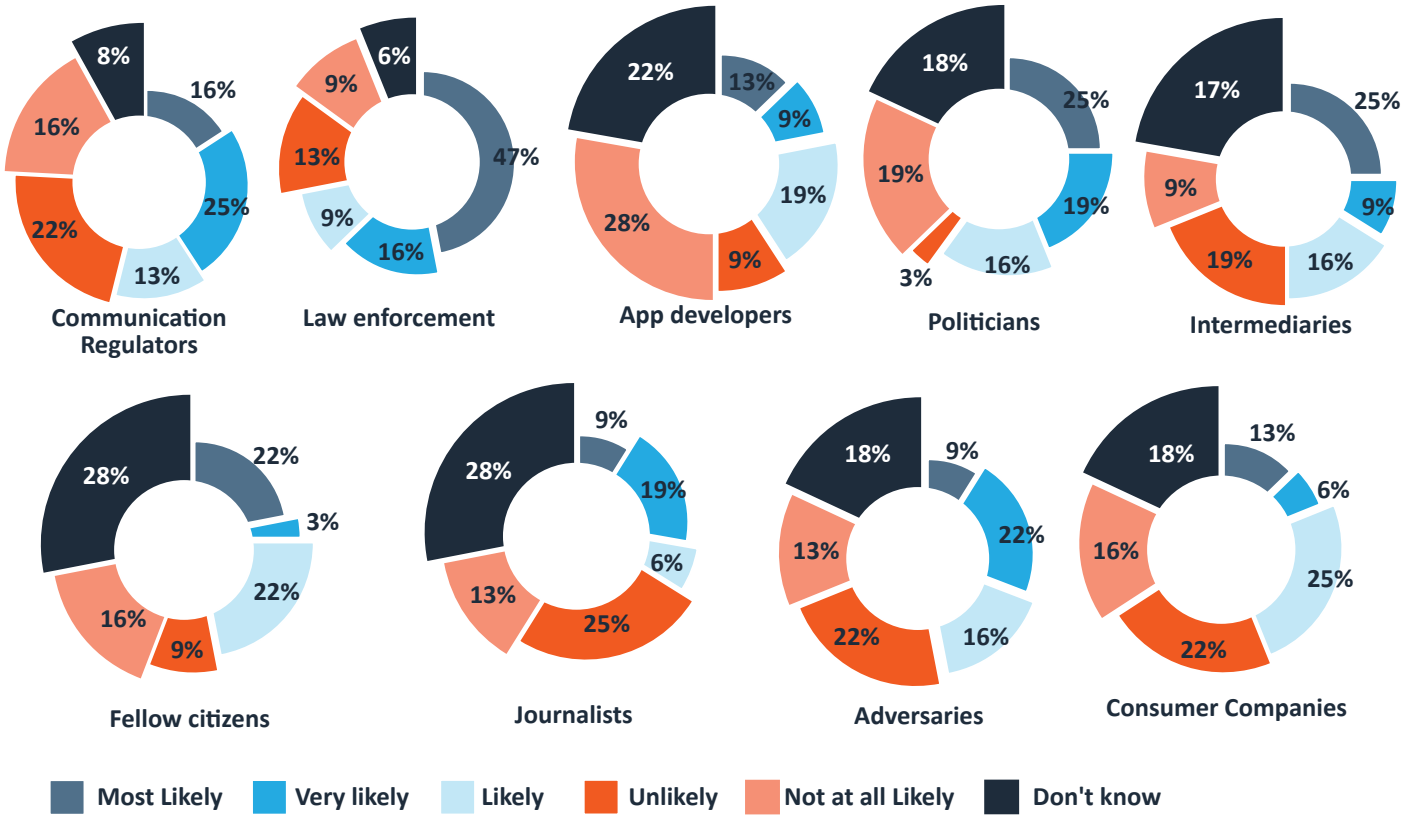

Figure 5: Who are the most likely to violate privacy and security of citizens' and organisations' communications?

