CENSORED CONTINENT

Understanding the use of tools during Internet censorship in Africa: Cameroon, Nigeria, Uganda and Zimbabwe as case studies.

Babatunde Okunoye

A research report for the Open Technology Fund (OTF) Information Controls Fellowship

July 31 2020

Censored continent

Understanding the use of tools during Internet censorship in Africa: Cameroon, Nigeria, Uganda and Zimbabwe as case studies

Babatunde Okunoye

A research report for the Open Technology Fund (OTF) Information Controls Fellowship

July 31 2020

Table of contents

Research Summary and key findings

This report examines the use of Internet censorship circumvention tools in Cameroon, Nigeria, Uganda and Zimbabwe, four countries in Africa with varying degrees of Internet censorship, including Internet bandwidth throttling, social media app restrictions and website blocks. Interviews were done with 33 people including students, members of civil society, businessmen and teachers, revealing how communities mobilized to defeat censorship.

Important findings include:

- Civil society played an important role in mobilizing people to use circumvention tools.
- Some of the most important reasons for VPN adoption were community recommendations, cost of use, and ease of use.
- Messaging apps like Signal and Telegram which were unknown to government censors and were not blocked served as alternative messaging channels when more popular apps like Facebook and WhatsApp were blocked.
- People used innovative means of sharing VPNs, such as through USBs and Bluetooth when downloads were no longer possible from official sources such as websites of VPN makers and smartphone App stores.

1. Introduction

In the past two decades Internet censorship has been on the rise in Africa. In general, media spaces have long been under strict government control in Africa, particularly in repressive political contexts on the continent, as governments realized the well-established link between the control of information and the stability of states[1]. As a consequence, Internet censorship in Africa has intensified, as African governments began to observe the potential of the Internet to facilitate challenges to state power, or to facilitate mass citizen uprisings. One of the first instances on the continent where the Internet was used in mass political mobilization in Africa was in Ethiopia's Parliamentary elections of 2005[2]. Here, the Ethiopian blogosphere was very active and the major online platforms such as Nazret and Ethiomedia carried commentaries and manifestoes which were printed into leaflets to mobilize people in real time, also leveraging on the power of mobile phones and SMS services – scenes that would be re-enacted in the Arab spring of 2011. The post-election violence which followed the Kenyan 2017 election was another case where the Internet was a conduit for mass protests[3]. Here, the use of blogs and social media were among the range of media tools used to spread messages of hate and division among the Kenyan electorate. However perhaps most notably the Arab spring uprisings particularly in Tunisia and Egypt witnessed the use of social media platforms[4] to mobilize citizens in real time and led to regime change in both countries.

In the scenarios described above, the potential of the Internet to facilitate mass citizen mobilization was noted by governments in Africa. In response, governments across the continent developed the capacity to exercise greater

1 Price Monroe, Media and Sovereignty: The Global Information Revolution and its challenge to State Power (Cambridge Massachusetts: MIT Press) 2002.

2 Gagliardone Iginio, The Politics of Technology in Africa: Communication, Development and Nation Building in Ethiopia (Cambridge University Press) 2006.

3 George Gathigi, Kenyan democracy cannot take shape until its media step up, Quartz Africa, August 30 2017, https://qz.com/africa/1063980/kenyan-elections-2017-kenyan-democracy-cannot-take-shape-until-its-media-becomes-more-self-aware/

4 Heather Brown, Emily Guskin and Amy Mitchell, The Role of Social Media in the Arab Uprisings, Pew Research Centre, November 28 2012, https://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/

control of the Internet within their territories. This control included the technical means for various forms of Internet censorship including Internet disruptions (Internet shutdowns or Internet bandwidth throttling), social media app restrictions, blocking of websites, arrest of bloggers and online surveillance[5][6][7][8]. The pervasive use of Internet censorship mechanisms in Africa is demonstrated by the fact that outside of Asia, Africa has witnessed the most Internet disruptions in the world[9]. As described in the narrative above, most of these acts of Internet censorship have occurred around political events when state power was perceived to be under threat.

In response to this censorship, citizens in many countries on the continent have often mobilized to defeat the censorship implemented in their countries, for example by adopting the use of Internet censorship circumvention tools such as Virtual Private Networks (VPNs). A VPN allows for the creation of a secure connection to another network over the Internet[10]. VPNs can be used to access restricted content online, and shield browsing activity from privacy intrusions. There are a lot of VPNs available to users, some free, others subscription based. VPNs also have different levels of privacy protection online.

