Exploring Data Anonymisation and Internet safety in East Africa

Submitted to: Research ICT Africa

Type of Document: Policy Paper

Author: Duncan Kinuthia

Date: October 2020

409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa
Phone: +27 21 447 6332
Fax: +27 21 447 9529
www.researchictafrica.net

Acknowledgement

This study was carried out during the Tech Exchange fellowship funded by the Media Democracy Fund. The author would like to thank Research ICT Africa for support as the host organization, all focus group participants as well as AccessNow for their support in gathering the Internet shutdowns data used for the study. The author also thanks the reviewers: Dr Enrico Calandro and Alex Comninos for their input.

Executive Summary

Internet adoption in East Africa has faced several challenges with the high cost of bandwidth being the key challenge. Nevertheless, once people are online, censorship, Internet privacy, geo-blocking of content and Internet shutdowns are some of the major challenges faced by Internet users in East Africa. The use of virtual private network tools for data anonymisation and Domain Name System (DNS) manipulation techniques are being adopted in the region to circumvent these obstacles to Internet use.

Maintaining anonymity over the web is a growing concern for users not only in East Africa, but also around the world. This has been fuelled by numerous data privacy breaches leading to illegal access or illegal exposure of user data collected by numerous platforms and sometimes shared with third parties. Rising censorship and geo-blocks over the Internet are also driving Internet users into a quest for anonymity online, as a means to overcome the targeted barriers.

The use of Virtual Private Networks (VPNs) has been on the rise as an effective data security technique, due to the added encryption that VPNs offer to the data during transmission over a less secure network such as the Internet. The use of VPNs for privacy and anonymity, achievable through maintaining the confidentiality of data tunnelled from a user through the VPN provider, is also on the rise to overcome these barriers. From a technical point of view, achieving complete anonymity and communication privacy is relative to the VPN provider ensuring user data privacy. There is also no standard protocol guiding user logging for VPN providers. Bugs in VPN software can also lead to privacy breaches. This makes VPNs more suitable for user privacy than for anonymity as compared to the Tor network. While users have to trust VPN providers for privacy and anonymity, the Tor network ensures complete online anonymity. DNS manipulation is also a popular technique used to hide the origin of one's traffic over the web. This is the subversion of the resolution of DNS queries, with a key aim to hide a user's real location.

There is limited data and statistics on the current level of online security and on the use of data anonymisation tools in East Africa, yet such data is necessary to inform regional and global policy debates on privacy, safety, and security online in Africa. There is also a lack of adequate research on the volumes of VPN usage and the reasons why VPNs have been used in Eastern Africa, with most of the statistical reports being done by the VPN service providers. Yet, that research can also shed light on how to make users safe and secure online. The main objectives of this study are, on one hand, to highlight what privacy, safety, and security risks East African Internet users have encountered to access to the Internet; and on the other hand, to explain why Internet users are employing data anonymisation tools in the region, focusing on the use of VPNs and DNS manipulation techniques. Last but not least, this research also provides specific recommendations on how to be safe and secure online through data anonymisation across the region.

Contents

List of Tables and Figures

List of Abbreviations and Glossary

VPN: Virtual Private Network. A connection set up to simulate a private network over a public network like the Internet and depends on the use of temporary connections that have no real presence (Erwin, et al., 1998).

GDPR: General Data Protection Regulation. A data privacy and protection regulation in the European Union laws for all citizens of the European Union and the European Economic Area.

GPS: Global Positioning System. A twenty-four satellite-based global navigation system.

IP: Internet Protocol. A set of standardized rules that govern the format, addressing and transmission of data over the Internet or other networks

DNS: Domain Name Service. This is a naming database used to resolve domain names into Internet Protocol (IP) addresses.

HTTPS: Hypertext Transfer Protocol Secure. The use of Transport Layer Security (TLS) to ensure secure data transmission and communication over a computer network.

L.T: Low technical. Individuals with limited knowledge of how to use technology to perform different tasks.

M.T: Medium technical. Individuals with intermediate knowledge of how to use technology to perform different tasks.

H.T: High technical. Individuals with high knowledge of how to use the latest and a wide variety of technological devices.

1. Introduction

Improvement of mobile broadband connectivity in East Africa has led to an increased number of Internet users in the region over the last decade. This has led to the adoption of digital communication and commerce services in the region, which has transformed economic and social practices. Through technology, East Africans now have access to information on market prices, health, weather and good farming practices (Kende-Robb, 2015). Nevertheless, considering that Internet use in the region is still a relatively young phenomenon, data privacy and Internet security remain key challenges facing novice Internet users in Eastern Africa. Cybercrime has been on the rise in Eastern Africa, with both individual users and organisations making massive losses from cyber-attacks (Serianu, 2017). For many East African Internet users, social media is the Internet, as a majority of Internet users in the region mainly use it exclusively through social media platforms. The growing episodes of Internet censorship (Matfess & Jeffrey, 2018) in the region, hence, massively affect social interactions between users as social media platforms are the main targets of this censorship. The social media usage tax in Uganda has also been a key challenge to the use of the Internet in the region for the past year. The introduction of the Over The Top (OTT) tax led to a decrease in the number of Internet users in Uganda by 30% between March and September 2018 (Esselaar, 2019). Geo-blocking of entertainment and educational content is also a barrier to access to knowledge and information for East African Internet users where a lot of content is unavailable due to limited profitable markets for content providers or due to copyright and content licensing restrictions. The use of circumvention and data anonymisation techniques has emerged as an effective way to mitigate all the above challenges, at least for tech-savvy users. Eastern African Internet users have hence started adopting several data anonymisation techniques to evade different forms of censorship and blockages, and to ensure information privacy and security over the Internet are maintained and respected.

Virtual Private Networks (VPNs) are the most used anonymisation tools by Internet users in East Africa to maintain access to censored social platforms (Atieno, 2016). The added encryption of data by VPNs ensures protection against cybercriminals who might be interested in intercepting data and communications on the Internet. In addition to VPNs, the manipulation of DNS records through the use of services like Smart DNS[1] is a growing practice, especially to circumvent geo-blocks imposed on content over the web in East Africa. Smart DNS provides proxy DNS servers across the world, and Internet users have the freedom to select their DNS server locations. The unencrypted form of DNS requests makes it possible for these requests' manipulation, but with the upcoming new DNS over HTTPS, DNS manipulation is becoming a challenge. Although the use of VPNs and DNS manipulation techniques for data anonymisation is evident in East Africa, without the necessary statistical evidence on the scope of and reasons for this phenomenon, it is difficult to inform national, regional, and global policy debates on data anonymisation in the region. Most East African VPN users rely on VPN service providers for data anonymisation, but past experiences have revealed that some of these providers keep user activity logs and confidential user details stored, which might expose these users to surveillance practices. A need to assess what the most commonly used VPN providers are, is hence crucial to identify and recommend the most trustworthy VPN providers. There is also a lack of non-biased, neutral VPN provider reviews, as much of the reviews are driven by industry. Last but not least, raising awareness on safety and security online in East Africa is also required to win the fight against cybercrime in the region because while organisations invest in the improvement of information security

[1] A service that offers the subversion of the resolution of Domain Name System queries for Internet users. See more: https://www.smartdnsproxy.com/

technologies, uneducated Internet users remain the weakest link and a key target for hackers (Aloul, 2012).

2. Understanding Data Anonymisation Techniques and their Use in East Africa

Data anonymisation is the process of de-identifying sensitive data while preserving its format and data type (Balaji, 2013). The key driver for data anonymisation is the need to protect the privacy or the confidentiality of personal data.

Data anonymisation can be defined as the removal of personally identifiable information from data sets either through the deletion or encryption of this information. The key aim of data anonymisation is to make it difficult or impossible to relate a data set to a particular individual. Unlike data pseudonymisation, anonymisation of data ensures that sanitised data cannot be re-identified. The cybersecurity Confidentiality, Integrity and Availability (CIA) model defines important goals to ensuring that data is handled appropriately. Confidentiality ensures the privacy of data, where only authorised persons should have access to private information. The integrity of data ensures that it is not changed from its original form maliciously or accidentally during transmission, storage or processing. Availability guarantees that users should have the ability to access any technological resources, both hardware and software, that they require when they need them, securely, enhancing efficiency and reliability (Nweke, 2017).

According to the General Data Protection Regulation (GDPR), there are two categories of personal confidential information (Irwin, 2018). They are the personal identifiers and personal characteristics data points:

Personal Identifiers	Personal Characteristics
Name ID (Social security or driver's license number) Physical address E-mail address Photo IP address GPS location	Ethnic background Political views Religion Physiological data like DNA Medical conditions

Table 1: Categories of personal data

Source: Data science under GDPR with pseudonymization in the data pipeline (Lindquist, 2018)

Data anonymisation disables the correlation of personal identifiers with other data through one-way hashing, encryption or the deletion of personal identifiers data. Unlike pseudonymization where another attribute is created to link personal identifiers to the anonymized identifiers, de-anonymisation of anonymized data is impossible.

2.1. Online Anonymity

Online anonymity is the ability of an Internet user to interact with the Internet without their identity being revealed to another user or a third party. There is a distinct difference between online privacy and anonymity. While online anonymity prevents disclosure of the identity of an Internet user, online

privacy is the protection of user information, activity and identity from unauthorized access. Anonymity is achieved through the protection of the privacy of a user's identity only (Edmundson, 2018). Online identity is primarily done using the IP address, which is a numeric (IPV4) or a hexadecimal string (IPV6) that is assigned to all devices connected to the Internet and that use the Internet protocol for information exchange. The two key functions of the IP address are to identify the network interface or host and as well as the physical location of the host. Although IP addresses are most often assigned temporarily to Internet users per session in dynamic IPV4 and stateful IPV6 configurations, Internet Service Providers (ISPs) log the assignment information, which can be used to identify an Internet user even after they log out of a session (Palme & Berglund, 2004). Online anonymity hence targets spoofing an Internet user's IP address, complemented by the use of fake identities over the web for full anonymity.

