The Nature of Information Controls during Electoral Processes

The Case of Kenya 2017 and Zimbabwe 2018 Elections.

The Centre for Intellectual Property and Information Technology Law (CIPIT) is a think tank within the Strathmore Law School, Nairobi Kenya. We further non-partisan research at the intersection of law, technology, and society to ensure ICT applications both spur innovation and respect human rights.

ACKNOWLEDGMENTS

CIPIT is grateful to the Ford Foundation for its grant to our Internet Freedoms Program, now the Technology and Society Program that facilitated this primary research on the legal, policy, and technical forms of information controls during political processes in Kenya and Zimbabwe. We now share our research findings to enable governments, corporates, advocacy organizations, policy circles and human rights defenders shape their programs guided by concrete and verifiable evidence. We're also grateful to all those that participated in data collection and analysis including respondents to the survey, Liquid Telecom, Safaricom PLC, and The Communications Authority of Kenya.

TABLE OF CONTENTS

ABBREVIATIONS

Technical

DASH – Dynamic Adaptive Streaming over HTTP

DNS – Domain Name Server

DoS – Denial of Service

HTTP – Hypertext Transfer (or Transport) Protocol

JSON – JavaScript Object Notation

NDT – Network Diagnostic Test

OONI - Open Observatory of Network Interference

SSH – Secure Shell

TCP/IP – Transmission Control Protocol / Internet Protocol

VPN – Virtual Private Network

Social – legal

AIPPA - The Access to information and Protection of Privacy Act

BAZ - The Broadcasting Authority of Zimbabwe

BSA - The Broadcasting Services Act

CA - The Communications Authority of Kenya

CLCRA - Criminal Law (Codification and Reform) Act

CMTA - Communications and Multimedia Appeals Tribunal

CSP – Content Service Provider

ICA – Interception of Communication Act

IRA - Internet Research Agency

KICA – Kenya Information and Communication Act 1998

KNCHR - The Kenya National Commission on Human Rights

MICC - Monitoring of Interception of Communications Centre

NCIC - The National Cohesion and Integration Commission

POTRAZ - The Postal and Telecommunications Authority of Zimbabwe

SABC – South Africa Broadcasting Corporation

SLAA - Security Laws (Amendment) Act 2014

ZMC - Zimbabwe Media Commission

EXECUTIVE SUMMARY

The Internet has enabled and improved access to and sharing of information in society. However, as more people gain access to the Internet, some actors are seeking ways of controlling it on different levels. This is particularly so during elections, and related political processes and events. In fact, globally, Internet shutdowns have risen steadily from 75 in 2016, 108 in 2017 to 188 in 2018.[1] Most of these shutdowns have happened during elections. Despite these overt controls on the flow of information, there is little primary data to explain how these shutdowns happen and the laws on which they are anchored. If the Internet is to enable meaningful participation in the electoral processes on the African content, it is necessary to understand the nature of information controls for better policy and technical responses.

The Centre for Intellectual Property and Information Technology Law's (CIPIT) research program on information controls applies a systematic, multi-disciplinary approach that involves computer scientists, political scientists and lawyers to better unmask the nature and forms of these controls and shutdowns. This report looks at how Internet freedom is linked to electoral and other political processes by analyzing the legal and policy framework governing information control in Kenya and Zimbabwe. It looks particularly at the controls leading to the August 2017 elections in Kenya and the July 2018 elections in Zimbabwe. The aim is to contribute evidence to the conversation on the relationship between the Internet, human, rights and the wider democratic processes. Therefore, our main research objective is to analyze information controls in Kenya and the region in a systematic manner; in order to identify existing legal structures and policy motivations, and the technical nature of these controls through Internet shutdowns and other forms of censorship.

Background

Elections are intrinsically connected to the democratic trajectory of the country. The Internet offers a platform for the exercise of robust participatory citizenship through access to, and sharing of information. It is therefore necessary to have focused, evidence-based inquiries into the nature and impacts of Internet shutdowns and other activities. Due to the limited data on the nature of such information controls, debates and conversations on Internet shutdowns have assumed a reactionary perspective. This report improves the conversation through proactive research conducted before and after elections in Kenya and Zimbabwe. It seeks to answer the following questions:

1. What are information controls?
2. What legal framework governs information controls?
3. Which actors are involved in the control of information? What role(s) do they play?
4. How is information controlled from a technical perspective?
5. What legal, policy and technical responses do citizens resort to?

[1] Access Now, 'Internet shutdowns in context: Insights from the shutdown tracker project (STOP)' -*< https://www.accessnow.org/keepiton/#take-action> on 6 June 2019.*

We continue to see increased research on the impact of the Internet on socio-political processes especially as an enabler of better social services provision, as a source of hard-to-repress information, and as a platform for expression.[2] In this regard, the former United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression noted:

> *Unlike any other medium, the Internet facilitated the ability of individuals to seek, receive, and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole.*[3]

However, the promise that the Internet offers in promoting human rights can be realized only if people - in their individual capacities - can access and use it in the first place. Barriers to access may be related to economic affordability, digital capacity, or political actions. Information controls before, during, or after elections in Africa are gaining root as a form of censorship. In fact, the African Commission on Human and Peoples' Rights, acting through its Special Rapporteur on Freedom of Expression and Access to Information in Africa, has expressed concern on the continuing trend of Internet shutdowns in Africa including in Chad, Gabon, Democratic Republic of Congo (DRC), Sudan and Zimbabwe.[4]

Complete shutdowns were observed in Chad, Congo Brazzaville, and Uganda for periods of ninety days around election-related events. These shutdowns were justified generally by the respective governments under national security concerns and were enforced through Internet service providers.[5] The shutdowns have led to the denial of access to information at a time that accurate information is most in need. Furthermore, this trend seems to be gaining momentum with more sophisticated forms of control.

The UN passed a non-binding resolution HRC/C/L.20 condemning intentional Internet shutdowns. This was a build up from the previous UN Statement on digital rights that 'the same rights people have offline must also be protected online'.[6] Even after adopting these resolutions, countries such as Ethiopia and Zimbabwe continued to block part or all of the Internet for political reasons, especially protests.

[2] Castells M, 'The impact of the Internet on society: A global perspective' MIT Technology Review, 8 September 2014 -<https://www.technologyreview.com/s/530566/the-impact-of the-Internet-on-society-a-global-perspective/ > on 6 June 2019; Castells M, Networks of outrage and hope: Social movements in the Internet age, John Wiley & Sons, New Jersey, 2015; Wellman B and Rainie L, Networked: The new social opening system, MIT Press, Massachusetts, 2012.

[3] Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Franck La Rue, 16 May 2011, UN Doc A/HRC/17/27, 19.

[4] African Commission on Human and Peoples' Rights, 'Press release by the special rapporteur on freedom of expression and access to information in Africa on the continuing trend of Internet and social media shutdowns in Africa' -<http://www.achpr.org/press/2019/01/d440/> on 6 June 2019.

[5] Mohammed O, 'Twitter and Facebook are blocked in Uganda as the country goes to the polls' Quartz Africa, 18 February 2016 -<http://qz.com/619188/ugandan-citizens-say-twitter-and-facebook-have-been-blocked-as-the-election-gets-underway/> on 6 June 2019.

[6] 'Human rights council concludes thirty-second session after adopting 33 resolutions and one decision' United Nations Human Rights Office of the High Commissioner, 8 July 2016 -<https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=20252&LangID=E> on 6 June 2019.

Key Learnings

A) **There were no Internet shutdowns in Kenya and Zimbabwe in the electioneering period – we applaud the governments for defying the growing trend by African governments to shut down the Internet during elections:** There was no express shutdown of the Internet during the electioneering period in the countries under study. We were however not able to verify other alleged forms of control including throttling Internet connection speed and targeted localized and timed electricity supply disruption in restive zones. The collective experience while monitoring the Internet in Kenya and Zimbabwe during the elections shows that, as the Internet is integrated deeper into the economy, governments are wary to disrupt it. This is a rational decision based on anticipated losses, both political and economic. This was evident in Kenya, which did not explicitly shut down the Internet despite a contested general election and repeat election. Zimbabwe's Internet was considerably stable in the run up to the election on 30 July 2018. However, the resulting challenge of the electoral results led to the suspension of the electoral management body's website. Notably, this was control exerted by a private entity with the twitter account @zim4thewin[7] a digital activist that was protesting the military actions during the riots that followed the announcement of election results in Zimbabwe. In January 2019, Zimbabwe shutdown all Internet services following protests against a Government announcement that it would double fuel prices in that country. The shutdown occurred between 14 and 21 January 2019.

B) **There is a need for broader definitions of information controls beyond technical controls:** Definitions remain problematic. The term 'Internet shutdown' seems to be the most preferred term to describe Internet disruptions that seek to control citizens participation in the electoral process. However, the term information control has a wider scope and is able to cover a number of scenarios that include online censorship alongside Internet shutdowns. Besides governments that are typically considered initiators of Internet disruptions, this term also covers other actors such as Internet Service Providers (ISPs) and hackers. It allows also for more subtle forms of control such as Internet throttling. This was evidenced by CIPIT's investigation of the presence of a middlebox in one of Kenya's leading ISPs.[8]

C) **Internet integration is likely to determine the nature and level of information control:** Information controls online cannot be understood adequately without bringing in their relationship with traditional media (television and radio). Internet penetration and usage is significantly below that of television and radio, and as such government controls may target such media over the Internet. While Kenya did not shutdown the Internet, they eventually shut down four mainstream media channels for 7 days. Also, in the aftermath of the 2017 elections, Kenya passed The Computer Misuse and Cybercrimes Act which represented the Kenyan parliament's fourth attempt to criminalize libel. The Bloggers Association of Kenya challenged the constitutionality of this Act in in the case of *Bloggers Association of Kenya (BAKE) v Attorney General & 5 others.*[9] Subsequently, 26 sections of the Act are currently suspended pending the full hearing and determination of the case.

[7] 'The cyberattack against the Zimbabwe electoral commission' Qurium Media Foundation -*<https://www.qurium.org/alerts/zimbabwe/the-cyberattack-against-the-zimbabwe-electoral-commission/> on 6 June 2019.*

[8] Karanja M, 'CIPIT research reveals evidence of Internet traffic tampering in Kenya: The Case of Safaricom's network' CIPIT Blog, 23 March 2017 -*<https://blog.cipit.org/2017/03/23/cipit-research-reveals-evidence-of-Internet-traffic-tampering-in-kenya-the-case-of-safaricoms-network/>* on 6 June 2019.

[9] (2018) eKLR.

D) **Other actors besides government can exert information controls**: This report maps the actors concerned with Information Controls. Interview questions were conceptualized, and the research team interviewed the relevant officers. Besides the finding that no websites were blocked in Kenya during the elections, ISPs acknowledged that they block some websites using globally acceptable standards. Such websites include sites with child pornography content among others. These standards were, however, not provided and further research is needed to establish the nature of such standards. We should also highlight that it has proven challenging to secure interviews with most of the relevant legal or technical officers; it is likely that such individuals are shying away from engaging, possibly from fear of being quoted or otherwise put on record.

E) **Elections manipulation and foreign interference, a rising form of control:** Dis- and mis-information during the elections was the most used form of information control according to our observations. The project did not originally identify this area of focus, but it soon became clear that it may be the preferred option by political actors to control narratives during political campaigns. This is now a global phenomenon: particularly, Cambridge Analytica was alleged to have attempted to control narratives in Kenya, Nigeria, the Brexit campaigns, and the 2016 US elections. The alleged involvement of Cambridge Analytica in the Kenyan elections raises significant questions on the impact such interference had in that elections. We collected some relevant data from Social Media platforms for exploratory analysis on the possible impact of such control on democratic processes.

F) **Election manipulation seeks to control not access, but the narrative:** Following closely from the previous point E, various actors apart from governments can initiate information controls towards various ends. As Kenyans reflect on the 2017 elections, we continue to witness a lot of attention to fake news and the role of social media in the Kenyan elections. This sort of information control was not designed to deny citizens access to information, but to control narratives online. International media such as Channel 4 interviewed CIPIT in this regard and that research was reported in a number of international media outlets.[10]

G) **Anonymity was crucial for election manipulation to thrive:** From the survey conducted to understand citizens perceptions to information controls, a majority of our respondents considered the Internet as very important or even essential in helping them access, publish or share information during the 2017 elections period. Most of them did so on their mobile phones. However, only a fifth of the respondents thought the Internet was occasionally slow during this period. On the other hand, a majority of the respondents experienced fake news and hate speech during the elections period with the most attribution going to bloggers and social media bots. A third of the respondents did not know who was publishing this information. Most of the respondents did not report these incidences, which may be indicative of apathy or helplessness as to where to report such matters.

[10] Hilsum L, 'Kenyans bombarded with fake news in presidential election' Channel 4 News, 26 Mars 2018 -*<https://www.youtube.com/watch?v=525TpQNmbAI> on 6 June 2019.*

Key Messages (Recommendations)

A) **More technical resources need to be channeled towards studying subtle forms of information control:** CIPIT lauds the Kenyan and Zimbabwean governments for not implementing a complete shutdown of the Internet in the run up to and during their respective elections. That said, it was challenging to verify reports of more subtle forms of control such as the deliberate throttling of Internet speeds and targeted localized and timed electricity supply disruption in restive zones. Current evidence gathering methods cannot distinguish such observations from legitimate network management behavior. We call on the research community to build robust methodologies that can differentiate business-driven throttling from censorship-driven throttling.

B) **More research resources need to be dedicated to studying the information controls ecosystem:** Broader definitions help define the information control ecosystem, which will be more illuminating than individual studies of technical, regulatory, economic, social and political controls. This also ties in subject matter areas and attracts the relevant expertise so that African governments can shed the techno-determinism[11] tag and build confidence in their citizenry while advocating for the adoption of proposed systems. A highlight here is the Social Science One initiative which has partnered with Facebook on a project dubbed 'the effects of social media on democracy and elections', to offer selected researchers privacy-preserving access to Facebook's data.[12]

C) **More legal resources need to be channeled to define the scope and limits of digital rights.** The continued attempt in Kenya to criminalize libel is a form of control, which mis-appropriates the legislative process. This has been used in the past against traditional media but was declared unconstitutional by the Kenyan courts. 26 sections of the said Cybercrimes Act are currently suspended pending the hearing and determination of the issue in court. African parliamentarians need to be more vigilant when dealing with new legislative proposals that are comparable to provisions that have previously been declared unconstitutional by the courts. This will avoid expensive and elaborate proceedings in court. Where courts are not independent enough, as is the case in many African states, a new form of information control is then entrenched. Instead, more investment should be made on studies for how best to balance fake news and national security concerns on one hand, with existing guarantees on digital rights on the other.