Although communities in Africa have long used Internet censorship circumvention tools to defeat the censorship experienced in their countries, few studies have examined their use of these tools. Most studies examining the use of Internet censorship circumvention tools have largely focused on Asia – for instance how communities have circumvented the censorship

5 OONI Explorer, Cameroon, https://explorer.ooni.org/country/CM

6 OONI Explorer, Nigeria, https://explorer.ooni.org/country/NG

7 OONI Explorer, Uganda, https://explorer.ooni.org/country/UG

8 OONI Explorer, Zimbabwe, https://explorer.ooni.org/country/ZW

9 AccessNow #KeepItOn, https://www.accessnow.org/keepiton/

10 Chris Hoffman, What is a VPN and why would I need one, How-to Geek, November 22 2019. https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

typified by the great Chinese firewall[11][12], and North America[13][14].

This report sheds light on how communities in four African countries – Cameroon, Nigeria, Uganda and Zimbabwe have mobilized to defeat Internet censorship implemented in their countries. The report seeks to answer the questions:

- **What are the tools used during Internet censorship events in Africa?**
- **How and why are they used?**
- **What are the usability challenges encountered by users of these tools?**

11 Fei Shen and Zhi'an Zhang (2018). Do circumvention tools promote democratic values? Exploring the correlates of anticensorship technology adoption in China. Journal of Information Technology and Politics 15(2), 106-121, DOI: 10.1080/19331681.2018.1449700

12 Mou Yi, Kevin Wu, and David Atkin (2016). Understanding the Use of Circumvention Tools to Bypass Online Censorship. New Media & Society 18(5): 837–56. doi:10.1177/1461444814548994

13 Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner (2015). Tor's Usability for Censorship Circumvention. Proceedings on Privacy Enhancing Technologies 2015; 2015 (2):1–21.

14 Kevin Gallagher, Sameer Patil, Nasir Memon (2017). New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

The report focuses on an area of study which have received sparse attention over the years, and it is hoped that the insights gained will shed light on how communities in authoritarian political contexts in Africa have mobilized to defeat Internet censorship. It is also hoped that it will serve as a resource to these communities, and to human rights organizations and developers of circumvention tools who have worked collaboratively with these communities to defeat censorship.

2. Methodology

The methodology used in this study is qualitative interviews and desk research. Thirty-three interviews (15 men, 18 women) were done across the four countries studied, among staff of civil society organizations, students, businesspeople, journalists and other professionals. Face-to-face interviews were conducted in Nigeria and Cameroon, while online interviews for Uganda and Zimbabwe – a consequence of the pandemic-induced travel restrictions. Interviewee recruitment was done through referrals from the Internet freedom community in the four countries studied. The use of referrals was preferred because it has become clear that many users of VPNs globally use the tools not for defeating internet censorship but for other reasons[15], including to access online content they wouldn't normally be able to access because of their geographical location. This study was interested in users who employed VPNs to bypass Internet censorship. The interview questionnaire was developed collaboratively with subject matter experts in the use of circumvention tools in Internet censorship contexts. Pre-test interviews were also conducted to test the fitness of the interview questionnaire. A revised questionnaire (Appendix A) deriving from this exercise was used to collect data on the field in the four countries. Interview consent forms were distributed to interviewees, and data minimization was used in the recording of participant data, which was stored securely. Desk research was done to understand prior work done

15 Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P. Knijnenburg (2020). Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. Proceedings on Privacy Enhancing Technologies ; 2020 (1):83–102.

on the topic, and to learn the policy and legal landscape shaping internet censorship in these countries.

3. Internet censorship country contexts

The Internet censorship contexts prevalent in the four countries are similar. Generally speaking, Internet censorship in Africa in the past decade has been implemented from a supposedly legal "rule of law'' premise. Probably drawing from similar use of legislative authority to legitimize restrictions on Internet freedom elsewhere in the world, particularly from Russian and Chinese models[16], several laws have been passed in Africa to legitimize Internet censorship.

Internet censorship in Cameroon has taken the form of prolonged Internet disruptions, blocking of websites, blocking of social media apps and other messaging apps. For instance, Cameroon has witnessed one of the longest episodes of Internet disruptions in Africa. For 93 days, access to the Internet was cut off, throttled and access to social media and other messaging apps were blocked from January 2017 to March 2017 in the Northwest and Southwest English-speaking regions of the country[17]. This followed the eruption of conflict between these regions and the central government. The English-speaking region of Cameroon had long complained of marginalization by the majority French-speaking regions of the country. Some of the most important legislation employed in directing Internet censorship include Law n° 98/014 of July 14, 1998 governing telecommunications (amended December 29, 2005), Law n° 2010/012 of December 21, 2010 on Cyber Security and Cybercrime and the 2014 Law on the Suppression of Terrorist Acts[18].