While users in East Africa use online anonymity to mitigate censorship and gain access to geo-blocked content, online anonymity has been a contributing factor to rising cybercrime in the region, which has led to debates on the harm and psychological effects resulting from online anonymity. According to (Goleman, 2011), cyberbullying, a common and growing social threat to teenagers can be facilitated by the anonymity of communication interactions and social distance over the Internet. However, obviously online anonymity is the only cause of this phenomenon (Gackenbach, 2011). Nevertheless, linking true online identities to users may logically be an effective deterrent to control this toxic disinhibition (Suler, 2004). Online anonymity has also been found to improve interactions between some users as lack of eye contact and invisibility possess significant positive effects on personal self-disclosure, an effect called benign disinhibition (Lapidot-Lefler & Azy, 2015). However, there is no evident scientific consensus on whether online anonymity has a positive or negative psychological effect on Internet users. Although this research does not explore the psychological effects of online anonymity in more depth, it evaluates how free Internet users in East Africa feel in online interactions and in sharing their information on online social platforms.

There are many approaches used to achieve anonymity over the Internet. The use of fake identities over the web is the most popular practice on social media sites and other platforms that require every user to have an account to access the services. The use of IP address modification tools is a common practice as it ensures that the user and their physical location is virtually unidentifiable (Sudhanshu & Kumar, 2015). There are different ways to achieve this, with the key ones being the use of proxies, VPNs and anonymous networks like the Tor Network. This research focuses on the use of VPNs and DNS proxies.

2.2. Virtual Private Networks

A VPN simulates a secured private network over an insecure public network like the Internet, by providing a temporary (virtual) connection over the network (Erwin, et al., 1998). VPNs provide Internet security and relative online anonymity. This is enabled by the four key technologies implemented in VPN networks that are firewalls, authentication, encryption and tunnelling (Erwin, et al., 1998). While the use of VPNs ensures data privacy, security and online anonymity, some VPN providers are compromising the effectiveness of VPN networks by logging user activities. This is despite the VPN providers' promise to users that they do not keep user logs. For instance, in 2016, a Pure VPN user was charged with cyberstalking after records from the VPN provider revealed that the user was using a false identity for this cybercriminal activity (Chirgwin, 2018). Cyber-attacks on VPN providers have, in the past, lead to the breach of VPN users' private data and passwords. This makes the selection of a VPN provider very crucial for a user, before subscribing to its services.

2.3. DNS Manipulation

Internet routing is done using IP addresses that are machine-readable but not efficient for human use, hence the use of hostnames that are resolvable to IP addresses. DNS resolution queries and requests are done by recursive public DNS servers, which are servers around the globe that hold a distributed directory for hostnames to IP addresses resolution. ISPs assign recursive servers automatically to clients depending on the client's network settings, for convenience and congestion reduction. However, users possess the flexibility to select their recursive servers, giving them the ability to manipulate the DNS resolution path (Gayathri & Liu, 2015). DNS manipulation is done through the use of private DNS proxy servers, which intercept DNS queries sent to the public DNS server and respond with DNS answers resolved by alternate nameservers instead (Gayathri & Liu, 2015). DNS manipulation is mainly used to navigate around content geo-blocks and censorships, by using DNS proxies that are in the regions without the geo-block. However, it is crucial to note that DNS proxies do not offer the data encryption function provided by VPN, hence their use cannot guarantee data integrity and privacy. The trade-off in this is that DNS proxies are faster than VPN connections due to the lack of real-time encryption offered by VPN.

2.4. The use of VPN and DNS Manipulation in East Africa

The East African region is located on the geographical eastern part of the African content and covers Burundi, Djibouti, D.R. Congo, Eritrea, Ethiopia, Kenya, Rwanda, Somalia, South Sudan, Sudan, Tanzania, Uganda. The digital divide is vast in East Africa but Not for Government Organisations (NGOs) and governments are stepping up to put an end to it (Secorun, 2017). As a result of this effort, the region's access to the Internet is on the rise due to the development of mobile broadband infrastructure, a reduction in prices of mobile devices as well as a reduction in the cost of mobile data bandwidth in the region. Initiatives led by governments in collaboration with NGOs and private organisations have also enhanced access and the use of the Internet in the region. For instance, Facebook's Internet.org is an example of a private sector led initiative to bring Internet access to remote regions in Easte Africa through the Express Wi-Fi project. Another initiative worth mentioning is the Kenyan Laptop Project, a governmental project to eradicate the digital divide, also aimed at improving technological innovation in the country. There is an increase in the number of tech-based start-ups in the region. Initiatives by Huawei, Microsoft and Google have also led to increased investments in research, science and technology in the region. Growing innovation in the region can be seen through the efficiency of mobile payments in Eastern Africa, making it a worldwide benchmark for mobile payment.

However, although there has been a remarkable growth in the number of Internet users in East Africa, over the last decade, subscriber growth rate has gone down in the second half of the decade due to several challenges facing the adoption of the Internet in East Africa. The high cost of bandwidth is a key challenge facing the growth of Internet users in the whole Sub-Saharan African region (Gillwald & Mothobi, 2019). More Internet penetration is hence evident in countries with a higher gross domestic product per capita, for example, Kenya and Tanzania, as there are more people that can afford Internet subscription fees. The proposition of the removal of roaming charges has also failed in the region. The project started in 2015 and had brought together Uganda, Kenya, South Sudan, and Rwanda, while Tanzania and Burundi never joined the project. Telecommunication authorities blame discordant tax policies across the region for the failure of the project (Wakabi & Anyanzwa, 2018).

In addition to overcoming the above challenges to accessing Internet services in East Africa, the use of the Internet has also faced several obstacles in the region, which has led to the quest for data

anonymisation by existing Internet users. Internet censorship has risen in East Africa in the last five years, with governmental attempts to muzzle free speech and political opinions, especially during elections (Matfess & Jeffrey, 2018). Internet users in Ethiopia are the latest victims to experience this, after a ten-day Internet blackout following a report of an attempted coup in the country, paralysing business operations and social interactions in the country. Internet blackouts have also been experienced in many East African countries including Uganda, Ethiopia, Democratic Republic of Congo and Burundi, heavily costing businesses in the region, as shown in Figure 1 below.

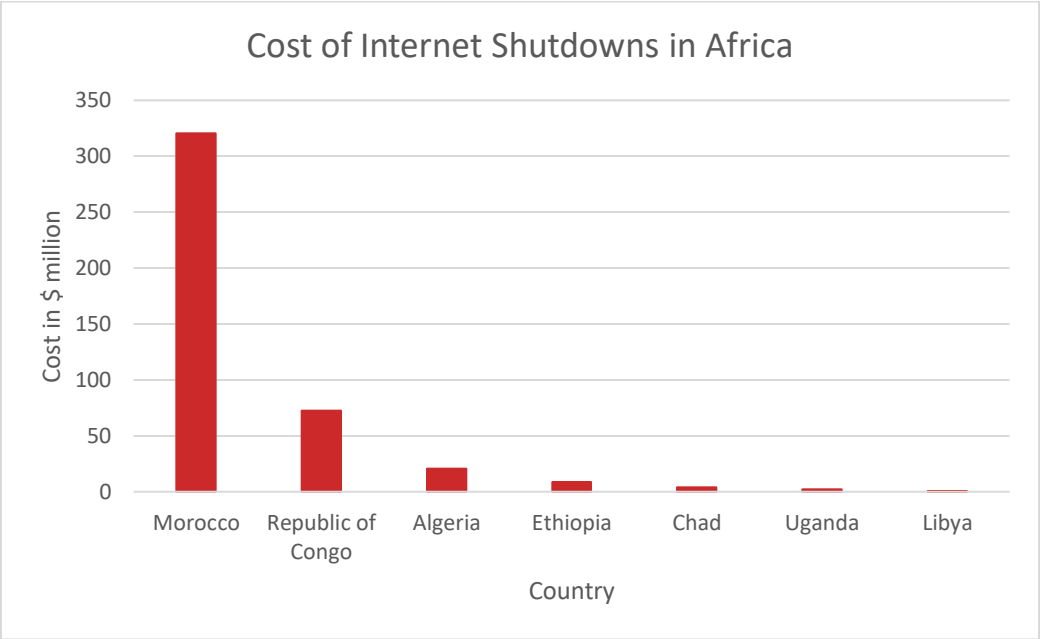

Figure 1: The cost of Internet shutdowns

Data source: theatlas.com

The Ugandan 2018/2019 budget saw the introduction of a daily $0.05 OTT services tax, which is a tax imposed on the use of social media platforms in the country. This affects Internet users who use Ugandan ISP's SIM cards to access the Internet. The use of over fifty major and minor social media platforms was affected by this new tax.[2] The new OTT tax is paid by the Internet users directly through the ISPs and access to these social platforms is denied unless the OTT tax is paid. At the same time, the country also experienced an increase in mobile services tax. This amounts to around $19 annually, and together with the high costs of data bandwidth, these costs heavily curtail social media use, given that the gross domestic product per capita in Uganda was only $604 in 2017. This was a huge blow to the users, as over 88% of Internet users in the country primarily use the network for communication through social media. In response to this increase of Internet use costs, the Ugandan Taxes Survey Report by Whitehead Communications Uganda revealed that 57% of respondents turned to the use of VPN to bypass the OTT tax as shown in table 2 below.

[2] See https://ooni.org/post/uganda-social-media-tax/#social-media-tax for a list of all the social media platforms affected by OTT tax.

Response	Frequency	Percentage
Paid the OTT tax	1,089	40%
Used VPN	1,545	57%
Use Wi-Fi hotspots	1,036	38%
Other	91	3%
Total	2,696	

Table 2: Users' response to Ugandan OTT taxes

Data Source: Uganda Social Media and Mobile Money Taxes Survey Report

Therefore, VPNs are the most used anonymisation tools by Internet users in East Africa to maintain access to censored social platforms (Atieno, 2016) or to avoid social media taxes.