D) **All actors should be transparent and have defined standards upon which they block websites:** ISPs, communication authorities and related institutions play a pivotal role in the citizen's ability to receive information online. Therefore, any standards upon which any such actor involved with Internet connectivity applies to block a website, or throttle Internet connectivity for business purposes or otherwise, should be clearly defined and explained to the public. Moreover, it should not be a decision taken by a single individual, but rather by a consensus e.g. by a national security council and even then, with proper judicial oversight. A proper legal framework should be developed in this regard. That said, more technical and legal research is needed here as we are yet to develop the appropriate legal theory to reconcile a number of emergent critical interests.

[11] Scherer S, 'Evgeny Morozov – The folly of technological solutionism' New Media for Social Change, 5 October 2014 - *<http://wpmu.mah.se/nmict142group5/index.php/evgeny-morozov-the-folly-of-technological-solutionism-2013/>* on 6 June 2019.

[12] 'Social science one: Building industry-academic partnerships, Social Science One -*<https://socialscience.one/>* on 6 June 2019.

E) **More research resources need to be dedicated to understanding fake news and disinformation campaigns:** There is little investigation into the alleged disinformation campaigns Cambridge Analytica ran in Kenya, Nigeria, and Britain. The Mueller report in the U.S. is the only comprehensive investigation into a disinformation campaign that indicted 13 Russians, 3 Russian entities and one U.S. citizen.[13] The Kenyan Government should launch a comprehensive investigation of Cambridge Analytica and the alleged interference operations during the 2018 election period. Principles are emerging on how to govern this issue. The Paris Call for Trust and Security in Cyberspace is a good start; it is endorsed by more than 50 nations, 90 non-profits and universities, and 130 private corporations and groups.[14] One of the nine goals of the Paris Call is to ensure foreign actors do not interfere with elections. However, more ought to be done to operationalize these principles in the legal systems of the signatory states.

F) **More institutions and resourced ought to contribute to fact-checking:** Fact-checking is one of the emerging tactics against disinformation campaigns. However, few institutions are currently involved in this including: Africa Check based in Kenya, Nigeria, Senegal, South Africa and the U.K;[15] Zimfact in Zimbabwe;[16] Pesa Check in Kenya, Uganda and Tanzania;[17] and Dubawa[18] in Nigeria. In a similar vein, BBC Africa have also begun a weekly program called Factfinder to analyze fake news on the continent; they show how journalists put a story together.[19] Further, institutions with data science resources can contribute sentiment analysis techniques to demystify, detect and expose psychographic techniques deployed in an active election scenario.

G) **Entrench transparency in campaign financing, Internet advertising and content moderation:** Kenya has a framework for managing electoral finance, the Kenya Election Campaign Financing Act.[20] Political parties are required to report their expenditures to the Independent Electoral and Boundaries Commission (IEBC) within 3 months after the elections. However, it is not clear whether the party expenditure-reporting mechanisms are effective. For instance, because of the Federal Election Commission in the US, we know that the Trump campaign paid Cambridge Analytica $6 million between July and December 2016.[21] Moreover, the legal frameworks for Internet advertising need to be aligned with their mainstream counterparts. It should be clear who is sponsoring the advertisement, why they are sending the message, which other messages are they promoting on a particular platform, and who is paying for it. Moreover, it ought to be easier to flag and enforce take-down orders for anonymous advertisements promoting disinformation and fake news. We therefore call on government, social media platforms, academia, and civil society to work together to develop a stronger policy framework and legal framework that is both relevant and enforceable from a technical perspective.

[13] Muller R, The Mueller report: The final report of the special counsel into Donald Trump, Russia, and collusion, Skyhorse Publishing, Inc, New York, 2019.

[14] 'Cybersecurity: Paris call of 12 November 2018 for trust and security in cyberspace' France Diplomatie: Ministry for Europe and Foreign Affairs -<*https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in*> on 1 April 2019

[15] See generally Africa Check: Sorting fact from fiction -<*https://africacheck.org*> on 6 June 2019.

[16] For the Zimbabwean online fact-checking platform, see ZimFact -< *https://zimfact.org*> on 6 June 2019.

[17] See PesaCheck -< *https://pesacheck.org*> on 6 June 2019.

[18] See Dubawa -< *https://dubawa.org* > on 6 June 2019.

[19] See BBC World Service TV - Factfinder -<*https://www.bbc.co.uk/programmes/w13xttsw*> on 6 June 2019.

[20] *Kenya Election Campaign Financing Act* (No 42 of 2013).

[21] Browse Disbursements - FEC.gov [Internet]. FEC.gov. 2016. Available from: *https://www.fec.gov/data/disbursements/?two_year_transaction_period=2016&data_type=processed&committee_id=C00580100&min_date=09%2F01%2F2016&max_date=09%2F30%2F2016*

1 INTRODUCTION

We began this project with a narrow focus on Internet shutdowns. However, the experience of other forms of control in the electoral process beyond Internet shutdowns, demanded we revise our focus to information controls in general. Several attempts have been made to define various forms of information controls. We continue here the analysis done in the Centre for Intellectual Property and Information Technology Law (CIPIT) May 2018 report, 'Intentional Internet disruptions Africa: Estimating impact in observable and shadow economies' [22]

1.1 Definitions

The phrase 'Internet shutdown' is the most preferred term to describe Internet disruptions that seek to control citizens participation in the electoral process. Our foregoing study defined an Internet connection disruption as:

> *a willful disconnection of access to the Internet or reduction in quality of connectivity by an actor (e.g. a government or terrorist) targeting a specific population within a geographical area for a set duration of time with the intention of limiting Internet communication to or from the area affected.*

While this term was sufficient for the purposes of the previous study, i.e. measuring the economic impact of direct interruption of Internet connectivity on the economy, it does not capture other forms of control that may not interfere directly with technical connectivity but may nevertheless affect citizens' ability to participate in the electoral process, for instance, taxation laws or fake news. Therefore, we adopt the term information control in place of intentional Internet disruption. This term is more comprehensive to accommodate these externalities, while being able to represent both covert and overt forms of information control. Overt control refers to the full-scale network shutdown or individual website blocking while covert control refers to subtle practices such as Internet throttling, which some define generally as online censorship.[23]

Additionally, information control covers other actors such as ISPs) and, hackers, beside governments which are typically considered the initiators of intentional Internet disruptions. It also covers for more subtle forms of control such as Internet throttling. The use of this wider term therefore helps us capture the different forms of control that can be exerted during the electoral process. We define information control for our purposes as follows:

> *A willful disconnection of access to the Internet or reduction in quality of connectivity or other form of control by an actor targeting a specific population within a geographical area that affects their ability to access, share information or otherwise participate in the electoral process online during an electioneering period.*

[22] CIPIT, 'Intentional Internet disruptions Africa: Estimating impact in observable and shadow economies' CIPIT, May 2018

[23] See for example the methodology section of 'Freedom on the net methodology' Freedom House *-<https://freedomhouse.org/report/freedom-net-methodology> on 6 June 2019 and Questions A3 and B1 and Freedom House -<https://freedomhouse.org/report/key-Internet-controls-table-2016 third column> on 6 June 2019 where social media or communications apps are blocked.*

This definition allows us to consider alternative forms of information control apart from the classical Internet shutdown and censorship categories. The rise of fake news, social media taxes, and mobile money taxes in several African jurisdictions have been considered a form of information control. A focus group on this issue also relayed the need to formulate a definition of information control that is not limited to elections. In this regard, we developed the following definition of information control:

> *A willful disconnection of access to the Internet or reduction in quality of connectivity or other form of control by an actor targeting a specific population within a geographical area that affects their ability to access, share information or otherwise participate online.*

1.2 How are information controls measured?

This is the first structured project CIPIT has undertaken with a methodology that combines legal and technical measurements. We partnered with the Open Observatory of Network Interference (OONI) which is a free software, global observation network for detecting censorship, surveillance and traffic manipulation on the Internet. We focused on Internet connection disruptions, which OONI defines as:

a) **Internet blackouts:** When the Internet is switched-off completely in a country or region. This can either be intentional (e.g. government-commissioned) or unintentional (e.g. accidental cable cut). Only an intentional Internet blackout is a form of censorship.[24]

b) **Blocking:** When a site or app is intentionally blocked.[25]

There are several software tests OONI conducts to collect evidence of Internet censorship.

1.2.1 Which websites are blocked?

a) **Web connectivity:** This test examines whether access to websites is blocked through Domain Name Server (DNS)[26] tampering, Transmission Control Protocol (TCP)[27] connection reset (RST) Internet Protocol (IP) blocking,[28] or by a transparent Hypertext Transfer (or Transport) Protocol (HTTP) proxy.[29] Specifically, this test is designed to perform the following:

- Resolver identification;
- DNS lookup;
- TCP connect; and
- HTTP GET request.

[24] OONI's working definition according to OONI's research director.

[25] OONI's working definition according to OONI's research director.

[26] Domain Name Server (DNS): This is the system which automatically translates Internet addresses to the numeric machine addresses that computers use.

[27] Transport Control Protocol (TCP): a set of rules that governs the delivery of data over the Internet or other network that uses the Internet Protocol, and sets up a connection between the sending and receiving computers.

[28] RST stands for Reset, which means a TCP Reset which can be used by a third party to terminate an existing Internet connection between two endpoints.

[29] Hypertext Transfer (or Transport) Protocol (HTTP) is a protocol which transfers or exchanges data across the Internet. It does so by handling a client's request to connect to a server, and a server's response to a client's request. Every time you connect to a server, you (the client) send a request through the HTTP protocol to that server. Such requests include 'HTTP header', which transmits various types of information, including your device's operating system and the type of browser that it is using. If you are using Firefox on Windows, for example, the 'user agent header' in your HTTP request will tell the server that you are using a Firefox browser on a Windows operating system. A transparent proxy is a server or application that intermediates requests between the user and the actual web server to provide a more seamless user experience.

By default, this test performs the above steps on both the user's server and control server except for the first step, which is only performed on the user's network. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, then the websites that the user is testing are likely censored.[30]

b) **DNS connectivity**: This test compares the DNS query results i.e. the result from a DNS resolver,[31] which is considered to be reliable, with the result being tested for DNS tampering. The DNS system is what is responsible for transforming a host name (e.g. torproject.org) into an IP address (e.g. 38.229.72.16). ISPs, amongst others, run DNS resolvers which map IP addresses to host names. In certain circumstances though, ISPs map the wrong IP addresses to the wrong host names. This is a form of tampering, which OONI can detect by running its DNS consistency test.

- This test compares the IP address of a given host name allocated by the Google DNS resolver (which we assume has not been tampered with) with the IP address mapped to that website by a provider. If the two IP addresses of the same website are different, then there is a sign of network interference. When ISPs tamper with DNS answers, users are redirected to other websites or fail to connect to their intended websites.

Note: DNS resolvers, such as Google or your local ISP, often provide users with IP addresses that are closest to them geographically. Often this is not done with the intent of network tampering, but merely for the purpose of providing users faster access to websites. As a result, some false positives might arise in OONI measurements.[32]

c) **HTTP host:** This test examines whether the domain names of websites are blocked. This test implements a series of techniques which help it evade getting detected by censors. It uses a list of domain names (such as bbc.co.uk) to connect to an OONI backend control server, which sends the host headers of those domain names back to OONI. If a 'middle box' is detected between the network path of the probe and the OONI backend control server, its fingerprint might be included in the JavaScript Object Notation (JSON) data received from the backend control server. Such data also reveals if the tested domain names are blocked or not, as well as how the censor tried to fingerprint the censorship of those domains. This can sometimes lead to the identification of the type of infrastructure being used to implement censorship.[33]

[30] See OONI - Web connectivity -<*https://ooni.torproject.org/nettest/web-connectivity/*> on 6 June 2019.

[31] The DNS resolver is that part of the DNS on the user's side that initiates and sequences the query of the resource being sought. For example the translation of a domain name into an IP address.

[32] See OONI - DNS consistency -< *https://ooni.torproject.org/nettest/dns-consistency/*> 6 June 2019.

[33] See OONI - HTTP Host -<*https://ooni.torproject.org/nettest/http-host/*> 6 June 2019.

d) **HTTP requests**: This test tries to detect online censorship based on a comparison of HTTP requests over Tor[34] and over the network of the user. To detect such cases of censorship, OONI has developed a test that performs HTTP requests to given websites over the network of its user, and then over the Tor network. As Tor software is designed to circumvent censorship by making its user's traffic appear to come from a different part of the world, OONI has chosen to use the Tor network as a baseline for comparing HTTP requests to websites. If the two results match, then there is no clear sign of network interference; but if the results are different, then the website that the user is testing is likely censored.[35]

If one of the following is present in the results, then there is a sign of network interference:

- The length of the body of the two websites (over Tor and over the user's network) differs by some percentage;
- The HTTP request over the user's network fails; or
- The HTTP headers do not match.

Note: False positives might occur when the Tor control connection is being discriminated by the server. This happens, for example, when a CloudFlare CAPTCHA (define) page appears.[36]

1.2.2 Which Instant Messaging Apps are blocked?

a) **Facebook Messenger:** This test is designed to examine the reachability of Facebook Messenger within a tested network. OONI's Facebook Messenger test attempts to perform a TCP connection and DNS lookup to Facebook's endpoints from the vantage point of the user. Based on this methodology, Facebook Messenger is likely blocked if one or both of the following apply:

- TCP connections to Facebook's endpoints fail;
- DNS lookups to domains associated to Facebook do not resolve to IP addresses allocated to Facebook.

b) **Telegram:** This test is designed to examine the reachability of Telegram's app and web version within a tested network. More specifically, this test attempts to perform an HTTP POST request, and establish a TCP connection to Telegram's access points (DCs), as well as an HTTP GET request to Telegram's web version (web.telegram.org) over the vantage point of the user. The test is triggered as blocking when connections to all the access points defined in the test fail. Based on this methodology Telegram's app is likely blocked if any of the following apply:

[34] Tor refers to an online anonymity network comprising of an Internet communication method for enabling online anonymity.

[35] See OONI - HTTP Requests -*< https://ooni.torproject.org/nettest/http-requests/ > 6 June 2019.*

[36] Why do I see a captcha or challenge page (Attention Required) trying to visit a site protected by Cloudflare as a site visitor? [Internet]. Cloudflare Support. Available from: *https://support.cloudflare.com/hc/en-us/articles/203366080-Why-do-I-see-a-captcha-or-challenge-page-Attention-Required-trying-to-visit-a-site-protected-by-Cloudflare-as-a-site-visitor-*

- TCP connections to all the tested Telegram access points fail;
- HTTP POST requests to Telegram's access points do not send back a response to OONI's servers.