16 Valetin Weber, Examining the Expanding Web of Chinese and Russian Information Controls, Berkman Klein Centre, September 17 2019, https://cyber.harvard.edu/story/2019-09/examining-expanding-web-chinese-and-russian-information-controls

17 AccessNow, Victory in Cameroon: after 94 days, the internet is back on, April 20 2017, https://www.accessnow.org/victory-cameroon-94-days-internet-back/

18 Simone Toussi, Overview of Cameroon's Digital Landscape, CIPESA, September 12 2019, https://cipesa.org/2019/09/overview-of-cameroons-digital-landscape/

In Nigeria, the Cybercrime Act of 2015 has been the major legal basis for the arrest of bloggers and online surveillance, which have been the most frequent manifestations of Internet censorship in the country.

Research from civil society in Nigeria has identified a spike in the arrest of journalists and bloggers from 2015[19], a trend which has continued until now. Although there has never been a case of Internet disruption in Nigeria, in 2017 a number of websites relating to the agitation for the creation of the independent state of Biafra from the Nigerian federation were blocked following orders to Internet service providers by the government[20].

Internet censorship in Uganda has taken many forms including Internet disruptions, in 2011, 2016 and the most recent in 2018 with the introduction of a social media tax in the country. In February 2016 access to social media sites such as Facebook and Twitter were restricted during the Presidential elections, in what the President described as "a security measure to avert lies''[21]. Similarly, social media platforms were inaccessible on the day of the President's inauguration on May 12 2016 following a directive from the Ugandan Communications Commission (UCC) to telecommunications providers, including MTN Uganda and Airtel Uganda. More recently the Ugandan government in February 2018 began implementing a social media tax whereby access to a list of 50 social media websites, and other popular websites are blocked to residents unless a daily tax of 500 Ugandan shillings (US $0.02) is paid[22]. The Internet censorship space in Uganda is also characterized by pervasive surveillance, and arrests of bloggers and citizens who challenge the authorities, thus creating a climate of fear when self-censorship thrives. As narrated by an interviewee in Uganda, " When I, as an ordinary Ugandan, see a renowned researcher known locally and

19 Babatunde Okunoye, Maria Xynou, Leonid Evdokimov, Sodiq Alabi, Adeboro Odulami, Elio Qoshi and Chukwuzitere Okoli, Tightening the Noose on Freedom of Expression: Status of Internet Freedom in Nigeria report 2018, June 11 2018, https://ooni.org/documents/nigeria-report.pdf

20 Sodiq Alabi, President Buhari's Secret War on Free Speech, Paradigm Initiative, November 17 2017, https://paradigmhq.org/president-buharis-secret-war-on-free-speech/

21 Briana Duggan, Uganda shuts down social media; candidates arrested on election day, CNN, February 19 2016, https://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/index.html

22 Freedom on the Net Report 2019, Uganda country report, https://freedomhouse.org/country/uganda/freedom-net/2019

beyond like Stella (Nyazi) go through what she's going through, I become afraid and self-censor''. This narrative refers to Stella Nyazi, the popular Ugandan academic who is currently being held by the authorities for critical comments against the government on social media.

The Internet censorship scene in Zimbabwe similarly mirrors those of the countries examined above. There have been social media app restrictions in Zimbabwe. For example in June 2016, following nationwide protests due to a deteriorating economy and widespread corruption, access to the messaging app WhatsApp was blocked in a bid to halt the momentum of protests which also had online expressions using hashtags such as #ThisFlag[23]. Also, in January 2019 following protests triggered by a sharp rise in the cost of fuel, the government blocked Facebook, Twitter and WhatsApp[24]. As with much of the continent, Zimbabwe has also been the setting for arrest of bloggers, journalists and widespread online surveillance.

When governments restrict access to the Internet, Internet messaging apps such as described above, block access to websites, order the arrest of bloggers and closure of media houses, they impinge on human rights, including the right to freedom of opinion, expression and association. Recognizing this, on July 1 2016 the United Nations passed a historic resolution condemning Internet shutdowns and affirming human rights online[25].