Geo-blocking is another challenge facing the effective and free use of the Internet in East Africa. A lot of entertainment and educational content is unavailable in the region due to copyright and licensing issues or lack of a profitable market for content providers, given that Internet adoption is still very low in East Africa. Examples of geo-blocked content in East Africa include Pandora, Hulu, HBO Now, much of Netflix, CBS All Access, Amazon Video, Google Music, Google Books and Spotify. The use of DNS proxies (Smart DNS) to access geo-blocked content is preferred by a majority of users compared to the use of VPN. The added encryption in VPNs makes it slower for content streaming as compared to Smart DNS, hence the popularity of Smart DNS for the streaming of online content (Jones, 2018).

2.5. Use of VPN in response to increasing cybercrime

VPNs are not only used to avoid Internet censorship and social media taxes, but are also promoted by government organisations to maintain online privacy and safety and security online. Governmental and non-governmental initiatives to fight cybercrime are on the rise in East Africa, with a focus on raising awareness to the public. For instance, the National Kenya Computer Incident Response Team Coordination Centre is an example of a governmental initiative to curb cybercrime. As part of their cyber awareness and education programmes, they are educating people on the use of VPNs for online privacy. This initiative aims at informing Internet users on the different social engineering techniques used by cybercriminals and on the use of tools to ensure online privacy, including the use of VPNs.

Cybercrime is a major challenge facing Internet users in Africa. Africa was described as a paradise for cybercriminals (Summers, 2018), with the continent leading, globally, in the number of losses from cyber-attacks. The cost of cybercrime in Africa is extremely high, as Figure 2 below demonstrates, with Tanzania having the highest cost of cybercrime in East Africa.

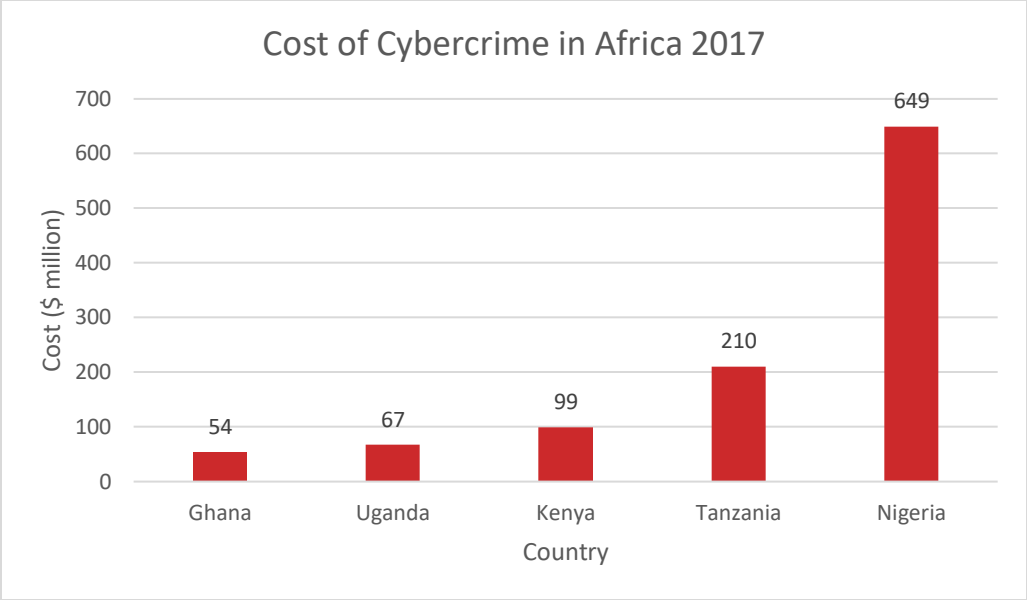

Figure 2: Cybercrime cost in Africa in 2017

Source: (Serianu, 2017).

Many African users have not had a lot of exposure to the use of the Internet, hence regional awareness to cyber threats is still low. Cybersecurity commitment on the African continent is relatively low among both individual users and organizations (Lavion, 2018). The Africa Cybersecurity Report 2017 highlighted the fact that 90% of organizations in Africa were below the security 'poverty line'[3] making them highly vulnerable to cyber-attacks. Banks are the main targets in East Africa according to the report, with other key targets being automated government services and universities.

[3] This is the annual estimated minimum level of income needed to secure a sum of all resources adequate to ensure access to the basic necessities of human life.

3. Research Findings

3.1. Internet use overview

Determining where East African Internet users spend their time on the Internet was crucial to the understanding of data anonymisation in the region. As expected, the cost of communication determines how people use the Internet in Kenya and Uganda. The Internet is mostly used for social media across all skill and age groups. Both less and more skilled IT users are aware of data bandwidth cost and use. "*Most of the time I mainly turn on data on my phone to reply to messages on WhatsApp and Facebook, otherwise my data will be turned off*" (female, L.T., Uganda). The most famous apps are WhatsApp and Facebook, with all focus group participants having both a WhatsApp and Facebook account. WhatsApp, as a means of communication, is also dominant over the use of Short Message Services (SMS) and calling, as not only is data cheaper than calls and SMS, but it also embeds the ability to send multimedia files cheaply, easily and efficiently. "*I have noticed that WhatsApp uses less data bandwidth than other applications such as Facebook and Instagram. It is also easier to chat over WhatsApp than the other platforms and also SMS*" (male, M.T., Kenya).

The prevalence in the use of both WhatsApp and Facebook in Kenya and Uganda can also be attributed to the use of the two platforms for e-commerce, social interactions, work, entertainment, and education. "*My twelve-year-old niece follows Facebook pages that offer cooking tutorials and she learns how to make good dishes from them*" (female, M.T., Uganda). Business owners use Facebook pages and groups to market and sell their goods while users log into the platform to search for any item that they would like to purchase. *"These days, small businesses especially fashion boutiques use their Facebook pages to display their products and I can easily order from them through direct messages. There are also Facebook groups where members post any item that they would like to sell in search of customers"* (female, M.T., Kenya). Work and profession related WhatsApp groups are also common in the region, with all the participants reporting that they have been in a work or educational related WhatsApp group at some point. Other social platforms such as Twitter, Instagram, Snapchat, Reddit and dating platforms are more common among the medium to high IT skilled users below 45 years age groups. Social platforms are also used to facilitate sports betting, which is another dominant use of the Internet, across all technical levels, especially among the male users. Only one female participant had an idea about how online sports betting works. Football is the most popular betting sport in Kenya and Uganda.

The use of the Internet for entertainment and content streaming was more dominant among the medium and high technical groups, with the high cost of bandwidth and the lack of free Wi-Fi hotspots being reported, as the key challenge to streaming online content. However, service providers are stepping up to offering solutions to this, like data bundle subscriptions that offer some free YouTube access bandwidth, including the Safaricom Kenya 5GB free YouTube bandwidth offer,[4] with every data bundle purchased. The most dominant online entertainment platform is YouTube, with all the participants having used it or having the knowledge of its existence, as opposed to other platforms such as Netflix and Amazon Prime. The use of the Internet for educational research is more dominant among the medium to high-level technical Internet users in Kenya and Uganda, with Google Search being the main online research tool. Internet use to specifically access news material was the least common among all the participants, with most of the participants reporting that social platforms also act as a good source of news. "*I have never logged into the Internet to specifically access news unless there is*

[4] See https://www.capitalfm.co.ke/business/2019/05/safaricom-monthly-bundles-to-offer-free-5gb-youtube-streaming/ on more about the Safaricom Kenya free YouTube bundle

breaking news or during the election period. Most of the time I get breaking news from Twitter then look it up on the web for more details" (Male, M.T., Kenya).

Smartphones are the most commonly used devices to access the Internet in Kenya and Uganda, with all the focus group participants owning a smartphone. "*I use my phone to access the Internet most of the time. At home, we only have one laptop while every adult has a smartphone*. *I think my laptop uses more data bandwidth than my phone, so I mainly use my laptop while around a Wi-Fi hotspot*" (male, L.T., Uganda). Ownership and the use of tablets to access the Internet is still low in the region, with only six out of the total sixty-five participants owning a tablet.

3.2. Online security and awareness in Eastern Africa

The research sought also to determine the level of online security and awareness across East Africa and approaches that Internet users are employing to ensure their online safety. Internet privacy and security are challenges in the region, as reported by a majority of the participants. Cases of social media account hacking, online banking credentials thefts, mobile money frauds and online impersonation were among the security issues highlighted as having been experienced before by a majority of participants.

"*It is really up to the user if the user is informed and equipped to protect themselves from online attacks. However, there is a limit to how much one can know, hence at some point, we are all vulnerable. My general view is that I feel safe up to the point that I am not safe anymore*" (male, H.T., Uganda).

Cases of online impersonation and social engineering to extort money from unsuspecting Internet users were the most dominant form of online frauds experienced. In Kenya, the majority of participants reported having received text messages informing them that they won an ongoing promotion and are requested to send a small fee, as a facilitation fee, to obtain the prize money. Mobile money is the main target of digital fraud, with cases of service provider employees being arrested for being accomplices to this (Daily Nation, 2017). In Kenya, participants reported that mobile money is the target of phishing scams, used to obtain mobile money account and user credentials by cybercriminals. Victims of this would receive a call from a criminal impersonating a Safaricom employee, inform them that they noticed something unusual with the victim's mobile money account, asking for the victim's ID number and mobile money PIN. Social media accounts hacking is another dominant concern of online insecurity in the region. The two main motivations behind the hacking of social media accounts in the region are defamation and extorting of money from the victims' online friends. "*It happened to me on Facebook when I was in campus, somebody hacked into my account and asked my friends for money*" (male, H.T., Uganda). The majority of the participants reported having knowledge of similar cases, where the online criminal, after gaining access to the victim's account, asks for money from unsuspecting victims' friends. This also happens after physical theft of users' devices, with mobile money being the key channel for money transfer.