Telegram's web version is likely blocked if HTTP(S) GET requests to web.telegram.org do not send back a consistent response to OONI's servers.[37]

c) **WhatsApp:** This test is designed to examine the reachability of both WhatsApp's app and the WhatsApp web version within a tested network. OONI's WhatsApp test attempts to perform an HTTP GET request, TCP connection and DNS lookup to WhatsApp's endpoints, registration service and web version from the vantage point of the user. Based on this methodology, WhatsApp's app is likely blocked if any of the following applies:

- TCP connections to WhatsApp's endpoints fail;
- TCP connections to WhatsApp's endpoints fail;
- TCP connections to WhatsApp's registration service fail;
- DNS lookups resolve to IP addresses that are not allocated to WhatsApp;
- HTTP requests to WhatsApp's registration service do not send back a response to OONI's servers.

WhatsApp's web interface is likely blocked if any of the following apply:

- TCP connections to web.whatsapp.com fail;
- DNS lookup illustrates that a different IP addresses has been allocated to webwhatsapp.com;
- HTTP requests to web.whatsapp.com do not send back a consistent response to OONI's servers.[38]

1.2.3 Which censorship technologies are in my network?

a) **HTTP Header Field Manipulation**: This test tries to detect the presence of network components ('middle box') which could be responsible for censorship and/ or traffic manipulation. This test emulates an HTTP request towards a server but sends HTTP headers that have variations in capitalization. In other words, this test sends HTTP requests which include valid, but non-canonical HTTP headers. Such requests are sent to a back-end control server which sends back any data it receives. If we receive the HTTP headers exactly as we sent them, then we assume that there is no 'middle box' in the network which could be responsible for censorship, surveillance and/or traffic manipulation. If, however, such software is present in the network that we are testing, it will likely normalize the invalid headers that we are sending or add extra headers.

i. Depending on whether the HTTP headers that we send and receive from a backend control server are the same or not, we are able to evaluate whether software – which could be responsible for traffic manipulation – is present in the network that we are testing.

ii. Note: A false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated software that is specifi-

[37] See OONI - Telegram test -<*https://ooni.torproject.org/nettest/telegram/ > 6 June 2019.*

[38] See OONI - WhatsApp test -*< https://ooni.torproject.org/nettest/whatsapp/ > 6 June 2019.*

cally designed to not interfere with HTTP headers when it receives them. Furthermore, the presence of a 'middle box' is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

b) **HTTP Invalid Request Line:** This test tries to detect the presence of network components ' middle box' which could be responsible for censorship and/or traffic manipulation. Instead of sending a normal HTTP request, this test sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method – to an echo service listening on the standard HTTP port. An echo service is a very useful debugging and measurement tool, which simply sends back to the originating source any data it receives. If a 'middle box' is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, we assume that there is no visible traffic manipulation in the tested network.

   i. If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error that will subsequently be sent back to OONI. Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it is not always clear what that software is. In some cases though, we are able to identify censorship and/or surveillance vendors through the error messages in the received HTTP response.

   ii. So far, based on this technique OONI has detected the use of BlueCoat, Squid and Privoxy in networks across 11 countries around the world.

1.2.4 Is Tor blocked?

a) **Tor bridge reachability:** This test examines whether Tor bridges work in tested networks. Tor is free and open source software which enables online anonymity and censorship circumvention. It was designed to bounce communications around a distributed network of relays run by volunteers around the world, thus hiding users' IP address and circumventing online tracking and censorship. However, ISPs in various countries around the world are often ordered by their governments to block users' access to Tor. As a result, Tor bridges were developed to enable users to connect to the Tor network in countries where such access is blocked.

b) **This test runs Tor** with a list of bridges and if it is able to connect to them successfully, we consider that Tor bridges are not blocked in the tested network. If the test, however, is unable to bootstrap a connection, then the Tor bridges are either offline or blocked.[39]

c) **Vanilla Tor:** This test examines reachability of the Tor network (which is designed for online anonymity and censorship circumvention). The Vanilla Tor test attempts to start a connection to the Tor network. If the test successfully boot-

[39] OONI - Tor Bridge Reachability -<*https://ooni.torproject.org/nettest/tor-bridge-reachability/> 6 June 2019.*

straps a connection within a predefined number of seconds (300 by default), then Tor is considered to be reachable from the vantage point of the user. But if the test does not manage to establish a connection, then the Tor network is likely blocked within the tested network.[40]

d) **Meek fronted requests:** This test examines whether the domains used by Meek (a type of Tor bridge) work in tested networks. Meek is a pluggable transport[41] which uses domains that are not blocked domains, such as google.com, awsstatic.com (Amazon cloud infrastructure) and ajax.aspnetcdn.com (Microsoft azure cloud infrastructure), to proxy its users over Tor to blocked websites, while hiding both the fact that they are connecting to such websites and how they are connecting to them. As such, Meek is useful for not only connecting to websites that are blocked, but for also hiding which websites you are connecting to. In short, this test does an encrypted connection to cloud-fronted domains over HTTPS and examines whether it can connect to them or not. As such, this test enables users to check whether Meek enables the circumvention of censorship in an automated way.[42]

1.2.5 Are proxies blocked?

a) **Lantern:** This test provides an automated way of examining whether Lantern works in a tested network. Lantern is a centralized and peer-to-peer proxy, which is used as a circumvention tool. It detects whether websites are blocked and, if so, it allows you to access them via Lantern servers or via the network of Lantern users.

This test runs Lantern and checks to see if it is working. If it's able to connect to a Lantern server and reach a control website over it, then we consider that Lantern can be used for censorship circumvention within the tested network. If, however the test is unable to connect to Lantern servers, then it is likely the case that they are blocked within the tested network.[43]

b) **Psiphon:** This test provides an automated way of examining whether Psiphon works in a tested environment. Psiphon is a free and open source tool that utilizes SSH,[44] VPN and HTTP proxy technology for censorship circumvention.

This test runs Psiphon and checks to see if it is working. If it is able to connect to a Psiphon server and reach a website over it, then we consider that Psiphon can be used for censorship circumvention within the tested network. If, however the test is unable to connect to Psiphon servers, then it is likely the case that they are blocked within the tested network.[45]

[40] OONI - Vanilla Tor -<https://ooni.torproject.org/nettest/vanilla-tor/> 6 June 2019.

[41] Pluggable Transports (PT) transform the Tor traffic flow between the client and the bridge. This way, censors who monitor traffic between the client and the bridge will see innocent-looking transformed traffic instead of the actual Tor traffic. See the Tor Project I Tor Project: Pluggable Transports -<https://2019.www.torproject.org/docs/pluggable-transports.html.en> on 6 June 2019.

[42] See OONI - Meek Fronted Requests -<https://ooni.torproject.org/nettest/meek-fronted-requests/> on 6 June 2019.

[43] See OONI - Lantern -<https://ooni.torproject.org/nettest/lantern/ > on 6 June 2019.

[44] Secure Shell protocol (SSH), a cryptographic protocol used to secure transmissions over an unsecured network.

[45] See OONI - Psiphon -< https://ooni.torproject.org/nettest/psiphon/> on 6 June 2019.

1.2.6 What is the speed and performance of my network?

a) **Dash streaming test:** This test measures video streaming performance. DASH is designed to measure the quality of tested networks by emulating a streaming video. This test is called DASH because it uses the DASH (Dynamic Adaptive Streaming over HTTP) streaming technique.

- Running this test can be useful to understand the baseline streaming performance of a specific network connection. It measures video-related metrics as well as network metrics that are key to understand the reason of performance issues.
- When you run the test, it emulates the streaming of a thirty-second video from an M-Lab server. The video is divided in fifteen two seconds segments. When the client requests a video segment, it must also specify the video quality (e.g., SD, HD, Super HD). Of course, the higher the request quality, the bigger the returned segment. During the streaming, the client seeks to use the higher quality that does not load the network, creating queues, so that the streaming can continue smoothly.
- We say the player is simple in that it does not employ algorithms that real players (e.g. YouTube, Netflix) implement to keep the streaming quality stable and to avoid stalls. This simplicity is, however, key to understand the contribution of the network to streaming quality, which otherwise could be masked by smart players' behavior.
- As a result, we expect real players to be generally faster than this test, because they implement more optimization techniques. However, if the throttling of video is caused by congestion at interconnection points, this test may result faster when the network path from the client to the M-Lab server does not pass through the congested interconnection point.
- This network performance test was originally developed by the Neubot project and later integrated into measurement-kit, the engine used by OONI probe-mobile.
- Disclaimer: DASH is a general-purpose performance test conducted against third-party servers provided by Measurement Lab (M-Lab). M-Lab's services require the retention and disclosure of IP addresses for research purposes. Learn more about M-Lab's data governance, see its privacy statement.

b) **Network Diagnostic Test (NDT) Speed Test:** This test provides a sophisticated speed and diagnosis test for understanding the performance of your network. This network performance test was originally developed by The Internet2 Project and is currently maintained by Measurement Lab (M-Lab). NDT is designed to measure the speed and performance of networks by connecting to M-Lab servers close to the user, and by subsequently uploading and downloading random data. In doing so, NDT collects TCP/IP low level information that is useful to examining and characterizing the quality of the network path between the user and the mLab server.

OONI utilizes an implementation of NDT for measurement-kit, which is a network measurement library for running both desktop and mobile network measurement tests. This NDT implementation is included as a test that can be run via OONI's mobile app. Running NDT can be useful as the type of information that it collects can potentially be used to examine cases of throttling.

Disclaimer: NDT is a general-purpose performance test conducted against third-party servers provided by Measurement Lab (M-Lab). M-Lab's NDT services require the retention and disclosure of IP addresses for research purposes. To learn more about M-Lab's data governance, see its privacy statement.

The foregoing exposition gives an appropriate methodology or toolset to discuss the tests we conducted in section 3 i.e. the connectivity tests, reachability of Tor, invalid request line, header field manipulation.

2. How are Information Controls Linked to Electoral Processes?

CIPIT conducted a comparative analysis of the two legal frameworks in Kenya and Zimbabwe that guide Information controls. We also examined legal tools that relate to elections in Kenya, provision of Internet, access to information and national security.

2.1 Kenya's Legal and Policy Framework

The main question to be interrogated here is, did Kenya's legal framework allow for robust participatory citizenship through access and sharing of information online during the electioneering period? We will look at the Constitution, communication laws, penal laws, and information laws in that regard.

2.1.1 The Constitution

The right to access and share information in Kenya is regulated by several bodies that enforce a number of legal frameworks starting with the Constitution. In its bill of rights, The Constitution of Kenya (CoK) defines and limits the freedom of expression in Article 33 (1):

> *Every person has the right to freedom of expression, which includes – Freedom to seek, receive or impart information or ideas; Freedom of artistic creativity; and Academic freedom and freedom of scientific research.*

This provision can be extrapolated to social media and other similar platforms citizens, artists, and academics are likely to use to express their views online. This right is however limited in article 33 (2) which states,

> *The right to freedom of expression does not extend to-*
>
> *a) Propaganda for war*
> *b) Incitement to violence;*
> *c) Hate speech; or*
> *d) Advocacy of hatred that –*
> *i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or*
> *ii) Is based on any ground of discrimination specified of contemplated in Article 27(4).*

Finally, Article 33(3) cautions that in the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others. A few regulatory bodies have the mandate to enforce these elemental provisions in the Kenyan Constitution.

a) **The Communications Authority of Kenya (CA)** Kenya's communications sector is regulated by the Communications Authority of Kenya, a body established under The Kenya Information and Communications Amendment Act (KICA).[46] It has a mandate to facilitate the development of the information and communication sectors including broadcasting, multimedia, telecommunications, electronic commerce, postal and courier services. The Communications Authority may exert some forms of control on the freedom to communicate online alluded to in Article 33(2) above. Notably, this clause was included because of the ethnic post-election violence that took place in 2007-2008 in which hate speech was prevalent.

[46] Kenya Information and Communications Amendment Act (No 2 of 1998).

b) **The National Cohesion and Integration Commission (NCIC)** The NCIC was formed to further regulate hate speech.[47]

Section 13 of the NCIC Act defines hate speech as: threatening, abusive or insulting words or behaviour, or any written material, that is intended to or is likely to stir up ethnic hatred. Hate speech may also be in form of plays, shows or recordings. 'Ethnic hatred' is defined as 'hatred against a group of persons defined by reference to colour, race, nationality (including citizenship)'

Any person who commits an offence under section 13 shall be liable to a fine not exceeding one million shillings or to imprisonment for a term not exceeding three years or to both.

Some of this language may be read as likely to impede citizens ability to impart information online particularly when read with the accompanying sanctions.

c) **The Kenya National Commission on Human Rights (KNCHR):** The KNCHR is a constitutional commission created under the Kenya National Commission on Human Rights Act[48] with a mandate to promote respect for, and develop a culture of human rights and monitor, investigate and report on the observance of human rights in all spheres of life in the Country.[49] This can be read as promoting citizens access to online platforms during the electioneering period.

The following discussion considers how these institutions are involved in the flow of information online in light of communication, penal, and information laws alongside court jurisprudence.

2.1.2 Communication laws (Freedoms of the media and expression)

KICA expounds that the Constitution's freedoms of the media and freedom of expression can be limited under that Act or any other written law. However, such limitations operate only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. In fact, Section 88 of the KICA Act, which allowed the Minister for internal security to take temporary possession of any telecommunication apparatus or any radio communication station or apparatus, was repealed after much public pressure. Similarly, section 29 of KICA on improper use of a system[50] was declared unconstitutional for imposing penal consequences in terms which the judge found to be vague and broad, and therefore unconstitutional. This was decided in *Geoffrey Andare v Attorney General & 2 others,* where the Petitioner had allegedly posted a message on social media described to have been a grossly offensive electronic mail within the meaning of section 29 of the KICA.[51]

The CA is also empowered to make regulations for the better carrying out of the provisions of this section. In fact, in July 2017, The CA and NCIC jointly published Guidelines on the

[47] National Cohesion and Integration Act (No 12 of 2008).

[48] The Kenya National Commission on Human Rights (No 14 of 2011).

[49] Section 8, Kenya National Commission on Human Rights (No 14 of 2011).

[50] A person who by means of a licensed telecommunication system –
a) Sends a message or other matter that is grossly offensive or an indecent, obscene or menacing character; or
b) Sends a message that he knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person, Commits an offence and shall be liable on conviction to a fine not exceeding fifty thousand shillings, or to imprisonment for a term not exceeding three months or to both.

[51] (2016) eKLR.

Prevention of Undesirable Bulk Political Messaging via SMS.[52] These political messaging guidelines were designed to prohibit Content Service Providers (CSPs) from sending unsolicited bulk messages to customers who hadn't subscribed for the service. CSPs should ensure that all recipients of political messages choose to opt-in to the service. However, the CIPIT report on investigating the privacy implications of applying biometrics to the Kenyan elections showed that there was significant microtargeting during the campaign period using an opt-out as opposed to an opt-in mechanism. The report also shows that these guidelines were effective in controlling hate speech than protecting Kenyans biometric and voter data. This form of information control on hate speech is in compliance with the law. However, no messages in vernacular were allowed, which may relate to the sensitivity under which the hate speech law was enacted.