Major Causes of Privacy and Security Vulnerabilities

The major causes of privacy and security vulnerabilities in Tanzania were cited as being the result of a corrupt government and the lack of transparency in administration. This led to government surveillance practices for "fear of an informed citizenry." A journalist noted "ignorance and shortage of relevant IT experts in most public and private institutions" as a big privacy and security vulnerability in the country. Lack of user knowledge of digital safety and security was said to cause vulnerability of user devices and content especially to hackers and adversaries with malicious intent. Inadequate communications network infrastructure especially in cases of quick recovery of lost content and ineffective firewall protections, as well as the emerging threat of terrorism, was also mentioned.

Meanwhile, the lack of professionalism, ethics and technological know-how was said to result in some users not being able to censor their content before sharing it online.

Adequacy of Measures to Protect Citizens From Illegal Monitoring of Communications

When queried on whether there were adequate measures to protect citizens from illegal monitoring in Tanzania, 88% of those surveyed had a negative response. Only 12% thought sufficient measures were in place. These made reference to the recently enacted Cybercrime Act of 2015 which provided for recourse in case of infringements. The respondents who found the measures inadequate suggested the need for enactment of progressive laws to protect users' privacy. Other suggestions made towards improved measures to protect citizens' communications included the "prohibition" of unwarranted interception of communications, digital safety and security skills training drives and increased advocacy and awareness campaigns on online rights.

One respondent suggested that internet infrastructure should be locally owned to ensure citizens' safetyin accordance with national legislation as opposed to the laws of the host countries of the relevant telecommunications companies. Another recommended that the government should "develop guidelines which clearly show why citizens should be monitored to avoid any ambiguity and develop fair methods to prosecute those who violate the rules."

Figure 6: Are there adequate measures to protect Tanzanian citizens from illegal monitoring of their communications?

Respondents who felt that telecommunications service providers had a role to play in protecting subscribers' privacy and security urged the companies to put in place policies that ensure the confidentiality of customers' personal information and communications "at all times." "They are key players in getting people connected and therefore, should get involved in advocacy of good use of communication systems," noted a media activist.

Without stating why, other respondents saw no role for telecom companies and service providers to play in protecting privacy and security of subscribers' communications. Some were of the view that telecom companies were already playing their role in ensuring users' privacy and security. "All telecom companies have the rules and regulations which do not allow them to expose their subscriber's information," noted one respondent. Another felt that telecom services providers already had strong measures in place to protect subscribers.However, he added that in cases where a telecom company received a government request for user information, "there is nothing they can do but reveal everything."

4.3 Effect of Information Controls on Communication Behaviour

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

To Communicate or Not to Communicate Because of Security Risks

Majority of respondents (57%) stated that they have in the past decided not to communicate or share information because of a security risk; 43% had not. Among the reasons cited by respondents for choosing not to communicate was fear for their safety due to the introduction of the Cybercrime law and hackers. One respondent stated that he had been receiving "strange calls" from unknown individuals who wanted to meet him physically. "I had to stay offline for a while because I wasn't comfortable with the situation," he said. Others indicated not transacting on mobile money because "it is not safe", and not using websites that request for email addresses or names.

Figure 7: Have you ever made a decision not to communicate or share information because of a security risk?

Other respondents noted that privacy and security were a particular concern regarding the communication of sensitive government information - such as information which is considered as top secret especially when it involves high level government officials. This perception was related to recent scandals which exposed high level corruption in government, such as The External Payments Arrears (EPA), and the Independent Power Tanzania Ltd (IPTL) relationship with Pan-African Power Solutions (PAP).[28]

One critical blogger stated that he was afraid of sharing sensitive government information. "I got a hold of contracts that were signed by officials in the Prime Minister's office. There was something going on in Moshi Kilimanjaro. I could not do anything with the documents [as] I feared for my safety," he said. Similarly, a journalist explained, "As a columnist and someone that spends significant time on social media, I am well aware that my views may be watched and thus I have come to learn to censor my thoughts on social media." Another journalist stated that he chose not to communicate on "a regular basis" due to the nature of his work saying that, "communications are porous and little can be done to remedy the situation when things get out of hand."