Hacking of social media accounts for defamation is mainly from victims' lovers, especially after divorces or breakups, where one party illegally accesses the victim's social media account and posts inappropriate photographs of the account owner. This mainly affects women, with the males being reported as common perpetrators of these acts. In relation to the sharing of inappropriate and offensive photographs on social media, cyberbullying and stalking were also reported. In these cases, photos are shared from the perpetrator's account, causing ridicule of the victim. "*I believe that if I share my photo with my partner and he agrees to keep it private, then to share it online later, he has violated my rights and I think he should be held accountable*" (female, M.T., Uganda). Cases of online and digital banking

thefts were mentioned by only two participants who reported to have had money stolen from their bank accounts by using digital or online banking. "*I used my Mastercard to pay for a course online, but after a few days, 4000 Kenyan shillings was withdrawn from my account illegally using the card*" (female, M.T., Kenya). The low number of thefts committed through digital and online banking might be due also to the fact that thirty-five participants reported that they do not use online banking as they do not trust the safety of the platforms. One of the factors that have made Jumia the most popular e-commerce platform in both Uganda and Kenya is the pay-on-delivery feature that the platform offers, according to a majority of the participants, who do not trust online payments.

Professional impersonation is also rampant in the region, with conmen impersonating employers and asking unsuspecting job seekers for a small fee in exchange for employment. "*Around two weeks ago, two people were arrested in Mukono, one of them was impersonating the Minister of Works and they had conned money from unsuspecting people on Facebook*" (male, M.T., Uganda). One participant also reported the use of LinkedIn for professional impersonation.

Regarding personal data breaches, the use of malware to illegally access a user's private information was not reported by any participant. On the other hand, online surveillance is a major information privacy concern among East African Internet users. In Kampala Uganda, there is a public Wi-Fi hotspot project that provides free Internet access to users daily from 6 pm to 6 am on weekdays and full time during the weekend, to 6 am on Monday.[5] However, some participants reported their reluctance to use the public hotspots as they are required to provide personal details before gaining access to the Internet through these hotspots. "*Why would they need all my personal identification details for me to use the hotspot? I think they are tracking what I do online*" (female, M.T., Uganda). Conversely, participants did not report any concern over the physical security of using their devices in these public places. In Kenya, the majority of the highly skilled IT participants indicated their concern over the recent Facebook-Cambridge Analytica data scandal. Participants from Kenya also reported their concerns over the collection of biometric data by the government under the Huduma Number Project, expressing a lot of concern over the security of the collected data, given that the proposed Data Protection and Privacy Bill 2018 (ict.go.ke, 2018) was not yet implemented before the collection of the biometric data.

Although the majority of Internet users in East Africa are aware of online security threats, awareness of how to ensure online safety is only limited to the medium to highly technical Internet users in the region. "*I think the creators of these online platforms should find a way to ensure that it is not possible to hack another person's account*" (male, L.T., Kenya). This was, on the other hand, the view of a majority of the low technical participants. Only one participant had taken extra steps to ensure the online security of his email and social media accounts, through the use of physical USB drive keys for his Google and Facebook accounts. "*I feel safe on the Internet as I protect all my online banking, Gmail and Facebook passwords with these physical encryption USB drive keys. Personally, I think people feel safe on the Internet, mainly because they have no idea of the security risks on the Internet. This is why most people post their private photos and even live locations on social media. I feel safe because I create safety for myself*" (male, H.T., Uganda). Hence, it clearly emerged from the focus groups that despite users being aware of potential online threats they are not capable of identifying different ways to ensure online security and privacy. In addition, despite being aware of privacy and confidentiality threats on the Internet, East African Internet users trust online social media platforms because they give them enough freedom to express themselves. Over half of the participants reported that they interact more freely while on social media platforms than in person. In Uganda, the Women of Uganda Network (WOUGNET)

[5] See https://www.nita.go.ug/service/myug-free-wifi for more on MYUG free Wi-Fi

takes advantage of the opportunities presented by ICTs to promote and support the use of ICTs by women and women organizations in the country and to effectively address national and local problems of sustainable development. Although the benign online disinhibition effect has improved communication and useful information sharing, some Internet users tend to abuse the freedom and also overshare their private information on social media. One participant reported that in Uganda, a person was arrested after using Facebook and Twitter to hurl insults at the Ugandan President, an action they certainly would not undertake in person.

The education system in East Africa should be one of the key channels employed to raise awareness of the different ways that Internet users should undertake to ensure the security of their private and confidential information while online. However, this is not the case. While NGOs and governments are collaborating to increase digital literacy in the region, online security is not being emphasized as necessary. In the Kenyan primary school basic education curriculum framework, ICT cuts across all the learning subjects, mainly for research and learning material access, but online security is not addressed in the learning. This is slowly leading to a generation that can easily use the Internet, but is not aware of the dangers lurking on the Internet. These problem do not affect only online users, but also enforcement officials. For instance, one participant reported that the police force in East Africa is not well equipped to deal with cases of online privacy breaches and cases of cyber-bullying.

3.3. Internet disruptions in East Africa and Internet users' reactions

"*While I was in Sudan, I could not access Instagram and while other common sites could be easily accessed, connecting to Facebook was always an issue and very slow*" (male, H.T., Kenya). Internet disruptions are becoming a common event in East Africa. They take the form of Internet shutdowns, throttling of Internet speeds and blocking of targeted social media or news websites. Six out of the twelve countries in East Africa have had confirmed Internet disruptions over the last decade, as in the figure below:

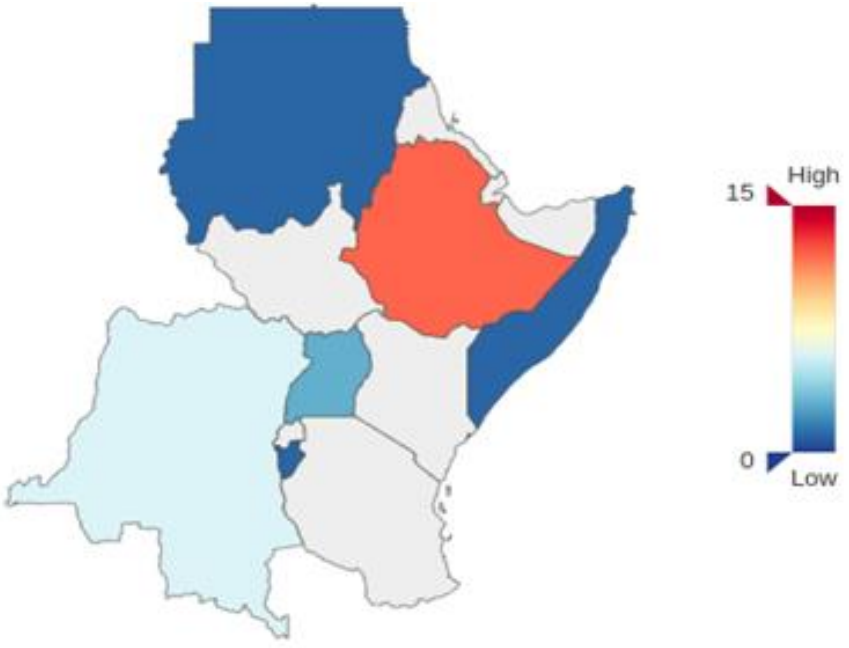

Figure 3: Internet disruptions in East Africa

Data source: AccessNow KeepItOn

Country	Number of disruptions	Causes
Ethiopia	12	Elections: 1, mass protests: 10, national examinations: 1
D.R. Congo	6	Elections: 1, political protests: 5
Uganda	2	Elections: 1, Prior to the swearing in of the president: 1
Sudan	1	Anti-government protests: 1
Somalia	1	Elections: 1
Burundi	1	Elections: 1

Table 3: Number of disruptions per country

Data source: AccessNow KeepItOn

Internet disruptions in East African countries are common during elections and mass protests, with one case of disruption in Ethiopia during a national examination, to prevent students from cheating by using social media. According to the government's officials, Internet disruptions during elections and protests are done to control the spread of fake news and rumours, which could potentially lead to misinformation of the public.

"Once you shut down the Internet in Uganda, not only you prevent Ugandans from knowing what is going on in Uganda and the world, but also you have prevented the whole world from knowing what is going on in Uganda" (male, M.T., Uganda). The majority of the participants, especially in Uganda, where there was a social media shutdown during the 2016 elections, had similar responses to Internet disruptions. As reported earlier, Kenyan and Ugandan Internet users depend on the Internet, especially social media, for e-commerce, social interactions, entertainment, and news. Internet disruptions, hence, massively inconvenience a large number of social and economic activities. Over three-quarters of the participants felt that Internet disruptions in the region are an infringement of the right to expression of the people, and is a form of censorship. "*People should have free access to information, as a right and shutting down the Internet is an infringement of this right. Also, people with online businesses and also service providers lose a lot during these shutdowns. I agree, there is always the issue of security, but Internet shutdowns just work as a short-term solution, but governments should find a long-term solution to this, especially for election periods."* (male, M.T., Uganda). One participant reported that when the Internet was shut down during the election period, she lost complete trust that the government was conducting a free and fair election process. "*Personally, I think that shutting down the Internet escalates the already delicate situation, as people are now suspicious that the government is hiding something"* (female, M.T., Uganda).

Two participants reported that they felt that Internet users are partially to blame for Internet disruptions. One of these participants reported that although campaigning during the election day is prohibited in Uganda, aspiring politicians, supported by social media users, continue their campaigns on social media on this day. Campaigning physically during the election day is a criminal offence that could lead to arrest; hence politicians turn to social media, which is harder to control, according to the participant. He also reported that he had noted that in most elections in East Africa, the political party that loses, is quick to claim that the election was rigged by the winning party, with social media playing a key role as the medium for this. "*I think that governments are forced to shut down the Internet during elections to stop the few people who incite others on social media with fake propaganda during the elections. There is normally so much fake news and hate speech going around during the election time. As much as I don't advocate for these disruptions, sometimes it is the citizens who are abusing these*

platforms" (male, M.T., Uganda). Another participant pointed out the use of social media by a small number of people to propagate incitements and rumours targeted towards causing unrests in East African countries. He referred to social media as the 'new radio', in reference to the use of some radio stations to escalate the 1994 Rwanda genocide. "*If you look at any past technology, people have abused it. For example, the role of mass media, mainly radio, in the Rwanda genocide*" (male, H.T., Uganda). He also pointed out that social media played a key role in the 2007 Kenya post-election violence. As reported earlier, most East African Internet users rely on social media for news and a few people spreading fake news on social media could potentially influence many Internet users in the region.