It is worth noting that the 2017 Kenyan elections occurred at a time when the Kenyan government was developing a new country-wide ICT Policy. This is important because of the dissonance that has been experienced between media policies and ICT policies in Kenya. It has been noted that while Kenya has actively promoted and supported the development of technologies that bolster the horizontal flow of information, it has devoted substantial effort to control the substance of information flowing via these technologies.[53] For instance, KICA establishes the Communications and Multimedia Appeals Tribunal (CMAT)[54] with jurisdiction to receive complaints from persons aggrieved by any publication or conduct of a journalist or media enterprise.[55] Among other remedies, CMAT may issue a fine of not more than **twenty million shillings** on any respondent media enterprise and a fine of not more than **five hundred thousand shillings** on any journalist adjudged to have violated KICA. These fines have been criticized as excessive and they may impede journalists publishing on social media particularly on controversial topics usually experience in a political campaign.

Moreover, journalists are additionally subject to the Complaints Commission established under the Media Council Act (MCA).[56] Here again, persons aggrieved by any publication by or conduct of a journalist or media enterprise in relation to the MCA may make a complaint to the Complaint Commission. The Commission also has jurisdiction to levy a fine of not more than **five hundred thousand shillings** on any respondent media enterprise and a fine of not more than **one hundred thousand shillings**, on any journalist, adjudged to have violated the Act or Code of Conduct. The need for this multiplicity of these complaints' mechanisms with overlapping jurisdictions, which may potentially lead to double jeopardy has in itself been questioned. [57] More importantly, it may intimidate journalists.

[52] Pamoja and Communications Authority of Kenya, 'Guidelines on prevention of dissemination of undesirable bulk and premium rate political messages and political social media content via electronic communications networks', July 2017.

[53] Gichuki D, Gwagwa A and Rutenberg I, 'Historical antecedents and paradoxes that shaped Kenya's contemporary information and communication technology policies' XII Africa Policy Journal, 2016, 61.

[54] Section 102, Kenya Information and Communications Amendment Act (No 2 of 1998).

[55] Section 102A, Kenya Information and Communications Amendment Act (No 2 of 1998).

[56] Media Council Act (No 46 of 2013).

[57] Ali I, 'Limitations on media freedom: Are the current media laws in compliance with the constitution of Kenya?' Published LLB Thesis, Strathmore University Law School, Nairobi, 2017.

2.1.3 Penal laws (Penal code, counter-terrorism)

In a bid to counter terrorism activities, Kenya passed the Prevention of Terrorism Act[58] in 2012 to provide measures for the detection and prevention of terrorism. An amendment in 2014 via Security Laws (Amendment) Act (SLAA) 2014,[59] was passed to ban publications of any material that promoted terrorism. Section 64 of the SLAA introduced a new section 30A in the Prevention of Terrorism Act. The section criminalized anyone who published or uttered a statement that is likely to be understood as directly or indirectly encouraging or inducing another person to commit or prepare to commit an act of terrorism. Section 30A (3) specifies that it is irrelevant whether any person is in fact encouraged or induced to commit or prepare to commit an act of terrorism.

2.1.4 Information Laws (Cybersecurity and privacy)

For citizens to participate meaningfully in elections debate, they need sufficient information for instance, on electoral data. IEBC passed the Elections (Technology) Regulations 2017 to regulate the electoral technology being used by the Commission. Part V on Information Security and Data Storage requires the IEBC to put in place mechanisms to ensure data availability, accuracy, integrity and confidentiality. The IEBC is therefore able to exert control over the free flow of information particularly during the voter tallying stage of the elections. Kenya did not have specific cybercrimes or privacy legislation during the period of study. It is noteworthy that the country subsequently passed the Computer Misuse and Cybercrimes Act 2018 and has promised to pass privacy legislation in 2019.

2.1.5 Court Jurisprudence

The Kenyan judiciary is largely seen to be independent compared to its contemporaries on the continent. It has made several moves to protect the fundamental rights of citizens online in the past few years. For instance, in a recent case, *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others,*[60] the court declared unconstitutional CA's decision to implement a Device Management System interfacing with Kenya's mobile network providers which would give access to subscribers' data and thereby breach their constitutional right to privacy. Even more importantly for the future, the Court declared that any policy decisions or Regulations affecting the public must conform to the Constitution and the relevant statute in terms of both its content and the manner in which it is adopted and failure to comply renders the policy decision, Regulation or guideline invalid.

In 2015, Section 64 of the Prevention of Terrorism Act 2012 as amended above, was declared unconstitutional in the case of *Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others.*[61] A five-judge bench of the High Court declared

[58] No. 30 of 2012

[59] No. 19 of 2014

[60] (2018) eKLR.

[61] (2015) eKLR and *James Omariba Nyaoga & another v Speaker of the County Assembly (Kisii) & 2 others* (2015) eKLR

unconstitutional Section 64 of SLAA alongside Section 66A of the Penal Code[62] for violating the freedom of the media and the freedom of expression guaranteed in articles 33 and 34 of the Constitution respectively.

In 2016, Section 29 of the Kenya Information and Communication Act was declared unconstitutional in the case of *Geoffrey Andare v Attorney General & 2 others.*[63] The High Court declared Section 29 unconstitutional because it violated Article 33 of the Constitution by imposing a limitation on the freedom of expression in vague, imprecise and undefined terms in a manner that goes outside the scope of the limitations allowed under Article 33 (2) of the Constitution.

In 2017, Section 194 of the Penal Code which provided for criminal defamation was ruled unconstitutional in *Jacqueline Okuta & another v Attorney General & 2 others.*[64] The High Court declared that Section 194 was unconstitutional for violating the fundamental right to the freedom of expression guaranteed under Article 33 of the Constitution.

Similarly, in the case of *Robert Alai v The Attorney General & another.*[65] Section 132 of the Penal Code, which provided for the offence of undermining the authority of a Public Officer, was declared unconstitutional. The High Court declared that the right to freedom of expression enshrined in Article 33 of the Constitution can only be limited in accordance with Article 24 of the Constitution and that Section 132, which criminalizes criticism is a curtailment of the right to speak about public officers and is in violation of Article 33 and therefore unconstitutional.

In 2018, 26 sections of the Computer Misuse and Cybercrimes Act were contested on the ground that they were contrary to the right to freedom of expression in the case of *Bloggers Association of Kenya (BAKE) v Attorney General & 5 others.* The said sections are currently suspended pending the full hearing and determination of the case.

The foregoing legal framework shows the tension between the Constitution's desire to entrench a participatory framework and the number of ways that the legislative process can be appropriated to curtail such efforts. The judicial arm of government is seen to arbitrate this conflict actively to restore balance and issue further guiding declarations. While a majority of this tension has played out offline with traditional media, it is likely to get more intense given the ubiquity and propensity of information going viral on social media platforms. We now look at other industry players and their take on information controls.

[62] Section 66A, Penal Code, (Cap 63 of 2014): Prohibited publications and broadcasts

(1) A person who publishes, broadcasts or causes to be published or distributed, through print, digital or electronic means, insulting, threatening, or inciting material or images of dead or injured persons which are likely to cause fear and alarm to the general public or disturb public peace commits an offence and is liable, upon conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years or both.

(2) A person who publishes or broadcasts any information which undermines investigations or security operations by the National Police Service or the Kenya Defence Forces commits an offence and is liable, upon conviction, to a fine not exceeding five million shillings or a imprisonment for a term not exceeding three years, or both.

(3) The freedom of expression and the freedom of the media under Articles 33 and 34 of the Constitution shall be limited as specified under this section for the purposes of limiting the publication or distribution of material likely to cause public alarm, incitement to violence or disturb public peace.

[63] 2016] eKLR.

[64] [2017] eKLR.

[65] [2017] eKLR.

2.1.6 Actor Mapping

We held interviews with industry players involved in Internet control processes to understand their roles and responsibilities. We interviewed a regulator, an ISP and a mobile service provider. The foregoing discussions were based on the following talking points:

1. On which laws is your mandate embedded in?
2. As the communications regulator, what is your role in ensuring that Kenyans' access to the Internet is not unduly restricted?
3. Are Internet disruptions such as (social media blackouts/Internet throttling/website blocking) founded on any law?
4. Do you receive any complaints from consumers who are affected by the disruptions in (3) above?
5. What are your standard operating procedures in dealing with consumer complaints?
6. What rights do consumers of Internet services have?
7. Are deliberate Internet disruptions, such as social media blocking, retrogressive to the economy?
8. As a regulator, how do you actualize your independence from state agencies and corporations?

Communications Authority (Regulator)

The CA emphasized that it is an independent body that is free from external controls and the State regarding the State Corporations Act Cap 466. It is governed by KICA. They expound on the right to information on Article 35 of the Constitution that grants every citizen the right to access information held by the State or any other person and required for the exercise or protection of any right and fundamental freedom. The CA explains that its statutory mandate is to license all systems including the Internet Service Providers (ISPs) which allows for access of Internet and a range of Internet services. The CA also licenses Kenya Network Information Centre (KeNIC) as the Registrar in charge of the management and administration of the dot ke Country Code Top-Level Domain.

The CA also give the consumer perspective by the Article 46 on consumer rights of the CoK together with the Consumer Protection Act No. 46 of 2012 that providers that every consumer has a right to access basic effective communication services and to receive quality service that is safe and secure. CA is therefore charged with the responsibility of protecting the interest of consumers in relation to the services rendered. It ensures that the Licenses have certain conditions as follows:

- The minimum quality of services that Licensees can offer to the consumer;
- The procedure to be followed in supply of these services;
- The benchmarks that have been set to maintain these standards; and
- The methods of redress availed to the consumer in any event that the service rendered fall within the stipulated requirement.

This also means that the Authority is governed by the KICA (Dispute Resolution) Regulations 2010 and the Communications Authority Dispute Procedure Manuals to handle disputes that arise from Licensees and Consumers.

The CA recognizes that in this era where economic initiatives are explored over the Internet, full realization of this key resource will allow the use of the Internet for the benefit of the Country's development and sustainability without limits. CA concludes that in its due capacity, it confers full access to information that safeguards public interest and integrity.

For the ISP and the mobile network operator, the interviews were based on the following talking points.

1. In your license, are there any clauses that touch on instances where the Regulator may order you to disrupt the Internet/ blackout social media/block a website?
2. What obligations and duties do you owe your customers?
3. Can a customer sue you for breach of these duties?
4. Under what circumstances will you throttle or deny your customers access to the Internet?
5. Have you ever participated in an Internet shutdown/ blockade/ disruption of service?
6. Have you ever been instructed to block a website? If yes, when? Why?
7. Are instructions to shut down the Internet in Kenya based on any law?
8. What has been the reaction of customers to Internet shutdowns?
9. Do you think you have an obligation to uphold the right of access to Internet as an ISP?
10. Under what circumstances would you be justified to control access to the Internet?
11. Would you cooperate with state agencies in shutting down the Internet?

Liquid Telecom (ISP)

Liquid Telecom (Liquid) is a leading independent data, voice and IP provider in eastern central and southern Africa. It supplies fiber optic, satellite and international carrier services to Africa's largest mobile network operators, ISPs and businesses of all sizes. It also provides payment solutions to financial institutions and retailers, as well as award winning data storage and communication solutions to businesses across Africa and beyond.

Liquid confirmed that there were no instances in its license with its regulator that may order it to disrupt the Internet, blackout social media, or block a website. The obligations Liquid considers owing its customers include good quality service, and confidentiality based on the contract signed with the customer. Liquid consider that they throttle or deny customers lawful access to the Internet where the customer is misusing the service and is using it for unlawful activity. Unlawful activity here includes fraud and spreading hate speech. The denial of service is usually in response to a court order or a warrant as Liquid does not track customer usage.

Liquid confirmed that they have not participated in an Internet shutdown, blockage or disruption of service to exert control over the flow of information. They have however had disruption of services due to cable cuts, which they term common. They usually email their clients to inform them of the disruption. They have a Service Level Agreement where, if there is a particular outage for a particular period of time, they apply an escalation matrix which affects the service credits. If a customer lacks Internet for a number of hours, they get a percentage of service credits. Liquid maintain a Network Operation Team in this regard.

Liquid are concerned that provisions of the Computer Misuse and Cybercrimes Act 2018 gives too much power to security agencies, concerns which they expressed during the draft bill negotiations. They consider their mandate both as an obligation to uphold the right of access to the Internet as an ISP and as a business interest. They would only be justified to control access to the Internet when the authorities flag a customer who is suspected to be using the Internet for unlawful purposes and would only cooperate with state agencies to shut down the Internet if it was justified by a court order.

Safaricom (Mobile Network Operator)

Safaricom PLC is a listed Kenyan mobile network operator. The firm offers mobile telephony, mobile money transfer, consumer electronics, ecommerce, cloud computing, data, music streaming, and fiber optic services. It is most renowned as the home of MPESA, a mobile banking SMS-based service.

Safaricom confirmed that there were no instances in its license with its regulator that may order it to disrupt the Internet, blackout social media, or block a website. They highlighted that section 88 of KICA was now repealed. This was a section that gave the minister in charge of internal security powers, on the declaration of any public emergency or in the interest of public safety and tranquility, by order in writing, direct any officer duly authorized in that behalf, to take temporary possession of any telecommunication apparatus or any radio communication station or apparatus within Kenya.

Safaricom consider their obligations and duties as: to provide their customers with services as have been advertised, other obligations as a licensee of CA, maintaining the quality of service, rates and communication of terms and conditions. A customer can sue for breach of this duties, but they have not yet been sued on issues touching on Internet service.

Safaricom confirm that they do not throttle the Internet. For products like fiber home Internet, the more the devices connected on a router, the lower the speeds. They confirm that they have not participated in an Internet shutdown, blocking of a website or disruption of Internet service. Safaricom considers itself to uphold the right of access to the Internet as an ISP but feel justified to control access in certain situations they describe as globally acceptable such as child sex online. On whether they would cooperate with state agencies in shutting down the Internet, they would only do so if the state agents demonstrate the legal basis of the instruction

2.2 Zimbabwe's legal framework

2.2.1 Introduction

The study of Internet shutdowns in Zimbabwe was done against the backdrop of the 2018 general elections and the protests following the announcement of fuel price increases in January 2019. The Mugabe regime was deposed through a military-assisted transition in November 2017, after which Emmerson Mnangagwa ascended as ZANU PF and State President until elections were held in July 2018. Violence broke out on 1 August 2018 after the election results were disputed. Soldiers were used to quell the protests. The economy continued on a downward spiral. Fuel prices were increased in January 2019 leading widespread protests. The Internet was shut down following a government directive for periods beginning 14 all the way to 21 January 2019 when the court issued the ruling that the Internet blackouts were illegal and ordered the government to restore full Internet access to the whole country.