Faced with these Internet censorship scenarios in their respective countries, citizens have often resorted to circumvention tools to access the Internet in order to continuously participate in protests, communicate with loved ones, to run their businesses, look for information, or whatever they had been doing with Internet access before it was cut off. This study examines the mechanisms of how citizens in Cameroon, Nigeria, Uganda and Zimbabwe have used circumvention tools to access the Internet during

23 Juliet Nanfuka, Zimbabwe Becomes the Latest Country to Shut Down Social Media, CIPESA, July 7 2016, https://cipesa.org/2016/07/zimbabwe-becomes-the-latest-country-to-shut-down-social-media/

24 ''Zimbabwe blocks Facebook, WhatsApp and Twitter amid crackdown'', BBC News, January 18 2019, https://www.bbc.com/news/world-africa-46917259

25 ''U.N. passes landmark resolution condemning internet shutdowns'', AccessNow, July 1 2016, https://www.accessnow.org/un-passes-resolution-condemning-internet-shutdowns/

periods of Internet censorship.

4. The tools used during Internet censorship in Africa

The tools used to circumvent Internet censorship in these four country contexts are similar, although their degree of use varied according to the particular country in focus. In general the tools used in these country contexts to access censored online content included VPNs and encrypted messaging apps. VPNs were used to access censored online content or apps in all countries studied. They were also used by people to stay anonymous online. The use of VPNs was more frequent from interviewees from Cameroon, Uganda and Zimbabwe who have experienced more incidents of blocked websites and Internet disruptions in the past 5 years. In Nigeria which has experienced few incidents of blocked online content, such as the blocking of 17 websites linked to a secessionist movement in 2017, VPNs were used by those interviewed mainly to stay anonymous online. The use of encrypted messaging apps was common in all the countries studied. Among the 33 interviewees in Cameroon, Nigeria, Uganda and Zimbabwe, about half (17) had 2 or more circumvention tools on their devices. Those who had more than one tool installed on their devices switched from one tool to another depending on which particular tool worked best during a specific Internet disruption. All interviewees used circumvention tools on mobile and desktop devices, although a majority (23) reported mostly using the tools on mobile devices.

5. How circumvention tools are used: Mobilizing during Internet censorship events.

Internet censorship events in Africa involve a number of actors, including governments, telecommunication companies and people who rely on the Internet for information, communication, business and other activities.

More attention seems to have been paid to the processes leading up to Internet disruptions in Africa – such as government orders to telecommunication companies[26], than to how ordinary citizens have coped in the face of Internet censorship. Drawing from interviews across the countries studied, a number of themes stand out.

5.1. The role of diaspora, local political groups, commercial actors and civil society

Diaspora communities, political groups and civil society played an important role in enabling citizens to circumvent Internet censorship. Although the levels of influence of these three groups in mobilizing citizens to defeat Internet censorship was different in the four country contexts studied, their role was nevertheless crucial. In Cameroon and Zimbabwe, for instance, diaspora communities were active in alerting locals to ongoing government plans to disrupt local internet connections, before some residents of these countries were aware of the fact. These groups also disseminated information to residents through a variety of channels (such as SMS messages) on the specific tools such as VPNs to use to circumvent Internet censorship. Also, given the political context of the conflict between the Northwest and Southwest regions of the country against the central government, political groups were also active in disseminating information about circumvention tools. A unique actor observed in the dissemination of information about circumvention tools was local tech businesses. In the Northwest and Southwest Cameroon, local technology entrepreneurs were very active in sharing information about circumvention tools and in helping people install them. Particularly for people who had no know-how on the installation of these tools, they were very helpful. Furthermore, when Internet speeds in these two Cameroonian regions were throttled and people could no longer download circumvention tools, these technology entrepreneurs helped to install them on their devices through USBs, Bluetooth and Xender app – mechanisms which will be described

26 Chiponda Chimbelu, ''The government or the people. Telecoms firms trapped in internet shutdowns'', DW, July 22 2019, https://www.dw.com/en/the-government-or-the-people-telecoms-firms-trapped-in-internet-shutdowns/a-49634343

in detail in this report. In all the countries studied, civil society were also active partners in mobilizing people to use circumvention tools.