Nevertheless, "*shutting down the Internet is not the ultimate solution to this*" (male, M.T., Uganda). The majority of participants responded to the above comments by saying that Internet disruptions are not a good solution, and potentially these acts have a negative effect on the existing situation. This is due to the fact that Internet or social media shutdowns, during elections, increase tensions.

3.4. Effect of Over the Top (OTT) tax in Uganda on Internet use

On 1 July 2018, the Ugandan government implemented a 200 UGX (~0.05 USD) tax per user per day to access OTT services.[6] The new OTT tax only affected Internet users who rely on mobile data from Ugandan service providers to access the Internet, which is a majority in the country. The reason behind the social media tax was that the new revenue stream would provide funds to improve Internet connectivity in the country and curb online gossip. This also affected mobile money services in the country, leading to an increase in mobile money transaction costs.

"*They (the government) say that OTT tax is aimed at reducing 'rugambo' (gossip) online, but I believe we have the right to free speech, even online, and this tax is just a way of censorship*" (male, M.T., Uganda). This was the dominant response from the majority of Ugandan participants to focus group discussions, who expressed their anger towards the OTT tax in the country. Over three-quarters of the participants from Uganda felt that the introduction of OTT tax was a censorship move by the government, mainly because this tax only targets social media platforms. "*If the government requires funds to improve the Internet infrastructure in the region, why are social media sites the only target? Why not YouTube and Netflix?*" (female, L.T. Uganda). All the participants with a low level of IT technical skills reported that since the introduction of the OTT tax, their social media usage had reduced significantly. "*We pay value-added tax when we buy airtime and data bundles, so I think adding another tax on top is too much. It is affecting our Internet use"* (male, L.T., Uganda). According to the Ugandan Taxes Survey Report, the use of social media platforms reduced significantly for the first three months after the introduction of OTT tax, as in the figure below:

[6] The Excise Duty (Amendment) Act, 2018, defines over the top services as "the transmission or receipt of voice or messages over the Internet protocol network and includes access to virtual private networks;" and the levy is listed in 13(b) as "UGX 200 per user per day of access" in The Excise Duty (Amendment) Act, 2018.

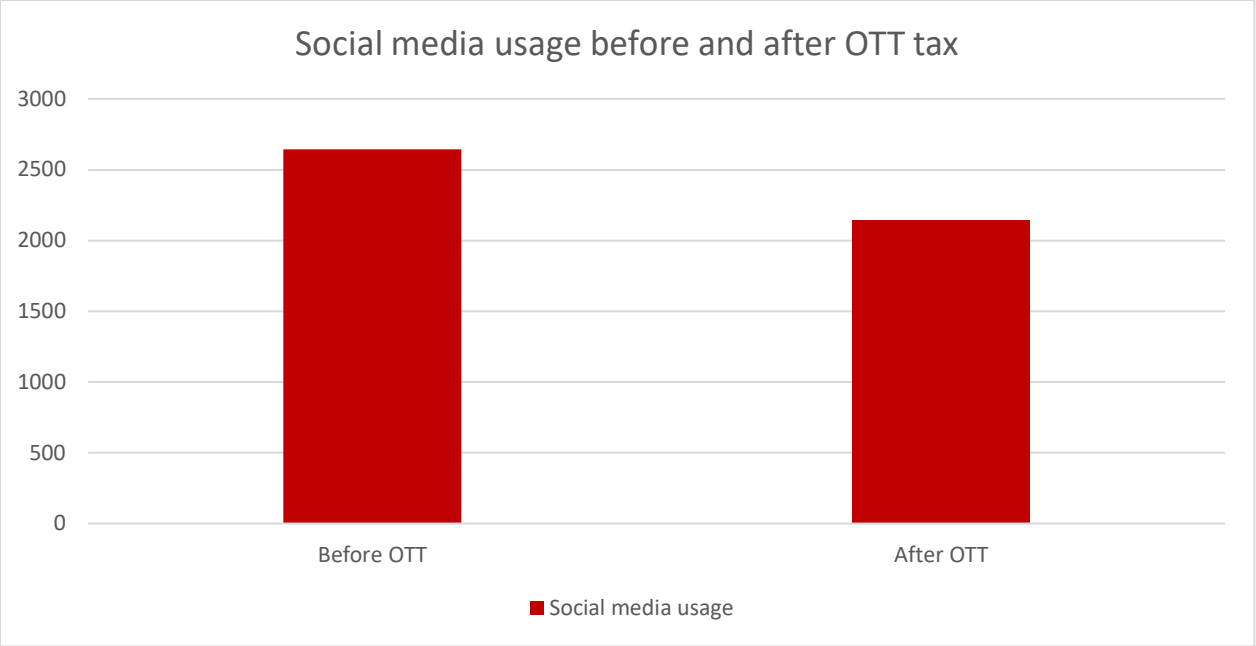

Figure 4: Effect of OTT tax on social media use

Data source: Uganda Social Media and Mobile Money Taxes Survey Report

The majority of focus group participants in Uganda also reported that OTT tax had greatly inconvenienced their interactions through social media platforms, especially WhatsApp. One participant reported that she knew online traders who had been greatly inconvenienced by the introduction of the OTT tax, as most of the small-scale e-commerce is done through social media platforms, especially Facebook. Respondents to Whitehead Communications' Uganda research (2018) also reported inconveniences on social media usage caused by OTT tax, classified with the degree of inconvenience as below:

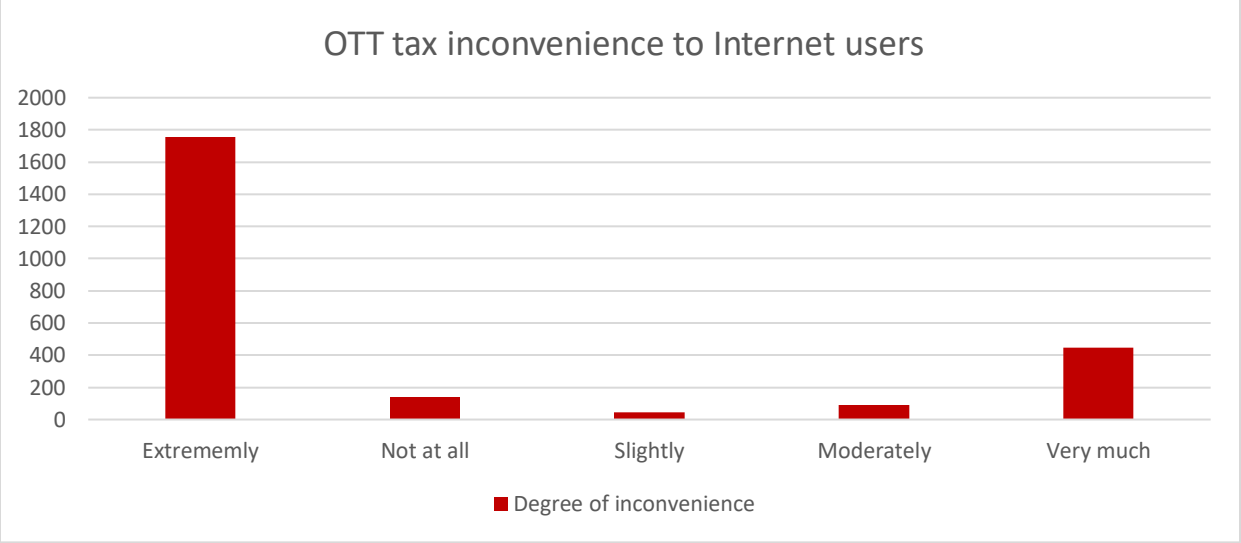

Figure. 5: OTT tax inconvenience to Internet users

Data source: Uganda Social Media and Mobile Money Taxes Survey Report

The use of VPN tools was the most dominant technique to evade OTT tax, with half of the participants reporting that they had tried out different VPN tools. The use of Wi-Fi hotspots to evade OTT tax was dominant especially among the more IT skilled Internet users. Most of the participants reported using Wi-Fi hotspots at their workplaces, with one participant reporting that she had noticed that most of her friends were offline during the weekends when out of their workplaces. "*During the weekend, my WhatsApp statuses have very few views from my contacts, as compared to weekdays*" (female, M.T., Uganda). This was confirmed also by one participant who reported that he would opt to stay off social media during weekends. No participants reported having used Smart DNS to evade the OTT tax. There were two key reasons behind the need to evade the OTT tax: the first one was the increased expenditure on Internet usage by the users, and the second one was a form of resistance to paying the tax, although some users could even afford it. *"I do not pay out of principle, because I think it is oppressive to pay the tax, so I use VPN"* (male, H.T., Uganda). However, all participants who had turned to the use of VPN tools to evade paying OTT, due to the increased cost, reported that they ended up paying OTT as VPNs proved not to be economically feasible compared to paying the OTT tax. "*When using VPN, I just watch a few videos on Facebook and my data bundles get depleted, while they last longer without using VPN. That is why I stopped using VPNs*" (female, L.T., Uganda). The participants reported that the use of VPN tools would result in using more bandwidth (Internet bundles), hence they would end up spending more than if they paid the OTT tax. This is caused by an increase in data size due to the data encryption done by VPN tools, which increases the size of the transmitted data anywhere from 5% to 15%. One participant reported that he noticed that the use of VPN resulted in faster smartphone battery drain and he pays to have his phone charged since he does not have electricity in his home. Although participants reported these challenges with the use of VPN tools, no participant had tried to use Smart DNS or any other DNS manipulation techniques.

Only one participant had a different view about the OTT tax, where he believed that the 200 UGX was a very small amount to have a huge impact on an already existing Internet user. "*If one cannot afford 200 UGX for the OTT tax, how will they afford 1000 UGX for the data bundles in the first place?*" (male, H.T., Uganda). However, his statement was heavily opposed by the other participants of the focus group discussion, with the other members telling him that his statement was from a point of financial privilege. Six out of sixty-five participants reported that they had just paid the OTT tax since its introduction and had not tried any evasion tools or techniques.