The new Government promised to conduct fundamental reforms that would open up the democratic space, which would include legislative reforms focusing on some of the laws used to stifle expression, association and assembly. None of these laws have been repealed to date.

2.2.2 Legal Framework

The aftermath of the 2008 elections broached a power sharing agreement between the incumbent Robert Mugabe and his closest challenger, Morgan Tsvangirai, The Global Political Agreement (GPA).[66] Discussions pursuant to the GPA led to a new constitutional dispensation in Zimbabwe 5 years later. The Constitution of Zimbabwe (CoZ) presents a Bill of Rights in part 2 which provide for a participatory environment online with articles 57 (right to privacy), 58 (freedom of assembly and association), 61 (freedom of expression and freedom of media) and 62 (access to information). Furthermore, the CoZ in Chapter 12 creates the Zimbabwe Human Rights Commission, the and the Zimbabwe Media Commission. These institutions ought to ensure that a suitable environment for citizens to assemble and discuss pivotal issues online during election campaigns.

Even then, laws from the pre-2013 Constitution remain that threaten such a participatory environment. These include the Access to Information and Protection of Privacy Act (AIPPA), the Broadcasting Services Act (BSA), the Criminal Law (Codification and Reform) Act, the Interception of Communications Act (ICA), the Statutory Instrument 142 of 2013 on the Postal and Telecommunications (Subscriber Registration) Regulations (Postal Regulations). This is just a sample to show the existing challenges that Zimbabwe's legal framework poses to citizens meaningful participation in the electoral process.

[66] Global Political Agreement. Zimbabwe; 2008.

2.2.3 Communication Laws (Access to Information and Protection of Privacy Act and Broadcasting Services Act)

The Access to information and Protection of Privacy Act (AIPPA): This Act meant to improve accountability of public entities by giving Zimbabweans a right of access to records and information held by public bodies. This entails a right to correct misrepresented information and to prevent unauthorized collection, use or disclosure of information by public bodies. Interestingly, AIPPA also regulates mass media through a Media and Information Commission. Access to information is pivotal to empower those who desire to engage on topical issues particularly in campaigns. Understandably there are exceptions to this provision, for instance, sensitive information that may be harmful to law enforcement processes and national security.[67] The exemptions to access are however thought to preclude a practical exercise of the right and thereby no corresponding obligation by the State.[68]

Zimbabwe Media Commission (ZMC): The Commission was first created under AIPPA and later on elevated to a Constitutional Commission via constitutional amendment 19 Of 2009.[69] The ZMC oversees an accreditation system under which journalists are required to seek accreditation. This is common practice, even Kenya has a Media Council in that regard. Such institutions are however run as professional bodies whereas the 9 Board of Commissioners in the ZMC are all presidential appointments. This questions the institution's independence as a regulator and indirectly its ability to be partial to the journalists it accredits.

The Broadcasting Services Act (BSA): The BSA establishes the Broadcasting Authority of Zimbabwe (BAZ) to provide broadcasting standards, regulate the broadcasting frequency spectrum, and license broadcasting services and signal carriers. The BSA signifies the reform by repealing its precursor the Broadcasting Act. The latter's provision was declared unconstitutional for violating freedom of speech; the provision declared the operation of a signal transmitting station outside the existing government infrastructure illegal.

The Broadcasting Authority of Zimbabwe (BAZ): The independence of the BAZ is similarly in question given that 9 of the 12 members of its Board are presidential nominees.[70] While the BSA gives the Information Minister discretion to give the BAZ general directions relating to policy, the BAZ is required to take all necessary steps to comply with any direction given to it in that regard.[71] The Kenyan equivalent of the BAZ, the Media Council of Kenya has been mandated in, The Media Council Act, to have a diverse governing committee made up of journalists, legal professionals and representatives of the executive to ensure all views are considered.

[67] Section 17, Access to information and Protection of Privacy Act (No 31 of 2016).

[68] Section 102, Kenya Information and Communications Amendment Act (No 2 of 1998).

[69] Zimbabwe Media Commission, 'About the organisation' *-< http://mediacommission.co.zw/index.php/about-the-company/> 1 April 2019.*

[70] Section 4(2)(a) Broadcasting Services Act (Chapter 221).

[71] Section 4B(1) and (2) Broadcasting Services Act (Chapter 221).

2.2.4 Penal Laws (Criminal Law (Codification and Reform) Act)

The Criminal Law (Codification and Reform) Act (CLCRA) was intended to consolidate and amend the criminal law of Zimbabwe stating in its preamble that it was desirable to codify and where necessary, reform the common criminal law of Zimbabwe in conformity with the fundamental principles set out in the Constitution and other fundamental principles developed over time by Zimbabwe's criminal justice system. Ironically, Chapter 3 – crimes against the state - Section 33 thereof makes it a criminal offence to undermine the authority of, or insulting the President by publishing in electronic or print media.

Undermining the President's authority seems to equate to any statement concerning the president with the knowledge or realization that there is a real risk or possibility that the statement is false and that it may engender feelings of hostility towards; or cause hatred, contempt or ridicule of the president. Insulting on the other hand constitutes an abusive, indecent or obscene statement about or concerning the president. This offense is accompanied by a jail term of up to one year. This provision has been used against dissenting voices and led to self-censorship among upcoming journalists and independent media.[72]

2.2.5 Information Laws (Interception of Communications Act [ICA])

The Interception of Communication Act (ICA) provides for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe. It also provides for the establishment of a monitoring center. The definitions of interception[73] – to listen to, record or copy the contents, whether in whole or part, communication which is sent - has been criticized as too broad as to enable the government to surveil its citizens and thereby infringe on their privacy. Telecommunication providers are then required to give an interception interface to The Monitoring of Interception of Communications Centre (MICC) established under the Act.[74] Moreover, there is no judicial oversight for applications of warrants of interception, the authorized persons can make the application directly to the Minister of Transport and Communications,[75] which usurps the native power of the judiciary. An analogy can be drawn between the MICC's mandate and that of the Device Management System in Kenya discussed in 2.1.5 above that was declared unconstitutional for infringement of privacy.

The Postal and Telecommunications (Subscriber Registration) Regulations (Postal Regulations): These are Regulations made by the Minister of Transport, Communications and Infrastructural Development made under The Postal and Telecommunications Act.[76] The Regulations make it mandatory for telecommunication service providers to register the

[72] Gichuki D, Gwagwa A and Rutenberg I, 'Historical antecedents and paradoxes that shaped Kenya's contemporary information and communication technology policies' XII Africa Policy Journal, 2016, 61.

[73] Section 2, Interception of Communication Act (No 6 of 2007).

[74] Sections 4 (Establishment of monitoring center) and 9 (assistance by service providers), Interception of Communication Act (No 6 of 2007).

[75] Section 5, Interception of Communication Act (No 6 of 2007) – authorized persons to apply for warrant of interception.

[76] Section 99 passed via Statutory Instrument 142 of 2013

customer details of a potential subscriber before any sim-card is activated. This includes their full name, permanent residential address, nationality, gender, subscriber identity number, and the national identification number or passport number.[77] Failure to provide accurate information attracts a six-month prison sentence. The same practice is the norm in Kenya and is mandated by the Communications Authority of Kenya (CA).[78] However, the Postal Regulations in Zimbabwe go on to create a central subscriber information database which is updated monthly through reports by the service providers.[79] The database is among other things meant to enable the Postal and Telecommunications Authority of Zimbabwe (POTRAZ) to assist law enforcement agencies or safeguarding national security.[80] Further, this enables surveillance particularly given most citizens will be using social media to access and share information online.

The vague and broad powers granted to the executive by this instrument also serve to defeat any potential of judicial oversight, hence there is an abrogation of normal constitutional guarantees.

2.2.6 Court Jurisprudence

In a recent landmark ruling, Zimbabwe Lawyers for Human Rights & Media Institute of South Africa vs The Ministry of State in the President's Office of National Security,[81] the High Court ruled that the Ministry of State in the President's Office responsible for National Security does not have the authority to issue any directive in terms of Interception of Communication Act and therefore the directives issued by the Minister to shut down the Internet in Zimbabwe was illegal. The decision further required mobile network operators and Internet service providers to restore full Internet access including access to social media applications and websites such as WhatsApp and Facebook which had been restricted since the morning of Tuesday 15 January 2019.

2.3 Conclusion

The foregoing analysis of the applicable legal frameworks in Kenya and Zimbabwe sets the necessary foundation to understand whether there is a co-relation between the legal framework of a country and the resulting technical controls to control information. In order to do so, we must first look at the nature of controls that occurred in that period.

[77] Regulation 4, Postal and Telecommunications.

[78] Kenya Information and Communications (Registration of SIM-Cards) Regulations, 2015.

[79] Regulation 8, Postal and Telecommunications.

[80] Regulation 8 (2)(b) Postal and Telecommunications.

[81] No 265 of 2019.

3. HOW ARE INFORMATION CONTROLS EXECUTED DURING ELECTORAL PROCESSES?

A significant motivation to conduct this project comes from the awareness that regulatory frameworks can be appropriated or even circumvented to exert different forms of information controls. We have explored the breadth of the legal frameworks in Kenya and Zimbabwe, classifying them into the relevant spheres of law e.g. communication laws (freedom of media and freedom of expression), penal laws (penal code), information laws (privacy, data protection and cybersecurity). Even without these legal justifications, actors may limit the right of other citizens to access and share information in the participative process that occurs during electioneering periods. A good example is the offline traditional media shutdown in Kenya.

The enactment of overly broad laws in both Kenya and Zimbabwe that have subsequently been declared unconstitutional also add to this argument. For instance, the Kenya's new Computer Misuse and Cybercrimes Act 2018 in Kenya was suspended for criminalizing libel. In the *Geoffrey Andare v Attorney General & 2 others* Justice Mumbi Ngugi declared section 29 of KICA unconstitutional.[82] Subsequently, the *Jacqueline Okuta & another v Attorney General & 2 others* rendered section 194 of the Penal Code unconstitutional.[83] Robert Alai's challenge against his charge for posting an offensive post against the President led to section 132 of the Penal Code [84] being declared unconstitutional in *Robert Alai v The Hon Attorney General & another.* The challenges against sections 23 and 24 of the Computer Misuse and Cybercrimes Act 2018 would imply a fourth attempt to use the legislative process to criminalize what is inherently a civil wrong. The challenges to the 26 sections are said to 'reintroduce the purged sections of the law while imposing even more restrictions on the freedom of expression'. [85] There is need for stronger regulatory frameworks to put to rest attempts to appropriate legislative frameworks in this manner.

[82] (2016) eKLR. In this case, it was held that a person who by means of a licensed telecommunication system—
(a) Sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
(b) Sends a message that he knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person, commits an offence and shall be liable on conviction to a fine not exceeding fifty thousand shillings, or to imprisonment for a term not exceeding three months, or to both.

[83] (2017 eKLR). Here, it was held that 'any person who, by print, writing, painting or effigy, or by any means otherwise than solely by gestures, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, is guilty of the misdemeanor termed libel'.

[84] (2017 eKLR). Here, it was held that 'any person who, without lawful excuse, the burden of proof whereof shall be upon him, utters, prints, publishes any words or does any act or thing, calculated to bring into contempt, or to excite defiance of or disobedience to, the lawful authority of a public officer, is guilty of offence and is liable to imprisonment for a term not exceeding three years."

[85] Wamathai, 'Justice Chacha Mwita suspends 26 sections of the Computer Misuse and Cybercrimes Act', BAKE, 29 May 2018 -<https://www.blog.bake.co.ke/2018/05/29/justice-chacha-mwita-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act/> on 6 June 2019.

3.1. Kenya's 2017 elections

3.1.1 OONI Measurements in Kenya

On technical measurements, OONI facilitated the population of the Kenyan-specific background profiles to enable relevant measurements during our research. The first step in measuring these forms of information controls is to determine the websites to be tested. In this case, it only required an update to an existing list maintained by the Citizen Lab i.e. Citizen Lab's Kenyan test list.[86] This ensures that as many URLs with the potential for blocking or censorship are tested. The types of URLs that were added to the Kenyan list fall under 30 categories,[87] ranging from news media, file-sharing and culture, to provocative or objectionable categories, like pornography, political criticism, and hate speech.

All of the URLs in both the Kenyan list and the global list [88] (containing internationally relevant websites) were tested for censorship through OONI's Web Connectivity test. This test is designed to examine whether access to websites is blocked through DNS tampering, TCP connection RST/IP blocking, or by a transparent HTTP proxy. Even then, testing was not limited to the blocking of websites. The reachability of the Tor anonymity network through OONI's relevant vanilla tor, was also tested. The HTTP invalid request line and HTTP header field manipulation tests were conducted in an attempt to examine whether systems i.e. middle boxes, that could be responsible for censorship and/or surveillance were present in the tested network.

OONI software tests were run from four local vantage points (AS36866, AS15399, AS33771, AS36914) in Kenya. The initial testing phase ran from 26 July 2016 and concluded on 14th December 2016. Once the testing period ended, the collected data was analyzed with the aim of examining whether access to sites and services was blocked, and whether proxy technologies were present in the tested network. There was no evidence of information controls; only one site appeared to be problematic http://www.sportingbet.com – multiple attempts to establish a TCP connection to this site failed, indicating the possibility of TCP/IP blocking.[89] Subsequently, testing continued until after the elections in October 2018 and there was no evidence of website blocking.

3.1.2 The Case of Middle boxes

Between 6 to 10 February 2017, the data analyzed indicated the presence of a middle box on the cellular network of one provider, Safaricom Limited (AS33771) that had not previously presented any signs of traffic manipulation.[90] Middle boxes assume dual-use character in that they can be used for legitimate functions (e.g., network optimization) and can simultaneously be used for traffic manipulation, surveillance and aiding censorship. In light of such dual uses, CIPIT's policy brief made it clear that service providers operating middle-boxes must communicate to the public in a transparent manner the justification for such activity.[91]

[86] See 'Citizen/Test-lists' GitHub -<https://github.com/citizenlab/test-lists/blob/master/lists/ke.csv> on 6 June 2019.

[87] See 'Citizen/Test-lists' GitHub -<https://github.com/citizenlab/test-lists/blob/master/lists/00-LEGEND-new_category_codes.csv> on 6 June 2019.

[88] See 'Citizen/Test-lists' GitHub -<https://github.com/citizenlab/test-> on 6 June 2019.

[89] Xynou M, Filastò A and Karanja M, 'Kenya: Censorship-free Internet?' -<https://ooni.torproject.org/post/kenya-study/> on 6 June 2019.