A popular means of sharing information about circumvention tools was the use of SMS messages and WhatsApp groups. As narrated by a Cameroonian resident,

> *"Even before the 93-day shutdown there was throttling. And then, I don't know how they used to do this but we would get messages saying the Internet is going to be throttled download VPN. Although I knew about VPNs in the past during this time it became a regular tool. These messages would come by SMS, or from WhatsApp groups and they look like fake news, forwarded as received. But shortly after the Internet would be shutdown as the messages warned they would".*

A Ugandan civil society activist noted,

> *"I shared information on the use of VPNs to my networks and community because I felt this was a public safety issue. I created a series of short links to Psiphon, Betternet and Tor I think that could fit into one SMS message and shared for onward redistribution".*

An interviewee in Zimbabwe stated,

> *"We educated people using SMS on circumvention tools and how to install and use them".*

5.2. Downloads, Bluetooth, Xender and USBs.

The most common method people used to access various circumvention tools was through website and app store downloads. In the four

countries studied, interviewees visited the websites and app store sites of circumvention tools to download the tools. However in Cameroon, in addition to downloads, people who lived in the Northwest and Southwest regions where Internet speeds were throttled had to rely on neighbours, friends and tech entrepreneurs sharing circumvention tool apps through USBs, Bluetooth and the Xender app. As related by a circumvention tool user in Cameroon,

> *"We shared the APKs from our computers to the devices of those that wanted these apps through bluetooth, Xender and USB cables".*

Another Cameroonian stated,

> *"For those who couldn't download VPN because of the throttling we shared VPN apps through Xender and Bluetooth since it would have been difficult to download online".*

Or as related by another user in Cameroon when asked about how he got the circumvention tool on his device,

> *"It was 'Xendered' to me and I started using it"*

A tech entrepreneur in Uganda remarked,

> *"I got the tools via bluetooth and file sharing platforms like Xender. I also downloaded those that could not be shared via Playstore and iPhone Appstore"*

About half (17) of interviewees already had circumvention tools installed before the Internet censorship events while others only sought after circumvention tools after the Internet censorship event.

5.3. Exploiting limited knowledge of censors

In the Internet censorship country contexts studied, the robustness of the community of messaging platforms made available for activists and human rights defenders resulted in the omission of important apps by government censors. When censors block the most popular communication platforms such as Facebook and WhatsApp as was done in Northwest and Southwest Cameroon, or create an extensive list of over 50 communication platforms to be blocked as in the case of Uganda, their limited knowledge of the messaging app ecosystem resulted in them omitting a few. These apps omitted from the censors list then become alternative communication lifelines for citizens. In Cameroon, people resorted to using Telegram, Signal and Firechat messaging apps to communicate and organize when Facebook and WhatsApp were blocked because government censors were initially unaware of Signal.

As narrated by a circumvention tool user in Cameroon,

> *"It also happened that some apps like telegram, which was not known to the government and had a small user base, were not blocked and people switched to using them. There were other lesser known apps too that were not blocked and we tested and recommended that others use them. One of them was firechat".*

Another Cameroonian activist noted,

> *"Since they used to block Facebook and WhatsApp, most of us were now using signal. You didn't even need VPN to access it because the government was not aware and had not blocked it at that time. However government officials became aware of signal. Those of us who were activists used Signal a lot because we were under suspicion as the one sending out information".*

An activist in Zimbabwe also reported using Signal because it was unblocked when other popular messaging apps like Facebook, Twitter and WhatsApp were blocked during the Internet disruptions which followed nationwide protests in January 2020,

> *"I used alternative instant messaging apps that were not blocked, like signal. I also used VPNs during the messaging out blackout but this did not work in the total shutdown"*

Similarly, despite the extensive blacklisting of over 50 communication platforms in Uganda, a resident of Kampala reported resorting to also using Signal and other apps because they was not censored at the time.

> *"In addition to using VPNs, I used mobile alternative apps – signal and Jitsi"*

6. Reasons for adopting specific tools

One of the questions this study sought to answer was what led to the adoption of specific circumvention tools by people experiencing Internet censorship. Given the numerous circumvention tools available and the many choices people have, the factors which led to the use of specific tools included:

6.1. Community recommendations

The most important reason why people in the four countries studied used specific circumvention tools was because of community recommendations. Whether in Cameroon, Nigeria, Uganda or Zimbabwe, people chose one tool over another primarily because their colleagues, friends, neighbours or civil society groups recommended that tool or were already using the tool. As related by a VPN user in Cameroon,

> *“Actually I didn’t have much choice - that was what was on the table, my brother told me it was working and I found out that it worked that I could connect online”.*

And by another activist in Cameroon,

> *“It wasn’t my personal choice. It was at a meeting it was recommended to me”*

6.2. Free cost and low data consumption

Among the interviewees in the four countries studied, the next most important reason for the adoption of circumvention tools was the cost. People generally avoided circumvention tools which demanded subscription fees before they could be used at all. They preferred circumvention tools which offered a free service. The cost of VPNs might have been important because the four countries studied had average incomes either in the lower middle-income group (Cameroon, Nigeria, Zimbabwe) or lower income group (Uganda)[27]. A VPN user in Uganda expressed the thought,

> *“There was a lot of trial and error, you install one and reinstall it when you realize you had to pay.”*

Closely related to this was that users preferred circumvention tools which they perceived to have low data usage to those which were perceived to use up a lot of data. Users of circumvention tools used a method of testing a lot of tools to arrive at those specific tools which they reckoned used less data, or they simply relied on community recommendations on which tools used less tools. For example in Cameroon, people who needed VPNs were referred to the local technology entrepreneurs who had the reputation of having the VPNs which used up less data.