3.5. Data anonymisation by Eastern African Internet users

Data anonymisation was evident among Internet users in Kenya and Uganda, with different users having different motivations for it. The dominant reasons for anonymisation in East Africa include online anonymity and privacy, online security, evasion of OTT tax, Internet disruptions, access to geo-blocked content and work remotely. Over half of the participants had anti-malware programs installed on their computers, but mainly used them to scan removable storage hardware and the computer hard drives for malware.

VPNs are the dominant data anonymisation tools used by Eastern African Internet users to ensure online anonymity, with nineteen participants having used them. Eleven participants also reported having used Tor for online anonymity. Besides, a skilled participant reported using bootable operating systems for online anonymity. He had used the Whonix Operating System before.

The use of anonymisation tools for online anonymity and privacy was mainly dominant among the high to average skilled IT Internet users in East Africa. Out of the total 45 participants that had connected to the Internet anonymously, 25 reported that they had done so to ensure their online anonymity. Twenty-

four of these participants were high to average skilled IT users, with one participant with low IT skills reporting that she had used her browser's incognito mode, which is not really an anonymisation technique. One participant with low technical skills reported that he felt the need to connect to the Internet anonymously to ensure the privacy of her information, but had no idea how to do it.

Internet disruptions in East Africa lead Internet users to a quest for anonymisation online, especially with the use of VPNs. From the analysis of the past four-year Google Trends data[7], a trend is evident, where there are increased interests in VPN tools during or immediately after a period of Internet disruptions. In figure 7 below, there was a trend where the number of Internet users in the Democratic Republic of Congo searching for the keyword 'VPN' increased immediately after or during Internet disruption periods.

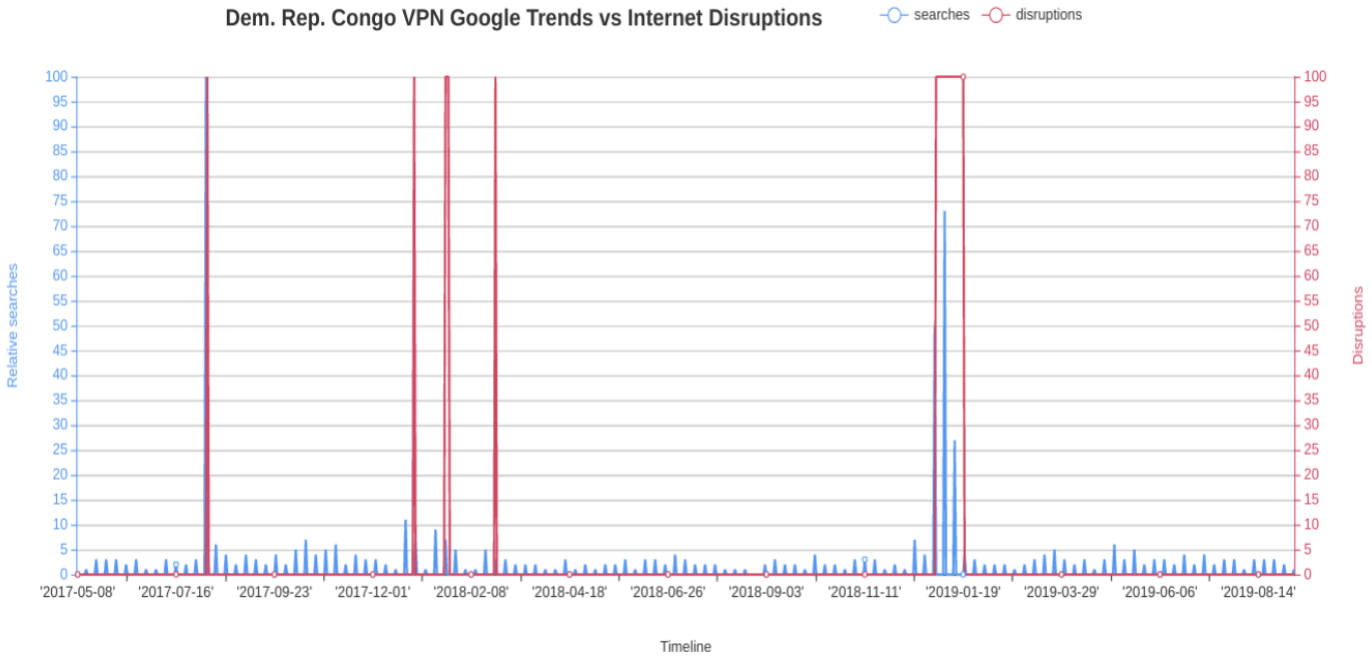

Figure 6: Google Trends vs Internet disruptions DR Congo

This is also the case in Ethiopia as in figure 8 below, where a similar trend can also be noted.

[7] Google Trends is a search trends feature that shows how frequently a given search term is entered into Google's search engine relative to the site's total search volume over a given period of time.

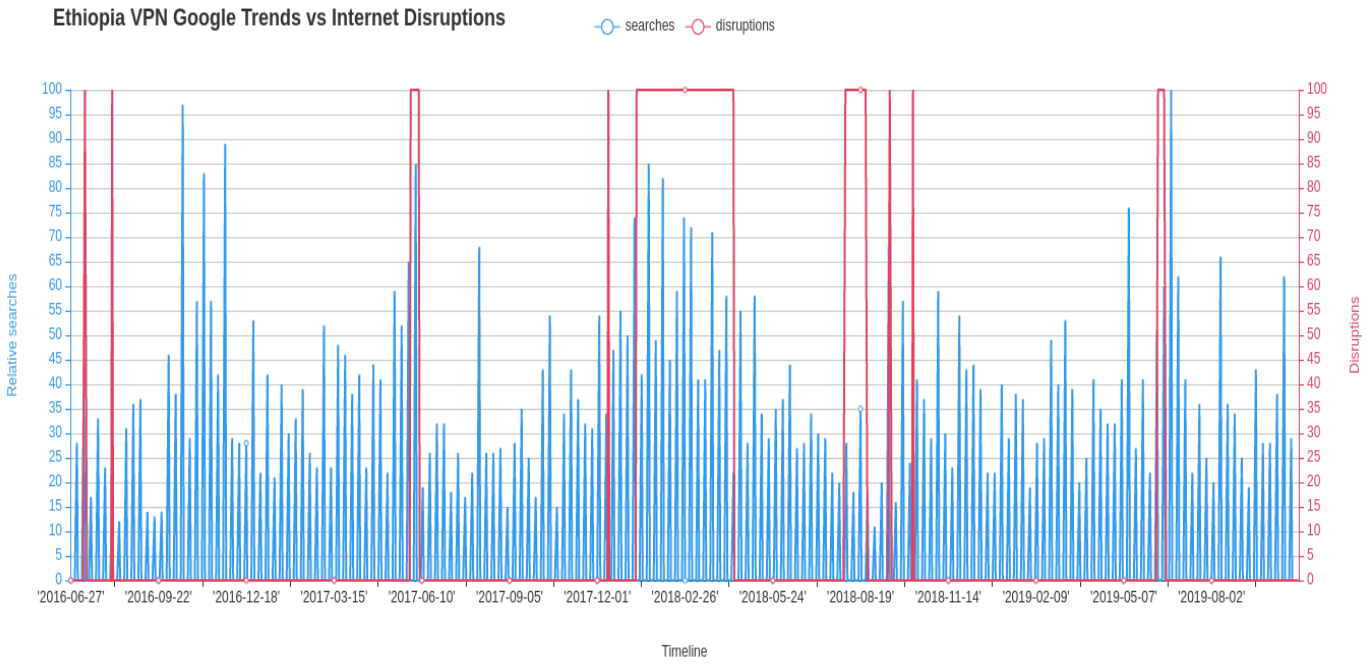

Figure 7: Google Trends vs Internet disruptions in Ethiopia

It was also evident that the existence of Internet disruptions in a country increases the Internet users' knowledge of data anonymisation tools, especially among unskilled Internet users. In Kenya, where there has never been an Internet disruption, five out of the seven participants with low IT skills reported that they ultimately had no idea what a VPN was, while in Uganda, all the participant had at least an idea of what a VPN was. Compared to DNS manipulation tools, VPN tools are also the main data anonymisation tools used to evade Internet disruptions, with no evident trend in the Google Trends searches data for DNS manipulation. The use of data anonymisation tools for online security was the least reported reason, with only one Internet user reporting having taken extra steps and tools to ensure online security, as reported earlier. The majority of participants relied on the measures provided by the online platforms, like two-factor authentication, which was popular among the participants. Although many participants in Uganda knew that with VPN, a user could hide the location, hence evade the OTT tax, they had no idea that these tools could be used to ensure online security.

The evasion of the OTT tax in Uganda is a dominant reason for the use of data anonymisation tools in East Africa, as reported earlier. Although there many geo-blocked platforms exist in East Africa, especially entertainment content, geo-blocking was only a concern among the below 45-years age groups and highly skilled Internet users in the region. The existence of geo-blocked platforms in East Africa is unknown by the majority of focus group participants in Kenya and Uganda, with most of them relying on YouTube, other third-party free music download sites and social media platforms for entertainment. "*Why pay for music (Spotify) while I can download any song from the Internet or YouTube?*" (female, M.T., Kenya). However, seventeen participants had used data anonymisation tools to access geo-blocked content, with all having used VPN tools and four participants having used DNS manipulation techniques for this. However, one participant reported that the use of VPN to access geo-blocked content was not an effective solution, as not only do VPNs make streaming content slower, but also, most of the platforms require payment cards or PayPal accounts that are registered in the country where the service is available. "*I used VPN to register for Spotify, but since a US PayPal account and card were required, I could only access the free version, but only the paid version could be used with my new*

Amazon Echo. After a bit of searching online, I purchased a Spotify gift card from a different site, which I used to pay for the subscription, but lost the free trial which is not issued if one uses a gift card. I even have an Amazon Prime subscription, but sadly Prime Music is not supported in Kenya. I am paying for a service that I cannot fully use" (male, H.T., Kenya).