[90] Karanja M, 'CIPIT research reveals evidence of Internet traffic tampering in Kenya: The case of Safaricom's network' CIPIT Blog, 23 May 2017 -<https://blog.cipit.org/2017/03/23/cipit-research-reveals-evidence-of-Internet-traffic-tampering-in-kenya-the-case-of-safaricoms-network/> on 6 June 2019.

[91] Karanja M, 'Kenyan elections and alleged hacking: A look at the available evidence' CIPIT Blog, 18 August 2017 -< https://blog.cipit.org/2017/08/18/kenyan-elections-and-

3.1.3 Hacking attempts

During the 2017 elections period, there were multiple hacking attempts of the election commission's website, while the opposition claimed the electoral results were hacked, leading to the opposition candidate's loss. None of the hacking claims were substantiated. The mysterious sudden death of the electoral commission's IT manager, Chris Msando, days before the August elections did little to dispel concerns about the security and integrity of the electoral polling systems. CIPIT investigated the hacking claims but was not able to substantiate the claim.

3.2 Was the Internet Throttled?

On the eve of the fresh presidential elections in Kenya, Internet users reported slow Internet speeds while accessing social media and streaming platforms.[92] Network performance fluctuates, especially when more subscribers come online, for example during major events. That ISPs have the capability to discretely throttle their users' bandwidth is no secret, justified as de-congesting the network or for pressing clients towards more expensive plans, a major contention of the net neutrality principle. Throttling has also been used to control information during political processes. There are documented instances of throttling being used to limit the exchange of multimedia over social media during protests across the world.[93] In Kenya, if the claims made on the eve of elections were to be confirmed, they would amount to limitations of freedom of speech online, a right entrenched in Article 33 of the Constitution.

CIPIT investigated these allegations in the following way: we ran the NDT which are designed to measure the speed and performance of networks by connecting to M-Lab servers close to the user, and by subsequently uploading and downloading random data. In doing so, NDT collects TCP/IP low level information that is useful for examining and characterizing the quality of the network path between the user and the M-Lab server. The results showed inconsistencies in the upload and download speeds compared to those advertised by the service providers, which can be interpreted as signs of throttling on the network.[94] However, a sufficient methodology does not yet exist to determine this effectively. The results may have been influenced by network congestion and other infrastructure-related factors. Also, there are unconfirmed reports of throttling targeting individuals' devices and not the public in general. CIPIT therefore urges ISPs to publish their capping and throttling practices at a sufficient level of detail in order to differentiate themselves.

3.2.1 Traditional media Shutdown

The Kenyan 2007/08 post-election violence report drew a cause-effect relationship between the media blackout that was declared by the incumbent government during the votes tallying stage of the election and the immediate violence that rocked the country.[95] The information vacuum that was seen as a trigger to the spontaneous violence that led to

alleged-hacking/> on 6 June 2019.

[92] See -*<https://twitter.com/kenyanpundit/status/923217714281361409>* on 27 October 2017. For example, this tweet with experiences of Internet connection speed.

[93] See for example 'Freedom on the net 2016: Silencing the messenger: Communications apps under pressure' *< https://freedomhouse.org/report/freedom-net/freedom-net-2016>* on 27 October 2017 with a focus on Ethiopia, Brazil and Kashmir -

[94] Muthuri R, 'Internet speed throttling surrounding repeat election?' CIPIT Blog, 27 October 2017 -*<https://blog.cipit.org/2017/10/29/Internet-speed-throttling-surrounding-repeat-election/>* on 6 June 2019.

[95] Kenya National Commission of Human Rights, 'On the brink of the precipice: A human rights account of Kenya's Post-2007 election violence' KNCHR, 2008, 32.

the killing of over 1,300 Kenyans. The media landscape has changed tremendously since the 2007 skirmishes, with the Internet penetration increasing from a penetration rate of 9% in December 2007 to 112.7% in September 2017.[96] Internet sources were ranked third after radio and TV as the primary source of news in Kenya while consistently ranked top as the leading source of secondary news.[97] The need to understand the policies guiding this landscape is important.

It is not clear to what extent the events offline may predict the controls online. Indeed, Kenyans voted in two elections without any Internet disruption. The Supreme Court nullified the first election which raised tensions in the country but there was no Internet disruption during that period. During the rerun that took place in October 2017, there were no Internet disruptions. On 31 January 2018, NASA leaders held a swearing in ceremony at Uhuru Park. All media houses that attempted to air the event were shut down for 7 days. The haste in which government rushed to shut down television stations probably shows us the reality that it may not be that hard to shut down the Internet in Kenya. Some speculate that it is because there are not as many people online as compared to those who watch television and listen to radio. There was no legal justification for the media shutdown.

3.2.2 Foreign influence – Cambridge Analytica

It is not clear to what extent external forces may control the Internet. CIPIT's report on the privacy implications of applying biometrics to Kenya's 2017 elections revealed parallels with the political micro-targeting allegedly deployed by Cambridge Analytica in the 2016 US elections and the Brexit leave campaign.[98] In this vein, our study of the online activity in Kenya revealed the use of well-coordinated disinformation campaigns of apocalyptic adverts painting the gloom that would come upon Kenya if Raila were to win the election.[99] This too was an attempt to control the flow of information by providing information that could then be easily shared to influence the election outcome. Interestingly, 175 of the video clips created on the Real Raila Facebook page remain on the Facebook page to date.[100] This shows a misalignment between Facebook's content moderation policies and the hate speech laws in Kenya.

[96] Communications Authority of Kenya, 'First quarter sector statistics report for the financial year 2017/2018, July-September 2017. This figure is controversial: ITU's Measuring the Information Society Report (2017) indicated that the percentage of individuals using the Internet in Kenya was 26%. The main difference in the two methodologies is the definition of who an Internet user is. For ITU an Internet user is one who is actively connected to the Internet while for CA an Internet user is one who is a mobile data subscriber. This is why the two institutions report different values of Internet penetration. However, it should be noted that CA is currently reviewing the methodology for estimating Internet penetration.

[97] 'Ipsos Kenya SPEC poll 17 April 2015' Ipsos Public Affairs, 17 April 2015 -<https://www.slideshare.net/ipsoske/ipsos-kenya-spec-poll-17-april-2015> on 6 June 2019.:

[98] Muthuri R, Monyango F and Karanja W 'Biometric technology, elections, and privacy: Investigating privacy Implications of biometric voter registration In Kenya's 2017 election process' CIPIT, Strathmore Law School, 2018.

[99] 'Kenyans bombarded with fake news in presidential election' Channel 4 News, 26 March 2018-<https://www.youtube.com/watch?v=525TpQNmbA> on 6 June 2019.

[100] 'TheRealRaila' -< https://www.facebook.com/pg/TheRealRaila/videos/?ref=page_internal > on 6 June 2019.

Beyond the admissions of SCL Group's involvement by the Jubilee party in Kenya, the confessions by Cambridge Analytica on the Channel 4 exposé,[101] and the fact that Cambridge Analytica is owned by the SCL group, it is still unknown the extent to which Cambridge Analytica was involved in the Kenyan elections in 2013 and 2017. What we do know is that that there were signs of tactics used in previous elections in which Cambridge Analytica has been involved:

- **Microtargeting:** CIPIT's research on the privacy implications of deploying biometrics in the Kenyan elections shows that, on both sides of the political divide, there was evidence of micro-targeting during the campaigns to increase voter registration and turnout.[102]

- **The attraction of opposites to reinforce stereotypes:** Cambridge Analytica is known to study the politics of a certain jurisdiction and then apply stylistics and social cognition tools to reinforce existing stereotypes. This consists of promoting dual messaging that exploits false dichotomies such as pro-Trump and anti-Clinton messages or pro-leave EU and anti-remain messaging.[103] In Kenya this took the form of two contrasting websites, 1) TheRealRaila[104] and 2) UhuruforUs,[105] with the former (Raila Odinga) portrayed as totally unreliable so the latter (Uhuru Kenyatta) could look better for it. These two sites, TheRealRaila and UhuruforUs, shared the same Google Analytics Tracking Code with HarrisMedia LLC. HarrisMedia LLC, is a Texas company known for building hate speech websites; its previous clients include the Trump campaign and several far-right European parties.[106] Cambridge Analytica has admitted to using front companies and HarrisMedia could very well have been one such entity.

- **Sowing division through disinformation and hate speech:** The apocalyptic depiction from a video in TheRealRaila site is similar to an ad from the Nigerian presidential race of 2015. In that earlier ad, the prospect of Buhari becoming the Nigerian president was depicted as 'a dark, scary and very uncertain, Sharia for all"[107]. Both the anti-Buhari ad and TheRealRaila video are carefully scripted ads betraying the same use of an array of ad hominem and strawman fallacies to demonize their subject characters. This is highly unethical. In the Channel 4 News exposé, Cambridge Analytica admitted to working in Nigeria.

[101] 'Cambridge analytica uncovered: Secret filming reveals election tricks' Channel 4 News, 26 March 2018 -<https://www.youtube.com/watch?v=mpbeOCKZFfQ > on 6 June 2019.

[102] Muthuri R, Monyango F and Karanja W 'Biometric technology, elections, and privacy: Investigating privacy Implications of biometric voter registration In Kenya's 2017 election process' CIPIT, Strathmore Law School, 2018.

[103] 'Cambridge analytica: Undercover secrets of Trump's data firm' Channel 4 News, , -<https://www.youtube.com/watch?v=cy-9iciNF1A> on 6 June 2019.

[104] See -<http://www.therealraila.com> on 7 June 2019.

[105] See -< http://www.uhuruforus.com> on 7 June 2019.

[106] 'Texas media company hired by Trump created Kenyan president's viral 'anonymous' attack campaign against rival, new investigation reveals' Privacy International, 15 February 2017 -< https://privacyinternational.org/long-read/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack> on 7 June 2019.

[107] 'How Cambridge analytica tried to intimidate Nigerian voters' Channel 4 News, 4 April 2018 -< https://www.youtube.com/watch?v=KOpKkgXNb50> on 7 June 2019.

Below is a visualization of some of the twitter activity on the accounts belonging to Uhuru4Us connecting to 980 nodes and TheRealRaila with 653 nodes. The visualization was done using NodeXL.[108] We've edited out the names of the other nodes to protect their privacy. The following observations were made:

1. **Userbase:** Notably, the twitter users who responded to the tweets from both accounts were similar. This is not what one would expect considering the tensions between the supporter of the two main candidates at the time;
2. **Activity level:** The UhuruforUs account had a wider outreach and more interaction than TheRealRaila tweets. It had a lot of accounts respond to its tweets not only during the election period but also during the periods preceding and after the election.
3. **Most interaction:** There was more interaction between TheRealRaila and The Star Kenya, the social media account of a local daily newspaper. Most of the tweets referred to articles from that newspaper. The UhuruForUs account mainly shared news stories from Kassfm, a local language radio station and other local news stations.
4. **Peak month:** The UhuruForUs account had its most interaction and therefore impact during the month of May 2017. It is during this period that they had their most liked, retweeted and commented on tweets. For TheRealRaila account, the most interactive month was August during the election period, this is when their activity started to truly peak and when they experienced their most interactive tweets.
5. **Privacy:** When we cross-checked the actual accounts on twitter, more users in TheRealRaila than UhuruForUs had activated their privacy settings i.e. requested for their accounts note to be displayed;
6. **Active users:** The most active users were engaging both UhuruForUs and RealRaila during the study period, which would be necessary to Cambridge Analytica's tactic above on using the attraction of opposites to reinforce stereotypes.
7. **Engagement:** There was more engagement between the accounts interacting with the UhuruForUs account than TheRealRaila account. For UhuruforUs there were more replies not only to the main tweets but also to the subsequent replies of those tweets. For TheRealRaila account, there were mainly retweets and likes and the interaction between the accounts was less as compared to the UhuruForUs.
8. **Diversity:** UhuruForUs had a more diverse interaction with users on the platform i.e. there were more new accounts interacting with their tweets in comparison with TheRealRaila account. Most of the interactions with the RealRaila tweets were from accounts that were already engaging with them.
9. **Self-interaction:** There was more self-interaction with TheRealRaila account tweets than with the UhuruForUs tweets. This means that many people who commented on the RealRaila account tweets as well as TheRealRaila account itself were liking and retweeting their own tweets.
10. **Hashtags:** These two accounts were responsible for the generation of the most popular hashtags during the election period.

[108] NodeXL, 'Your social network analysis tool for social media' Social Media Research Foundation -*< https://www.smrfoundation.org/nodexl/> on 7 June 2019.*