27 Umar Serajuddin and Nada Hamadeh, New World Bank country classifications by income level: 2020-2021, World Bank blogs, July 1 2020, https://blogs.worldbank.org/opendata/new-world-bank-country-classifications-income-level-2020-2021

6.3. Speed of connection and ease of use

Closely linked to the need for free cost and low data consumption was the need for fast and reliable connections by circumvention tools. Users of circumvention tools spoke of the need for VPNs which ensured fast connections, particularly in the context of the poor Internet connectivity in many parts of Africa. Circumvention tool users tend to have known by the experience of using different circumvention tools which tools afforded fast connections to the Internet. Closely linked to ease of use was that users preferred circumvention tools which were easy to use. For instance VPNs which had interfaces which could be easily navigated were preferred. This was best reflected by an activist in Nigeria who reflected,

> *"I didn't want anything complicated as an exam"*

6.4. Safety and security

Following the concerns listed above, the need for safety and security of communications was also raised as a reason for the choice of specific circumvention tools. This was the case with investigative Journalists and activist communities who felt at risk of government surveillance and monitoring. Activists in these contexts were concerned about not leaving a trace online when looking for sensitive information on websites of governments and security agencies for instance. As narrated by an investigative Journalist in Nigeria,

> *"The need for safety informed my choice of tools - the desire not to compromise or jeopardize myself and my sources. One cannot overemphasize the importance of safety"*

7. Usability challenges with tools

The usability challenges encountered by circumvention tool user in the countries studied included:

7.1. Slowness of access with VPNs

The most common usability challenge expressed by circumvention tool users was that the use of VPNs resulted in slow connections to the Internet. Nevertheless, most users who expressed this challenge also understood that this was as a result of how VPNs worked. As narrated by a VPN user in Uganda,

> *"It was slow and cranky and I think that makes sense if you understand how they work"*

In two of the four Internet censorship contexts studied, in addition to using VPNs, people also had other options for defeating the Internet censorship. During the Internet disruption in Northwestern and Southwestern Cameroon some residents of these regions simply migrated to the regions where Internet access was not blocked. As described by a Cameroonian interviewee, they were called "*Internet refugees*",

> *"I returned to Yaoundé because I could not progress with what I was doing in the Northwest region. We were calling ourselves Internet refugees or Internet Internally Displaced persons"*

Similarly, in Uganda people could opt to pay the government mandated social media tax. Interviewees explained that there seemed to be a difference between the Internet censorship of 2016 and that of 2018. In February 2016 access to social media sites such as Facebook and Twitter were restricted during the Presidential elections and they mentioned those websites could easily be accessed with the use of VPNs. With the social media tax of

2018 however they expressed the concern that the implementation of the blockage of websites done by ISPs was done in such a way which made even accessing these websites through VPNs a very unpleasant user experience. Ugandan users of circumvention tools also mentioned that VPNs used in this context used so much mobile data it was just as costly as paying the government mandated social media tax. For many users of these tools in Uganda a combination of the very unpleasant user experience and the increased mobile data consumption of VPNs forced them to pay the social media tax. In Uganda some of the sentiments expressed included,

> *"It was consuming more data and with time you realized you were not saving and that it was perhaps better to pay the 200 Shillings (tax). The government is winning, I have made peace with the fact I have to pay the OTT taxes. What choice do we have?''*

> *"Occasionally I just pay the tax if I'm not in the mood of using VPN. Sometimes the VPN is very stressful.''*

> *"Both for the censorship events (2016 & 2018) I used VPNs. However for the OTT tax I used the VPN for only a week and then got sick of it, I did not enjoy the experience and started to pay the tax. It was slow to turn on, sucking your data and disconnects after a while of not using it. It wasn't worth my emotional and mental health. I know a lot of people use VPNs as a stance against the government, but this felt like we were losing no matter what we did.''*

> *"In 2016 I didn't encounter any difficulties but now with the OTT tax and blocks it's a bit more difficult.''*

In Uganda, another option people had to access the uncensored Internet was through public Wi-Fi and corporate broadband providers who only serviced corporate clients. The social media tax was implemented on

mobile Internet service providers, which service the majority of Ugandans.