3.6. VPN vs DNS manipulation usage in Eastern Africa

The use of VPN tools is the most dominant data anonymisation technique in Kenya and Uganda across all age groups and IT skills levels, as compared to the use of DNS manipulation tools. While the use of DNS manipulation tools is only common among the highly skilled Internet users, VPN usage cuts across all IT skill levels. VPNs for anonymisation are used for many reasons, as demonstrated in figure 9 and table 6 below.

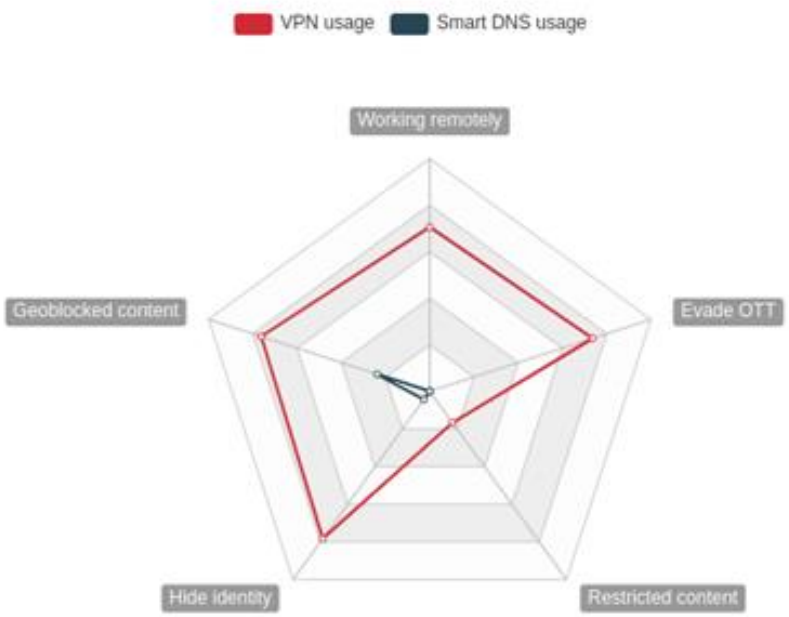

Figure 8: VPN usage vs Smart DNS usage across all technical groups

Technical Level	Used VPN tools	Used DNS manipulation tools
High	Yes: 24 No: 1 No idea what it is: 0	Yes: 6 No: 19 No idea what it is: 0
Average	Yes: 14 No: 16 No idea what it is: 0	Yes: 0 No: 20 No idea what it is: 10
Low	Yes: 3 No: 2 No idea what it is: 5	Yes: 0 No: 3 No idea what it is: 7

Table 4: VPN vs DNS manipulation usage across technical groups

Although participants reported that the use of VPN tools led to more bandwidth usage and slower connections, almost all of them had no idea that the use of DNS manipulation tools could solve some of their problems. As reported earlier, the introduction of the OTT tax and Internet disruptions has led to an increased awareness of the use of VPN in Uganda. In comparison to Kenya, more Ugandan users with low IT skills know about VPNs. The five unskilled participants who had no idea what VPNs are were all from Kenya. The use of DNS manipulation tools is significantly low, with only six highly skilled participants reporting having used them before. All the six participants had used DNS manipulation tools to access online geo-blocked content, with international Netflix content access being the most dominant reason.

4. Conclusions and Recommendations

4.1. Online security and awareness

Despite increasing digital literacy in East Africa, the awareness for data anonymisation by Internet users in the region, for online security, is still lagging. Although Internet users in East Africa are aware that privacy issues over Internet use exist , most of them are not aware of the steps and measures to employ to ensure this. It is also clear that cybercriminals targeting Eastern African technology and Internet users are taking advantage of the lack of awareness among users, hence using social engineering as their first line of attack. Mobile money platforms play a critical economic role in Kenya and Uganda, due to their ease of use and efficiency for transactions, even for the less technical users in the region. This has made the platforms easier targets for cybercriminals in East Africa. For most of the Internet users in East Africa, social media is the main reason for Internet usage. Social media platforms play social, economic and entertainment roles in the region, making them another key target for cybercriminals. Many reported cases of social media account hacking in the region mainly result from the lack of adequate knowledge by users on the different measures and tools that they can employ to secure their accounts. However, although Internet users in East Africa are aware of the privacy threats and have also experienced social media account breaches, most of them feel a sense of security and freedom on social media. Internet users in the region feel that they can share more and interact better over social media. Hence social media is a powerful tool for economic, social and political empowerment in the region. However, misuse of the platforms is also evident, with users lacking awareness of the extent of private information that they should share online.

Recommendations

It is possible to achieve a more secure Internet in East Africa. The first key step towards this is to improve Internet users' awareness. By educating Internet users in the region on the different privacy threats on the Internet, the users will have the ability to protect themselves from social media account hacking and social engineering. Some of the basic yet powerful techniques that can be taught to users include:

- Using strong passwords
- Setting up two-factor authentication (which is provided by most social media platforms) and
- How to identify online fraudsters and social engineering attempts by cybercriminals.

Internet users' awareness of online responsibility will also lead to a decrease in social media freedom abuse. Lastly, educating Internet users in East Africa on the different data anonymisation tools that they can use will lead to using reliable VPN tools over public networks. This might result in decreased account breaches in the region, for example.

The education system in Eastern Africa has a key role to play in raising users' online security awareness. Although it has been playing a commendable role in improving digital literacy in the region, training on online security is insufficient. Educating young students on privacy threats online and how to mitigate them will be a significant step towards improved online security in Kenya and Uganda. Laws and policies Tere exist across the East African countries to protect the online privacy and security of Internet users in the region. However, enforcement of these laws by the police is lacking. Governments in the region should equip and educate the police force on how to deal with online security and privacy breaches, for a safer and better Internet.

4.2. Internet disruptions

It is clear that, over the last decade, Internet disruptions are on the rise in East African countries, becoming one of the main challenges to Internet reliability in the region. Half of the countries in the region have been plagued by more than one Internet disruption over the last six years, with the majority of disruptions occurring during the election times. Internet disruptions, to control mass protests, are also common in the region. The most common disruptions are full Internet shutdowns and social media and news site blackouts and throttling. Internet disruptions have had a negative social and economic impact during shutdown periods, with reported losses of over one million USD per day of disruption. Internet disruptions are also a major blow for still-growing Internet adoption in the region and a hindrance to faster adoption. The case of the OTT tax in Uganda has evidently and massively affected Internet usage and adoption in the country, given that the cost of bandwidth is still high in the country, where most of the citizens daily budget is under one dollar. Internet shutdowns during elections to curb the spread of fake news only lead to worsening of the already delicate situation, due to uncertainty among citizens, caused by Internet or social media shutdowns. Citizens' trust of their government is also negatively affected by Internet and social media shutdowns since their freedom of expression is violated by a government that should be safeguarding it.

Recommendations

Although malicious individuals whose aim is to spread fake news and cause unrests during election periods exist, shutting down social media platforms and the Internet is not a long-term solution to ensuring violence-free elections. Internet user education is one of the best long-term solutions that can be employed by governments to ensure the reduced spread of fake news through social media. Through this, Internet users will easily identify fake news and individuals spreading hate speech during delicate periods, like election times. Internet users should also be educated against the abuse of the freedom that social media grants them, and the importance of being responsible over the web. Governments should also implement laws and policies governing the spread of fake news and hate speech online, to curb this problem, instead of shutting down the Internet in the whole country, affecting every Internet user in the country, over the actions of a handful of malicious Internet users. Ethiopia is in the forefront of implementing reforms in East Africa over censorship and Internet disruptions, unblocking hundreds of previously blocked news platforms in 2019 (Xynou, et al., 2019). However, this took a step backwards in 2020 when Internet users in the country had one of the longest Internet shutdowns in Africa.

4.3. Data anonymisation

The use of data anonymisation tools for online security, mitigation of Internet disruptions and OTT tax, geo-blocking and online anonymity is evident among Internet users in Eastern Africa. VPN tools are the most dominant data anonymisation tools in the region. The main motivation for the use of data anonymisation tools is mainly to mitigate Internet disruptions in the region, with users from all technical levels trying out different VPN tools. Although the majority of unskilled users use VPN tools to mitigate Internet disruptions and censorship in the region, they are not aware that the same tools can be used for online privacy and security. Internet disruptions in the region are increasing awareness of VPNs in the region as seen in countries that have experienced disruptions, compared to countries that have not. Selecting a reliable VPN service provider is crucial for ensuring that the privacy of the user is protected. However, most Internet users in East Africa mainly select VPN providers based on affordability.

There is a lot of geo-blocked content in the East African Internet space, especially entertainment and educational material. This is a concern for a majority of the skilled and highly skilled Internet users, and a reason for the use of data anonymisation tools. The use of VPN tools is dominant to access geo-blocked content in the region. Faster consumption of bandwidth (data bundles) and smartphone battery power are the main challenges facing effective use of VPN tools in Eastern Africa, making them not feasible economically, especially for streaming online content. However, most users in the region are not aware that DNS manipulation tools and services, such as Smart DNS can be used in place of VPNs for this.

Recommendations

Data anonymisation for online security and privacy should be emphasized in East Africa, for more secure Internet access in the region. East African Internet users should also be educated on the different data anonymisation techniques and tools, and the suitability of each tool for a wider choice. Selecting the right VPN service provider is also crucial for ensuring online privacy, and East African Internet users should be made aware of the metrics to use to determine a safe VPN tool. Online platforms that rank the different major VPN providers in terms of privacy reliability also exist. Policies to control geo-restrictions should also be introduced in the region, like the European Union digital media portability regulations (European Commission, 2018). This will erase the current physical boundaries on the Internet, for a more globally interconnected network.

5. References

Aloul, F., 2012. The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology,* III(3), pp. 176 - 183.

Atieno, M., 2016. *African Governments Are Increasingly Blocking Social Media, But VPNs Are Increasingly Becoming A Pain In Their Foot.* [Online]
Available at: http://innov8tiv.com/african-governments-increasingly-blocking-social-media-vpns-increasingly-becoming-pain-foot/
[Accessed 15 January 2019].