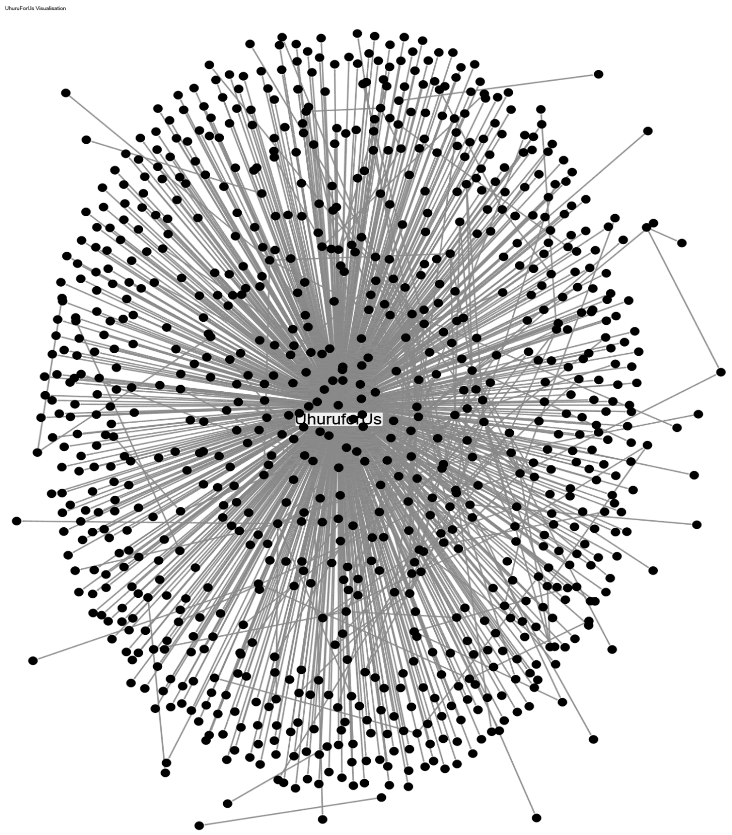


Figure 1: The UhuruForUs Twitter Account Activity Visualization

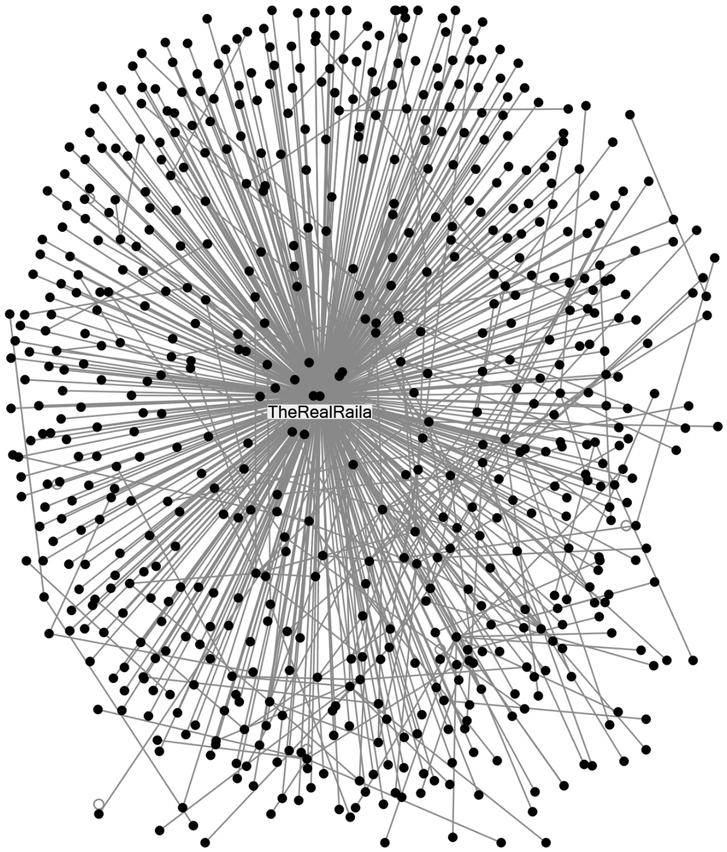
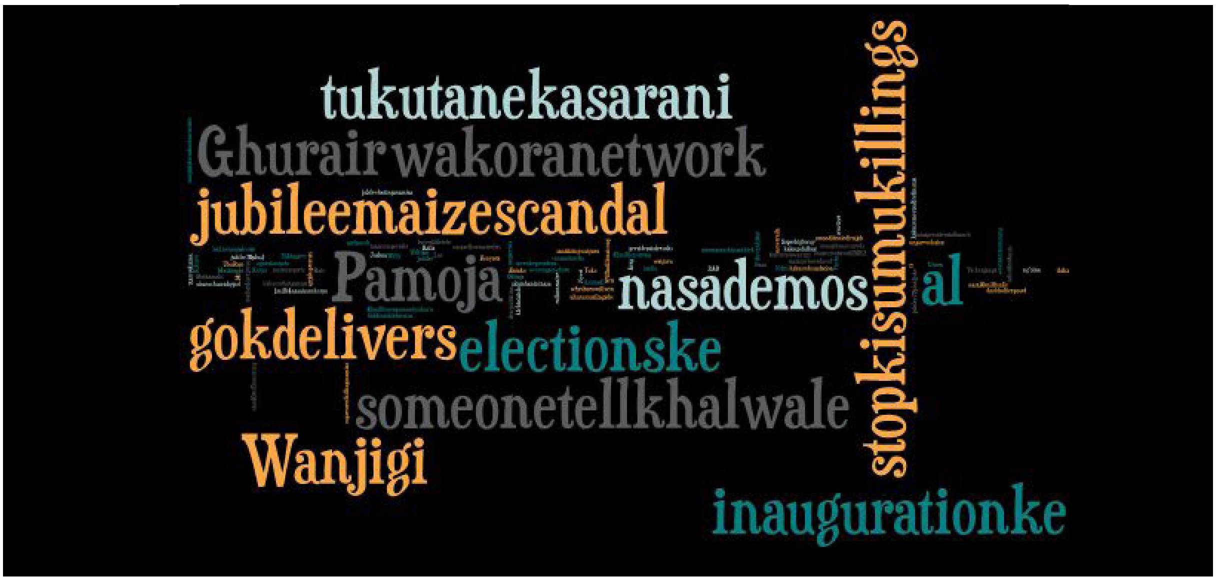


Figure 2: The RealRaila Twitter Account Activity Visualization



The foregoing visualizations are only indicative of the activity that went on various social media accounts. For a proper analysis to be undertaken, these platforms need to release the data so that researchers can study the effect and impact of both disinformation and foreign interference on elections. Social Science One is a partnership of academic partners pursuing this goal. In April 2018, it launched a project jointly with Facebook on 'the effects of social media on democracy and elections', to offer researchers privacy-preserving access to Facebook's data.[109] We call on funding organizations to pursue and promote similar initiatives.

Cambridge Analytica's admission to working with proxies to inject certain messages into the Internet ecosystem, overlapped significantly with Russia's role in promoting certain messages, particularly divisive messages in the US 2016 elections.[110] Facebook found messages from Russian linked accounts reached some 126 million Americans while purporting to be from activists and civil society.[111] Special Counsel Robert Mueller, the lead investigator for the FBI found evidence of Russian interference in the US election.[112] 13 Russian nationals and 3 Russian entities were indicted including the Internet Research Agency (IRA) with violating US criminal laws in order to interfere with the US elections and political processes.[113] One US national was also charged for his role in supplying false or stolen back account numbers that allowed the IRA conspirators to access US online payment systems by circumventing those systems' security features.[114] A similar investigation ought to be conducted in Kenya with regard to Cambridge Analytica's interference with the electoral process and the law reformed accordingly.

[109] 'Social science one: Building industry-academic partnerships, Social Science One -<https://socialscience.one/> on 6 June 2019.

[110] 'Cambridge analytica: Undercover secrets of Trump's data firm' Channel 4 News, , -<https://www.youtube.com/watch?v=cy-9iciNF1A> on 6 June 2019

[111] 'Cambridge analytica: Undercover secrets of Trump's data firm' Channel 4 News, , -<https://www.youtube.com/watch?v=cy-9iciNF1A> on 6 June 2019.

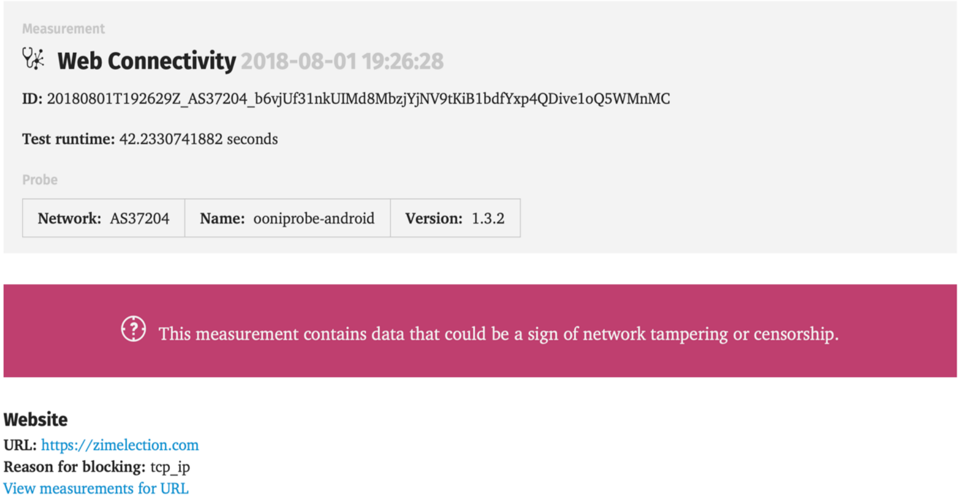
[112] Muller R, The Mueller report: The final report of the special counsel into Donald Trump, Russia, and collusion, Skyhorse Publishing, Inc, New York, 2019.

[113] See Muller R, The Mueller report: The final report of the special counsel into Donald Trump, Russia, and collusion, Skyhorse Publishing, Inc, New York, 2019, 174.

[114] Muller R, *The Mueller report: The final report of the special counsel into Donald Trump, Russia,* and collusion, Skyhorse Publishing, Inc, New York, 2019, 175.

3.3 Zimbabwe's 2017 elections

There was significant tension on whether Zimbabwe would shut down the elections during the July 2018 elections given the government had previously shutdown the Internet two years before in 2016.[115] However, that was a different regime so there was reason for optimism this time round. Indeed, there was no apparent shutdown in the run-up to the election. Even then, OONI data showed the TCP/IP blocking of zimelection.com,[116] an elections information and education website based in the UK.



Measurement

Web Connectivity 2018-08-01 19:26:28

ID: 20180801T192629Z_AS37204_b6vjUf31nkUIMd8MbzjYjNV9tKiB1bdfYxp4QDive1oQ5WMnMC

Test runtime: 42.2330741882 seconds

Probe

Network: AS37204	**Name:** ooniprobe-android	**Version:** 1.3.2

This measurement contains data that could be a sign of network tampering or censorship.

Website
URL: https://zimelection.com
Reason for blocking: tcp_ip
View measurements for URL

Figure 4: OONI'S Web Connectivity Test on zimelection.com

This blocking happened on TelOne, a state-owned ISP although OONI data was available in other Zimbabwean networks.[117] In another case, APC reported that the site of the Zimbabwe Electoral Commission (ZEC),[118] which is hosted on a .zw domain, showed a '404 Not Found' error in the days following the elections although it was subsequently restored.[119] This could be due to content removal, a domain takeover, or technical issues triggered, for example, by too much traffic towards the website or some malicious activity such as hacking.[120] A report by Qurium confirmed that the electoral commission's site was defaced on the evening of the 1 August 2018 and the attack was claimed by the twitter account '@ zim4thewin'.[121] This is a digital activist that was protesting the military actions during the riots that followed the announcement of election results in Zimbabwe. The same activist claimed the Denial of Service attack against the South African Broadcasting Corporation in 2016 to protest the filming of violent protests.[122]

[115] Bearak M, 'Shut down Zimbabwe' protests are met with Internet blackouts and arrests' The Washington Post. 2016, 6 July 2016 -*< https://www.washingtonpost.com/news/worldviews/wp/2016/07/06/shut-down-zimbabwe-protests-are-met-with-Internet-blackouts-and-arrests/?noredirect=on&utm_term=.0abf19c701e1>* on 7 June 2019.

[116] 'Zimbabwe election 2018' *-<https://zimelection.com>* on 7 June 2019.

[117] 'Digital society of Zimbabwe' -*< http://www.dszim.org/2018/08/10/zimbabwean-election-website-blocked-following-2018-general-elections/>* on 7 June 2019.

[118] Zimbabwe electoral commission' -*< https://www.zec.org.zw/> on 7 June 2019.*

[119] Majama K, 'Zimbabwe: 2018 general elections website blocked' Association for Progressive Communications, 14 August 2018 -*<https://www.apc.org/en/blog/zimbabwe-2018-general-elections-website-blocked>* on 7 June 2019.

[120] on 7 June 2019.

[121] 'The cyberattack against the Zimbabwe electoral commission' Qurium Media Foundation -*<https://www.qurium.org/alerts/zimbabwe/the-cyberattack-against-the-zimbabwe-electoral-commission/>* on 6 June 2019.

[122] 'The cyberattack against the Zimbabwe electoral commission' Qurium Media Foundation -*<https://www.qurium.org/alerts/zimbabwe/the-cyberattack-against-the-zimbabwe-electoral-commission/>* on 6 June 2019.

3.3.1 Verifiability and Auditability of the Voters' roll

The Zimbabwean opposition Movement for Democratic Alliance filed a petition challenging the 31 July presidential election results on the ground that the election was marred with irregularities that warranted the setting aside of the results. In a unanimous determination delivered by the Constitutional court following the opposition petition, in Chamisa v Mnangagwa & 24 Others,[123] the court stated that the evidence submitted was not sufficient to convince the court that the 30 July 2018 election was marred with irregularities that warranted the setting aside of the results. The opposition should have provided primary evidence the contents of the ballot boxes and primary evidence to prove its case. It should have sought to obtain evidence from the election residue (primary paper trail).

The period leading to, during and after the elections was characterized by a series of information controls relating to data either in transit, rest or in storage on the election management body servers including on the cloud. Through its Zimbabwe-based researcher working in collaboration with activists and international data science projects such as OONI and Virtual Road, CIPIT produced the following analyses which shed light to the information controls.

CIPIT had done an analysis[124] that examined election security ahead of the election and argued that a credible election requires a verifiable and auditable paper trail to evidence that every vote counted, and the election result was accurate. The paper trail must ensure that every final recorded and counted vote is easily traceable back to the polling booth. In the event of inaccuracies, such paper trail provides the basis for a remedy.

The above analysis was followed by another[125] that examined data-related breaches ahead of the election, some of which the electoral commission admitted. The breaches posed a significant threat to privacy, expression and political participation. While two of the cases involved an alleged interference with data stored and at rest in the election commission's servers, the other case concerned the 'black boxing' of the ballot paper's security features. The paper called for a revised cyber threat modeling based on revised indicators that would take into account a wide range of adversaries that potentially exploit vulnerabilities in decentralized technologies and also in data regardless of medium or whether such data is in transit, cloud, storage or at rest.

3.3.2 Impact of the cyber-attacks on democratic processes

The various data breaches ahead of the election had an impact on the outcome of the election court petition which was dismissed mainly on the ground that the opposition should have sought to obtain evidence from the election residue (primary paper trail).

The Independent Newspaper subsequently reported that the opposition lawyers had sought a court order compelling ZEC to bring (all) material on its servers and on the same day the Registrar of the Constitutional Court wrote back to opposition lawyers advising them that the court could not accept the subpoena. From this, it would appear the opposition, apparently, tried to access the source material but were denied by the court itself.

[123] 2018) ZWCC

[124] Gwagwa A, 'Verifiability and trust: Two key ingredients to a credible election in Zimbabwe' Medium -< *https://medium.com/@arthurgwagwa/verifiability-and-trust-two-key-ingredients-to-a-credible-election-in-zimbabwe-60b7f255b53f* > on 7 June 2019.

[125] Gwagwa A, 'Dynamic data obfuscation ahead of Zimbabwe's elections' Medium -<*https://medium.com/@arthurgwagwa/dynamic-data-obfuscation-ahead-of-zimbabwes-elections-6d223e9676b8*> on 7 June 2019.

However, what is not clear is the extent to which source material from the servers could have swayed the decision in favor of the applicant. It is also not clear whether ZEC's servers were up and running after the second hack. Nevertheless, what is clear is that access to information and denial and/or failure to access key information played a role in the election itself and the court challenge outcome but a direct impact on the outcome remains speculative and tenuous at best. However, commenting on this issue, David Coltart an opposition leader said, 'Access to the server was critical because it would have exposed differences between the input data and what they finally released. It would certainly have been a lot quicker than opening up 33,000 boxes to look at 4 million ballots'.