7.2 Data caps for VPNs

The second most common usability challenge encountered by circumvention tool users in this study was the data caps encountered in some VPNs. Some VPN services limited users to a daily limit on data after which they were disconnected. As related by a circumvention tool user during the Internet censorship in Northwest and Southwest Cameroon,

> *"I was looking for the one that would still allow me have quality Internet and the one that allows me connect for long before it automatically disconnects. I'm using the Internet within an hour the VPN will automatically disconnect. So I have to reconnect it. I could be in the middle of typing something very important. I could lose it when it disconnects. I don't understand why it was disconnecting. I just thought it was the way the VPN was designed to function. The best one I was using disconnected every one hour - I don't know why it behaved like that"*

This complaint was particularly a common thread in Cameroon, where people tried to stay online during the 93-day Internet disruption. It was clear among a group of 7 interviewees (out of 14) in Cameroon, who were Cameroonian students outside the Internet freedom community, that there was low awareness of free VPN services such which did not implement data caps.

7.3. Advertising pop-ups

Another usability challenge encountered by users of circumvention tools in these country contexts was advertising popping up on the tools. These pop-ups represented a distraction which impacted the user experience negatively. A Cameroonian user remarked,

> *“At the time I was using BestVPN because there were no ads. Others you had ads interrupting.”*

Another circumvention tool user in the Anglophone regions of Cameroon noted,

> *“The difficulty I had was the advertisements that kept popping up. So sometimes you had to turn it off because you don’t want those ads to keep popping up. There were too many ads on the free versions.”*

A tech entrepreneur in Uganda added,

> *“Ads popping up was a problem. Otherwise there was no problem in downloading, installing and using the tools”*

7.4. Authentication problems on accounts and services such as Facebook, Gmail and cPanel

Several users of circumvention tools reported authentication problems while accessing online services. This occurred because of the way VPNs work, by masking the true location of Internet users. Online services thus detect that the user’s natural location has changed, and will only permit access to accounts only after users have met authentication requirements. A businessman in Cameroon explained,

> *“Also with authentication problems and accounts being temporarily blocked on FB (Facebook) and gmail because of change of location. As a webmaster there was a problem with accessing CPanel because of complaints of IP address changes, hence you cannot control your website.”*

8. Recommendations and Further Research directions

This report details how communities in four African countries – Cameroon, Nigeria, Uganda and Zimbabwe mobilized to defeat Internet censorship. It revealed a number of useful insights for practice for the Internet freedom community. Drawing from the findings of the report, the following recommendations seem important, and point to potential future research directions:

1. Widening of information dissemination and support for circumvention tools: A key take-away from this study was that the further away people were removed from the Internet freedom activist community in their countries, the less reliable their VPN information and support was. During episodes of Internet censorship, civil society organizations and their immediate networks tended to have the most reliable information and support on the best circumvention tools to use. Other people far removed from this community – and these tend to be regular residents, such as students or businesspeople, are forced to rely on less than reliable information and support systems for circumvention tools. This was apparent for example in Cameroon where students affected by the 93 day Internet disruption were not aware of widely available free VPN services, and had to rely on subscription based VPNs which were an inconvenience for this group who required uninterrupted Internet access on a low budget. It might be important for the Internet freedom community to study how circumvention tool information diffuses, and also to address the effective diffusion and dissemination of circumvention tool information and support in order to reach the widest possible audience, not just within their familiar civil society contexts.

2. Understanding the "other" VPN users: Another takeaway from this study was that it brought to light again the fact that in any given sample of VPN users, at least half of them[28] use VPNs not to defeat

28 Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P. Knijnenburg (2020). Emotional and Practical Considerations

Internet censorship in the context of Internet freedom for democracy or open societies. Rather, VPNs are used to achieve commercial ends, for example to access online content not normally allowed in their given territories. That is, they used VPNs to overcome commercial censorship, and not necessarily the censorship of authoritarian regimes. It might also be important to understand this community, at least because of their acquired expertise which can be useful during Internet censorship.