Balaji, R., 2013. *The Complete Book of Data Anonymization: from Planning to Implementation.* 1st ed. Boca Raton: CRC Press.

Calandro, E., Gillwald, A., Moyo, M. & Stork, C., 2010. *Comparative ICT sector performance review 2009/2010,* Cape Town: Research ICT Africa.

Chirgwin, R., 2018. *VPN Logs Helped Unmask Alleged 'Net Stalker, Say Feds." The Register - Biting the Hand That Feeds IT.* [Online]
Available at:
www.theregister.co.uk/2017/10/08/vpn_logs_helped_unmask_alleged_net_stalker_say_feds/
[Accessed 18 January 2019].

Daily Nation, 2017. *Safaricom sacks 52 employees over M-Pesa fraud.* [Online]
Available at: https://businesstoday.co.ke/safaricom-sacks-52-employees-m-pesa-fraud/
[Accessed 5 8 2019].

Edmundson, A., 2018. *I Don't Think Internet Anonymity Means What You Think It Means.* [Online]
Available at: www.libertarianism.org/building-tomorrow/i-don't-think-internet-anonymity-means-what-you-think-it-means
[Accessed 15 January 2019].

Erwin, M., Charlie, S. & Wolfe, P., 1998. *Virtual Private Networks: Turning the Internet Into Your Private Network.* 2nd ed. New York: O'Reilly Media.

Esselaar, S., 2019. *OTT tax causes massive decline in estimated internet users in Uganda.* [Online]
Available at: https://researchictsolutions.com/home/ott-tax-causes-massive-decline-in-internet-subscriptions-in-uganda/
[Accessed 02 February 2019].

European Commission, 2018. *Cross-border portability of online content services.* [Online]
Available at: https://ec.europa.eu/digital-single-market/en/cross-border-portability-online-content-services
[Accessed 20 August 2019].

Gackenbach, J., 2011. *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications.* Burlington: Academic Press.

Gayathri, N. & Liu, J., 2015. An Adaptive Learning Model for k-Anonymity Location Privacy Protection. *IEEE 39th Annual Computer Software and Applications Conference,* 1(1).

Gillwald, A. & Mothobi, O., 2019. *After Access 2018: A Demand Side View of Mobile Internet from 10 African COuntries,* Cape Town: Research ICT Africa.

Goleman, D., 2011. The Social Brain Online. In: *The Brain and Emotional Intelligence: New Insights.* Massachusetts: More Than Sound.

ict.go.ke, 2018. *The Data Protection Bill, 2018,* Nairobi: ict.go.ke.

Irwin, L., 2018. *The GDPR: What is sensitive personal data?.* [Online]
Available at: https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data
[Accessed 12 January 2019].

Jones, G., 2018. *VPN vs Smart DNS.* [Online]
Available at: https://www.addictivetips.com/vpn/vpn-vs-smart-dns/
[Accessed 11 January 2019].

Kende-Robb, C., 2015. *Why Technology is Key to Africas Future.* [Online]
Available at: https://www.weforum.org/agenda/2015/01/why-technology-is-key-to-africas-future/
[Accessed 01 February 2019].

Lapidot-Lefler, N. & Azy, B., 2015. The Benign Online Disinhibition Effect: Could Situational Factors Induce Self-Disclosure and Prosocial Behaviors?. *Journal of Psychosocial Research on Cyberspace*, 1 July.

Lavion, D., 2018. *Pulling fraud out of the shadows: Global Economic Crime and Fraud Survey 2018,* London: PriceWaterhouseCoopers.

Lindquist, J., 2018. *Data science under GDPR with pseudonymization in the data pipeline.* [Online]
Available at: https://www.dativa.com/data-science-gdpr-pseudonymization-data-pipeline/
[Accessed 11 January 2019].

Matfess, H. & Jeffrey, S., 2018. *Africas Attack on Internet Freedom.* [Online]
Available at: https://foreignpolicy.com/2018/07/13/africas-attack-on-internet-freedom-uganda-tanzania-ethiopia-museveni-protests/
[Accessed 01 February 2019].

Nweke, L. O., 2017. Using the CIA and AAA Models to explain. *PM World Journal,* VI(12), pp. 1 - 3.

Palme, J. & Berglund, M., 2004. *Anonymity on the Internet.* [Online]
Available at: https://people.dsv.su.se/~jpalme/society/anonymity.pdf
[Accessed 14 January 2019].

Secorun, L., 2017. *Kenya's tech startups trial digital classrooms in drive for literacy.* [Online]
Available at: https://www.theguardian.com/sustainable-business/2017/jan/23/tech-startups-kenya-bridge-education-gap
[Accessed 02 February 2019].

Serianu, 2017. *Africa Cybersecurity Report 2017,* Nairobi: Serianu.

Sudhanshu, C. & Kumar, N., 2015. *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques.* Amsterdam: Elsevier.

Suler, J., 2004. The Online Disinhibition Effect. *CyberPsychology & Behavior,* 7(6), pp. 321 - 326.

Summers, A., 2018. *Africa is a Paradise for Cybercriminals.* [Online]
Available at: https://www.le-vpn.com/africa-paradise-cybercriminals/
[Accessed 14 January 2019].

unstats, 1999. *United Nations Statistics Division.* [Online]
Available at: https://unstats.un.org/unsd/methodology/m49/
[Accessed 12 January 2019].

Wakabi, M. & Anyanzwa, J., 2018. *One Network Area: Roaming charges are back.* [Online]
Available at: https://www.theeastafrican.co.ke/business/One-Network-Area-Roaming-charges-are-back/2560-4804088-oh7wsfz/index.html
[Accessed 13 January 2019].

Whitehead, A., 2018. *Uganda Social Media and Mobile Money Taxes Survey Report,* Kampala: Whitehead Communications.

Xynou, M., Karanja, M., Taye, B. & Filastò, A., 2019. *Resurgence of Internet Censorship in Ethiopia: Blocking of WhatsApp, Facebook, and African Arguments.* [Online]
Available at: https://ooni.io/post/resurgence-internet-censorship-ethiopia-2019/
[Accessed 23 August 2019].

6. Appendix: Research Methodology

In order to inform debates on anonymisation online and provide evidence as to why East African users are adopting Internet anonymisation tools and techniques, this research sought to answer the following questions:

1. What are the main reasons for using VPN and DNS manipulation as data anonymisation techniques in East Africa?
2. Who are the main VPN users in East Africa and what is the motivation for using such tools in the different user groups in terms of age and gender?
3. Why do Internet users and Non-Profit Organisations (NPOs) use VPNs and DNS manipulation in Eastern Africa?
4. Where has VPN and DNS manipulation for data anonymisation mostly been used and do any geographical trends on their use exist?
5. When were VPN and DNS manipulation used in East Africa? Is it possible to identify specific time periods of their use?
6. How has VPN and other data anonymisation tools been used to ensure information security and privacy in East Africa?

The research was based both on desk research and focus group discussions.

Desk study

The desk research involved a review and critical analysis of existing secondary data sources on data anonymisation in East African countries. Specifically, previous studies on data anonymisation, including news articles on the state of online security, censorship and the use of VPN and DNS manipulation to counter it in East Africa were reviewed. In addition, an analysis of the Google search trends[8] data by Internet users across East Africa was useful in establishing whether a trend exists between Internet disruptions periods and Internet users in the region searching for keywords such as 'VPN' or 'Smart DNS'. Together with data from AccessNow KeepitOn Campaign[9] on Internet shutdowns and disruptions in Africa for the last five years, this was useful in the investigation of whether Internet users in East Africa turn to any data anonymisation tools during Internet disruption periods. Quantitative data collected in Uganda one month after the introduction of OTT taxes in the country, through a survey conducted by Whitehead Communications Uganda, was used to supplement data collected through the focus groups in the country, to perform an analysis of the Internet users' opinions on the introduction and implementation of OTT taxes.

Focus group discussions

The purpose of the focus group discussions was to investigate the state of online security and privacy in East Africa by canvassing Internet users' views on Internet disruptions and on the Ugandan OTT tax, the use of data anonymisation tools and the challenges accompanying the use of these tools. Evaluation of user awareness on Internet security and the use of any tools and techniques to ensure safety and security online were also key areas of investigation of the focus groups.

[8] See https://trends.google.com/ for more on Google Trends data
[9] See https://www.accessnow.org/keepiton/ for more on the AccessNow KeepItOn campaign

A total of eight focus groups were conducted with twenty-eight female and thirty-seven male participants in Kenya and Uganda. A total of sixty-five participants took part in the focus groups. The focus groups were conducted in a mixed-gender setting, disaggregated by age groups (15 – 24, 25 – 44 and 45 – 64) and by the level of IT technical knowledge of the participants. The technical knowledge of the participants was divided into the following 3 levels:

Highly technical/technology savvy: these are people mainly whose profession is in technology, e.g. software developers and IT specialists;

Intermediate/less technical: individuals whose professions are outside the technology field, but have a good technical knowledge and can install software or troubleshoot a connection;

Non-technical/beginner level: individuals that use smartphones mostly, and the Internet to perform basic activities.

The table below shows a breakdown of the number of focus groups conducted in Kenya and Uganda:

	Low technical Users	Medium technical	High technical
Kenya	1	2	2
Uganda	1	1	1

Table 5: Breakdown of the number of focus groups conducted

The non-technical participants were required to at least have the ability to browse the Internet with a smartphone. However, it was a challenge to find participants older than 65 who could use the Internet without difficulty. All the sessions were around one hour long.

The focus group discussions were divided into three segments. The first segment evaluated an overview of the different uses of the Internet (social media, work, entertainment, shopping, news, and educational research) by the participants. This segment also evaluated the main challenges to access and use of the Internet faced by Internet users in the region. The second segment focused on online security, anonymity or the need for browsing the Internet anonymously among the participants, reasons for anonymity and tools that the participants had used, if any, to achieve this. The third segment narrowed down the discussion to the use of VPN tools and DNS manipulation services or techniques.

The focus groups were supplemented with interviews targeting mainly low technical Internet users in Kenya and Uganda.