Others stated that they did not share information deemed "disturbing" such as pictures of deceased people or information that was likely to "trigger violence in society."

Of the respondents who stated that they had never decided not to communicate because of a perceived security risk (43%), one cited the nature of their work as the primary determinant. "I work in a PR firm, whatever we communicate is open. There is nothing to hide in conversations therefore I can never think of not communicating anything," she said.

Common Challenges Faced Related to Internet Freedom

Respondents mentioned the lack of technical skills to secure their online activities, restricted access to social media (particularly in workplaces due to ICT policies), and hackers as common challenges to their use of the internet. Respondents acknowledged that the challenges faced online had directly influenced their security precautionary measures, tools and practices. In general, the perceived security threats prompted many respondents not to easily share "sensitive" content through online platforms. These respondents were actively seeking alternative ways to safely communicate. The use of pseudonyms was a norm in various social media platforms where there were heated debates. Using technical tools for safety, securing personal devices, and not sharing sensitive information such as personal and banking information online, were among the precautions adopted in light of existing challenges. "I use Hotspot Shield and aliases on several accounts. It makes me strengthen my safety in different ways," said one media practitioner. "The challenges have influenced me to take precautions like installing more security applications on my different devices," a blogger noted.

For one media respondent, the challenges associated with online security prompted him to"learn more about security and dangers of digital communication." Others indicated having adopted organisational practices that promoted staff security and privacy. "Existing challenges prompted me to train my fellow staff on privacy and security online," said a respondent who works with an NGO. One media activist said, "The (challenges) make it necessary to keep reminding colleagues on what is safe and what is not. But also the challenges push me to constantly be in search of better and simpler tools for them to use effectively."

28 The East African, Tanzania taxman reverses 'fraudulent' takeover of firm as escrow row heats up, http://www.theeastafrican.co.ke/news/New-twist-in-Tanzania-IPTL-escrow-saga/-/2558/2539600/-/qo3lim/-/index.html

5. INCIDENTS OF INTERNET FREEDOM VIOLATIONS

Respondents were not aware of the nature of government disclosure requests made to telecom companies. However, they assumed that any such requests were made by security officials, intelligence and police through the Ministry of Communication, Science and Technology. The recently signed Cybercrime Act was cited as grounds for government requiring disclosure from telecoms in the future. “I am pretty sure the disclosure of customers’ information happens from time to time,” said a respondent from an NGO.

But there was some indication that police was monitoring what citizens said on social media. A trader in Dar es Salaam was charged for distributing seditious material throughFacebook by allegedly congratulating bandits who attacked Stakishari Police Station where some police officers were killed and several firearms were robbed.[29] According to the July 28, 2015 charge sheet, on July 13, 2015, Bruno Colman Kimaryo "with intent to excite disaffection against Tanzania Police Force, distributed seditions publication by way of social network namely Facebook to a group namely Tanuru la Fikra".

Respondents were generally also not aware of instances where service providers and telecom companies had not complied with government disclosure requests. A respondent was of the view that prior to the enactment of the cyber crime law, ISPs and telecom companies could refuse to provide user information to government authorities.. However, since the law was passed, the respondent doubted that it would be possible to reject such requests.

According to the latest Vodafone Law Enforcement Disclosure Report, during 2014 the government of Tanzania made 933 requests for local subscribers’ data. However, it is not possible to compare this figure to that for the previous year, as Vodafone has reported that the figure of 98,765 which it gave for 2013 was erroneous.[30]

6. CYBERCRIME

According to research conducted in 2012, a total of 627 cybercrime cases were reported to the forensic section of the Tanzania police force that year – nearly double those reported in 2007.[31] More recently, a report from Abuse Watch Alerting & Reporting Engine (AWARE), showed there were 28 abuse incidents originating from Tanzania to the outside world, between January and February 2015. Of these, three were for web defacement, seven were related to phishing, five were malware and 13 spam.[32]