3. Understanding government and ISP cooperation for Internet censorship: Interviews done in the four countries suggested that in Uganda the implementation of the social media tax made the use of VPNs especially hard for people. Ugandans who used VPNs during the Internet disruption in 2016 following the Presidential elections, and all other users of VPNs in Cameroon, Nigeria and Zimbabwe did not report similar difficulties with accessing censored content using VPNs. Interviews with these Ugandans suggested that the implementation of the 2018 social media tax censorship made the use of VPNs tedious and impractical, unlike the case in 2016 when VPNs were used to access censored content relatively easily. The difference between the Internet censorship of 2016 and 2018 in Uganda was that while in the former ISPs were unwilling participants, in the latter they were willing partners given the financial incentives they stood to benefit from the social media tax. An important research question might be uncovering if this financial incentive for ISPs was a factor in the increasing sophistication of the censorship which made the use of the VPNs more difficult.

9. Acknowledgments

The author expresses appreciation to the Open Technology Fund (OTF) who funded this study. My appreciation also goes to the Tor Project, my host organization, and Antonela Debiasi, my contact person at the Tor

Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. Proceedings on Privacy Enhancing Technologies ; 2020 (1):83–102.

Project, and collaborator on this research project. Many thanks also go to many colleagues and friends in Cameroon, Nigeria, Uganda and Zimbabwe whose immense contributions made this study possible.

10. Conclusion

Africa is indeed a censored continent, where Internet censorship is a real and constant threat to human freedom. In this challenging context, communities have found ways to mobilize to access censored content using circumvention tools like VPNs.

Although only second in the prevalence of Internet shutdowns to Asia, few studies have been done to understand how communities in Africa mobilize to defeat Internet censorship. This report sheds light on this understudied area, and hopes to be a resource for the global Internet freedom community in their effort to ensure a free and open Internet in Africa.

The urgency of this work is underlined by the fact that in the weeks this report was being concluded, there were Internet disruptions in Ethiopia[29] and Somalia[30], both related to political reasons in both countries. Also, based on previous government action in similar contexts, there is an imminent threat of an Internet disruption in Zimbabwe as mass protests are being planned[31] to draw attention to government corruption. In this Zimbabwean context, it was significant to see a VPN maker, TunnelBear, offer up to 10GB of free data[32] for users of the TunnelBear VPN in the event of an Internet disruption. As noted in this report, data limits on VPNs was one of the major usability challenges users highlighted as a hinderance to accessing the Internet during Internet censorship. It is hoped that the

29 Samuel Getachew, The internet is back on in Ethiopia but there's every chance it'll be off again soon, Quartz Africa, July 24 2020, https://qz.com/africa/1884387/ethiopia-internet-is-back-on-but-oromo-tensions-remain/

30 ''Somalia internet shut down after parliament votes to remove prime minister'', Netblocks, July 26 2017, https://netblocks.org/reports/somalia-internet-shutdown-after-parliament-votes-to-remove-prime-minister-DA3lx6BW

31 ''Zimbabwe police clear streets ahead of anti-government protests'', BBC News, July 30 2020, https://www.bbc.com/news/world-africa-53593492

32 TunnelBear Twitter Account, https://twitter.com/theTunnelBear/status/1288875359723589632?s=20

insights from this report will help the Internet freedom community tailor targeted support for communities encountering Internet censorship in Africa.

Nevertheless, much more research needs to be done. This study examined Internet censorship in four African countries – Cameroon, Nigeria, Uganda and Zimbabwe, and although it revealed important insights, it is important that other country contexts are also put under the researcher's spotlight. It would be valuable for Internet freedom to also understand how communities in other African countries mobilize against Internet censorship.

Appendix: Interview Questionnaire

1. How do you use the Internet everyday?
2. Did you experience Internet censorship in the past?
3. How did you know you were encountering censorship (If 2 was answered as “yes’’)?
4. Did it affect you? If it did, how? Please describe the content that was being censored and the website(s) or app(s) affected.
5. Did you experience the censorship on your mobile devices, or desktop/ laptop or both?
6. What steps did you take in response to this censorship?
7. What tools or solutions do you use to access the internet (during) when you encounter Internet censorship in your country? Please name them.
8. Did you have the tool(s) already installed before the Internet censorship event?
9. How did you find out about these tools or solutions to this censorship?
10. Did you tell anyone else about the tool/tools? If so, who? (their relationship to you rather than their their specific identity (e.g. family member, friend, colleague, neighbour etc), and how?
11. How did you get the tool on your device?
12. What were your primary considerations or concerns in deciding to use this tool?
13. How many tools to overcome internet censorship do have installed on your devices?
14. Do you understand how these tools work? (Detail answer for each tool mentioned).
15. Do you have an interest in understanding how these tools work?
16. Did you encounter any difficulties in using each tool?
17. If yes can you please elaborate?
18. Do you consult anyone for help when you encounter difficulty in using these tools? If yes, who? (Detail responses for each tool mentioned)