29 FaustineKapama, Man who toasted Sitakishari bandits on facebook charged,

http://www.dailynews.co.tz/index.php/local-news/47770-man-who-toasted-sitakishari-bandits-on-facebook-charged

30 Vodafone, Country-by-country disclosure of law enforcement assistance demands 2015,

http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html

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

32 https://www.tzcert.go.tz/index.php/resources-2/incident-statistics/

7. Discussion

The findings of this survey show that Tanzanians frequently use SMS, email, WhatsApp, Facebook and other platforms including Instagram and GooglePlus. Respondents' definition of internet freedom in the survey indicates a fair level of understanding of what constitutes internet freedom. However, understanding was varied and in most cases was a reflection of the practice of securing (or lack thereof) of communications.

According to the findings of this survey, law enforcement agencies (police and intelligence services) are perceived to be the most likely violators of privacy and security of citizens' communications. Politicians especially from opposition were also said to be among those whose communications are most monitored, followed by journalists. This finding is very telling, given that these two groups are generally the most critical of government and are active in demanding transparency and accountability, which suggests government attempts to interfere with freedom of expression over new and traditional media through new and proposed legislation.

Freedom of expression online is curtailed by outdated legislation such as the Newspaper Act 1969. The attempted enacted of a progressive law to address media freedom further places caveat on freedom of expression online. The proposed Media Services Bill 2015 for instance has restrictive provisions that call for the establishment of a Media Services Council to regulate and monitor social media through registering social media users. However, the Bill does not provide clear measures on how social media licenses will be registered and monitored and whether every citizen creating a social media account should get a license.

Government focus on fighting cybercrime at the expense of protecting internet freedoms is evident given the rushed manner in which the Cyber Crime Act, 2015 was passed. Although cybercrime prevention is a genuine concern for both government and internet users, the findings show that there is no clear strategy on how to fight the vice while at the same time ensuring that user's rights online are protected. Further, the absence of data protection and privacy legislation puts online user at risk of surveillance from both state and non stateactos. This is further made worse existing laws that allow for mandatory SIM card registration for all telephone subscribers.

8. Recommendations

- Amendments should be made to the Media Services Bill prior to its enactment in order to elaborate on the selection and appointment process of Media Service Council members and rules of procedure of the council in preforming its functions to ensure accountability to the public, independence of the media from government, and to uphold the public's right to access a broad range of information and opinions.

- Government, civil society and private sector (particularly telecommunications companies) are urged to promote knowledge and awareness of digital safety and security through capacity building, tools provision and education campaigns.

- There should be oversight and transparency in the interception of communications to ensure authorities adhere to the law.

- Government officials should change their attitudes to allow for citizens to freely express divergent and critical views through both traditional and online media.

- Repeal provisions of laws that contradict constitutional guarantees of freedom of expression, a free press and individual privacy.

- Government should speed up the enactment of privacy and access to information legislation, following extensive consultations with relevant stakeholders such as academia, human rights defenders, the media and civil society.

- There is need for more research into internet freedom in Tanzania and beyond to enable learning and experience sharing, as well as benchmarking legislation.

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

8020fashions.com
Alliance for Change and Transparency (ACT)
bloguyawananchi.com
Chama cha Demokrasiana Maendeleo (Chadema)
Chama Cha Mapinduzi (CCM)
Change Tanzania
FikraPevu.com
IPP Media
isaamichuzi.com
Jamhuri Media Communications
Legal and Human Rights Centre
Masoko Tanzania
Mini Buzz TV
Ministry of Information, Youth, Culture and Sports
mpekuzihuri.com
New Habari Cooperations
Smile Tanzania
Start TV
Tanzania Communications Regulatory Authority (TCRA)
Tanzania Daima
Tanzania Human Rights Defenders Coalition (THRDC)
Tanzania Information Technology Association
The Habari.com
Union of Tanzania Press Clubs
University of Dar es Salaam
Vodacom Tanzania
Zantel Tanzania

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).

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