3.4 Conclusion

Internet censorship has been measured in both Kenya and Zimbabwe since 2016. There was no form of Internet control or disruption that took place in Kenya during the 8 August election period or the 26 October re-run period. CIPIT's 2016 policy brief reported that that there were no websites that were blocked in Kenya. However, an interview with Safaricom reveals that some websites have been blocked using globally acceptable standards. These websites include sites with child sex content among others although the actual standards upon which this is done were not shared with CIPIT. We should also highlight that it proved challenging to secure interviews with most legal or technical officers shying away from engaging with us possibly from fear of being quoted or otherwise put on the record. There was also no outright shutdown in Zimbabwe, but the electoral site was defaced by an individual and zimelections.com was blocked by a government owned Telcom provider. There was no justification given for this from a policy or legal perspective. We would therefore be unable to conclude that there currently exists any correlation between the existing legal and policy frameworks with the resulting controls on the flow of information. The reverse ought to be the case, i.e. a proper justification ought to be given before any control on the flow of information is exerted by any entity be it an individual, civil society organization, private organization or a government.

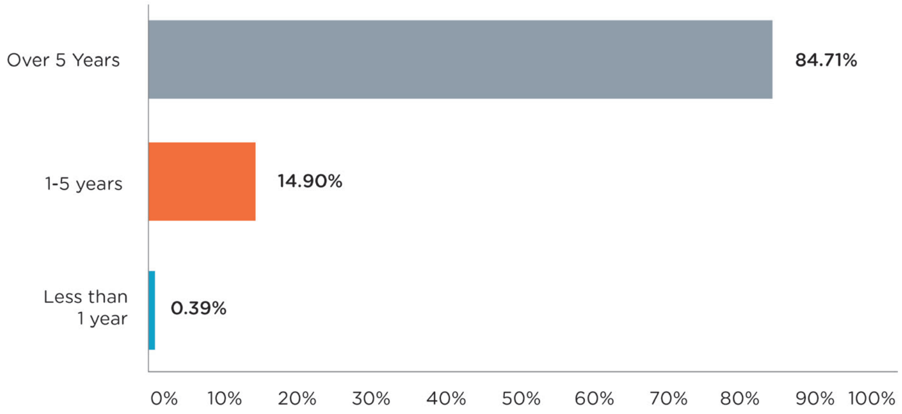
4. SHOULD WE PREVENT INFORMATION CONTROLS IN ELECTORAL PROCESSES?

To determine the attitudes and responses to incidences during the period under study, CIPIT conducted a survey on the state of Kenya's Internet during the 2017 elections. The main object was to understand if accessibility to the internet in Kenya was in any way impacted by the 2017 elections. The survey had 13 questions and involved 255 responses from students attending Strathmore University in the period under study.

4.1.1 A Survey of perceptions in Kenya

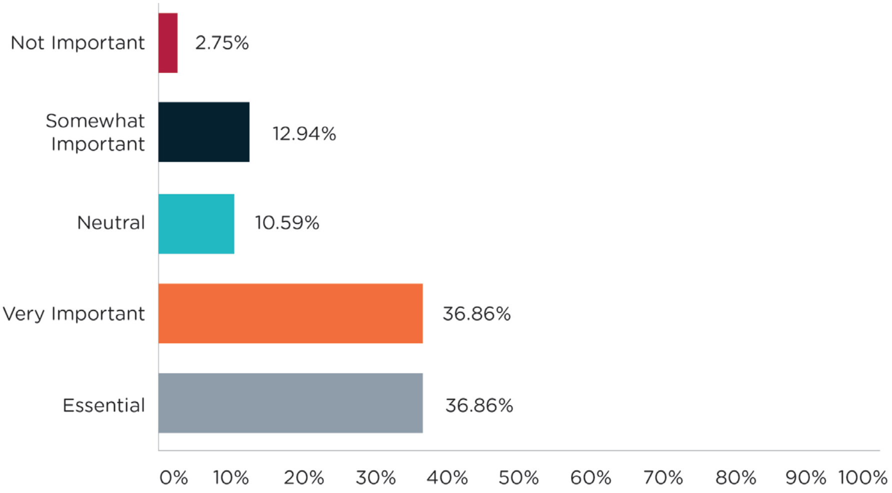
How did Kenyans respond on their ability to participate in the electoral process through access and sharing of information?

Q1: How long have you had Internet access?



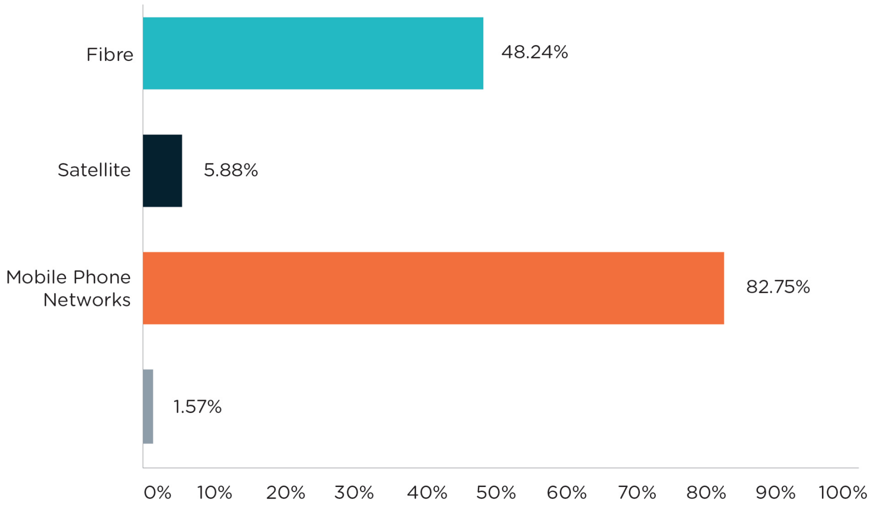
It is clear that a good majority of the respondents have had Internet access for over 5 years and almost all of them had Internet in the period leading to the election. This shows a high rate of Internet access leading up to the election period.

Q2: How would you rate the role of the internet in helping you access, publish or share information during the 2017 election period?



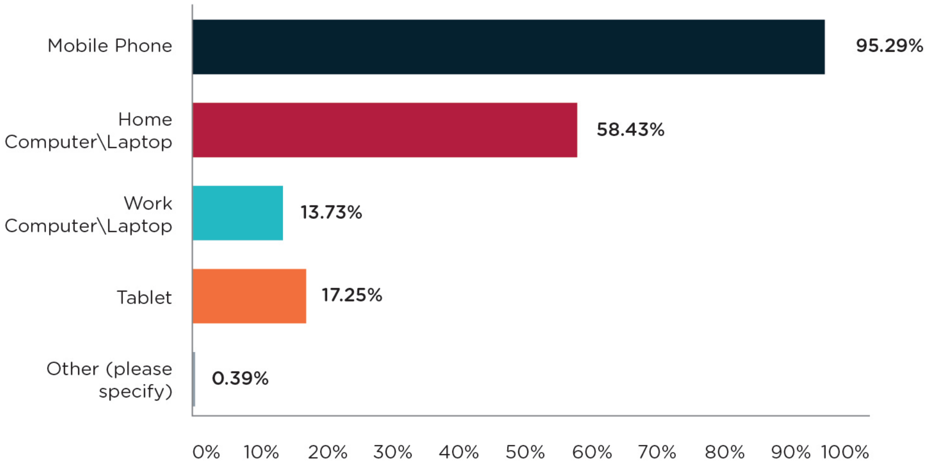
A total majority of 74% therefore find that the Internet played an important role in helping them to engage in and receive information on the 2017 elections. Compared to the much higher percentage of persons who had Internet access, about 26% of them did not consider it a vital mode of sharing and receiving information.

Q3: How did you access the internet before, during and after the election period in 2017?



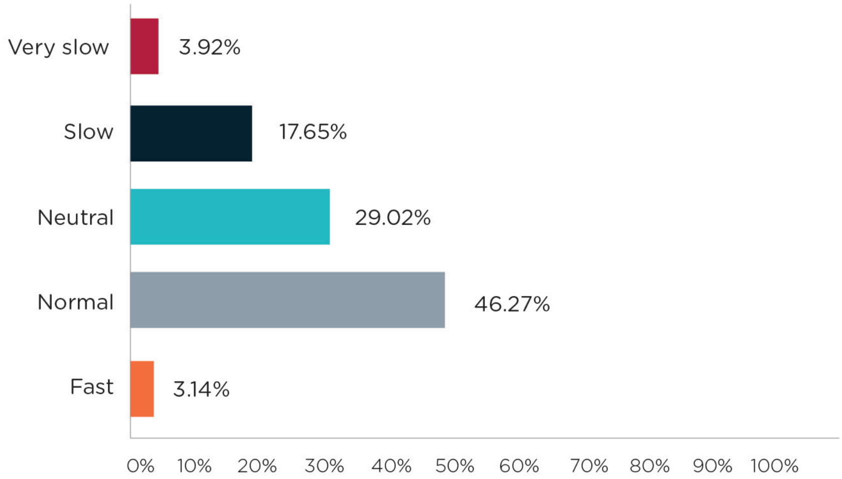
83% of the respondents used Mobile Phone Networks in accessing the Internet before, during and after the 2017 election period. Almost half of the respondents accessed the through fiber and a paltry 7% used satellite and landline respectively.

Q4: Which device(s) did you primarily use to access the Internet during this period?



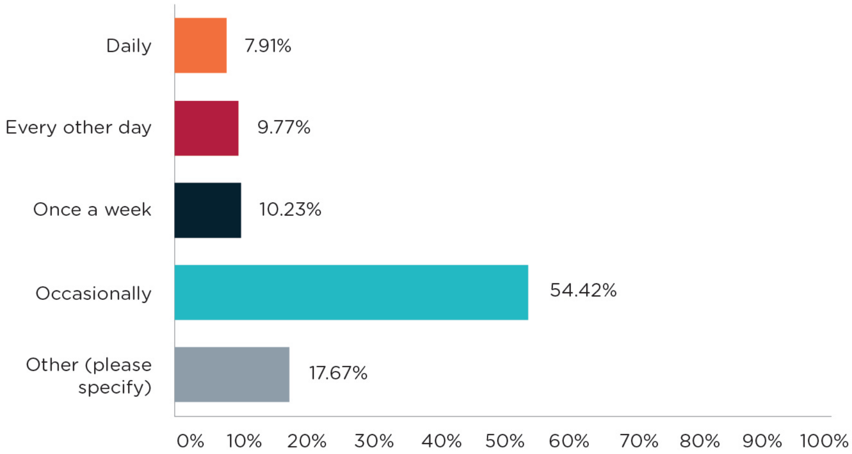
Mobile phones were the main devices used by Kenyans to access the Internet during the election period. Personal computers were also in prominent use. More tablets were used than work computers. This shows that Kenyans preferred personal devices in accessing the Internet during the election period over work devices.

Q5: How would you describe Internet speed during the election period in 2017?



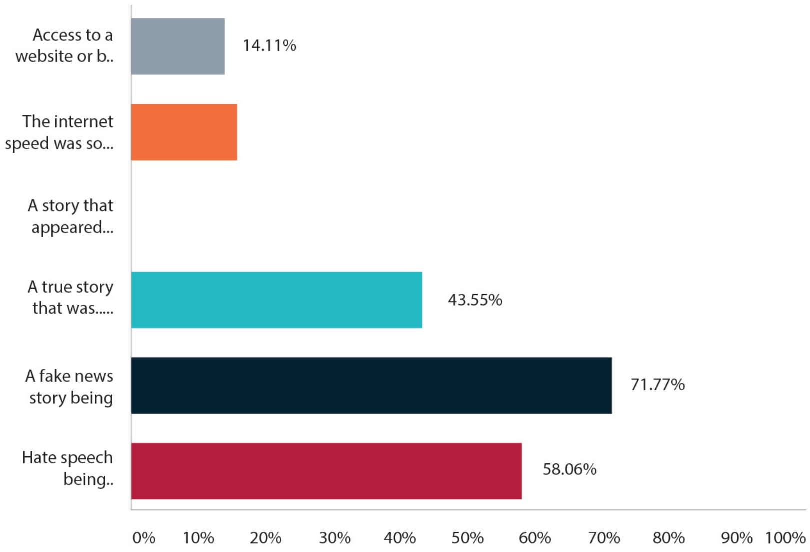
About a fifth of the respondents found the internet slower than usual during the election period. Almost half (46%) found it normal, with a small percentage even finding it faster than usual. This finding does not support the allegations on throttling of Internet speeds during the elections.

Q6: If slow or very slow, how often did you experience such speeds?



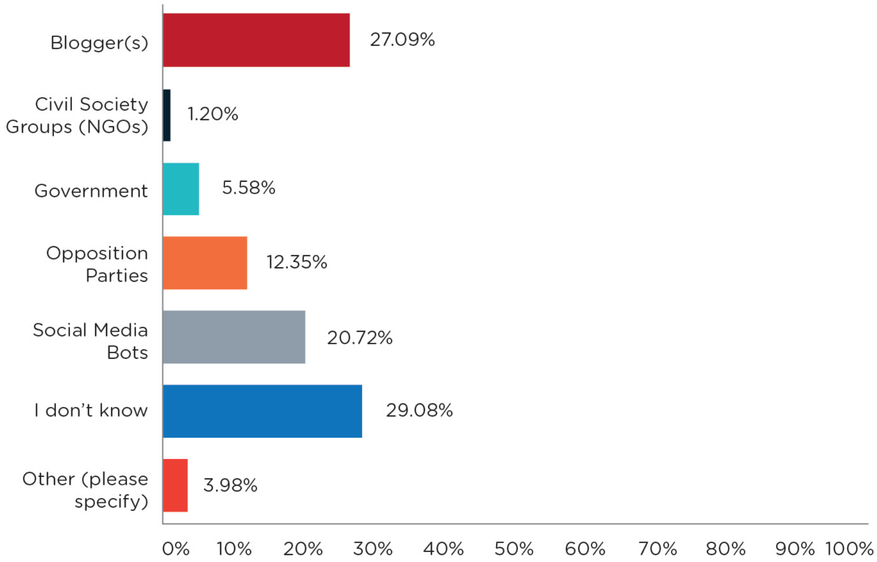
28% of the respondents who experienced slower Internet speeds during the election period experienced the slower speeds at least once a week; with some experiencing them daily. Most of the respondents who experienced slower speeds however, experienced them only occasionally. The cause of the disparity in Internet speeds for different users during the election period is not clear but should be addressed as it affects the user experience, with some users being consistently connected and able to share and receive information during the democratic process while others are sporadically and inexplicably locked out.

Q7: Did you notice or experience any of the following problems during the 2017 elections period?



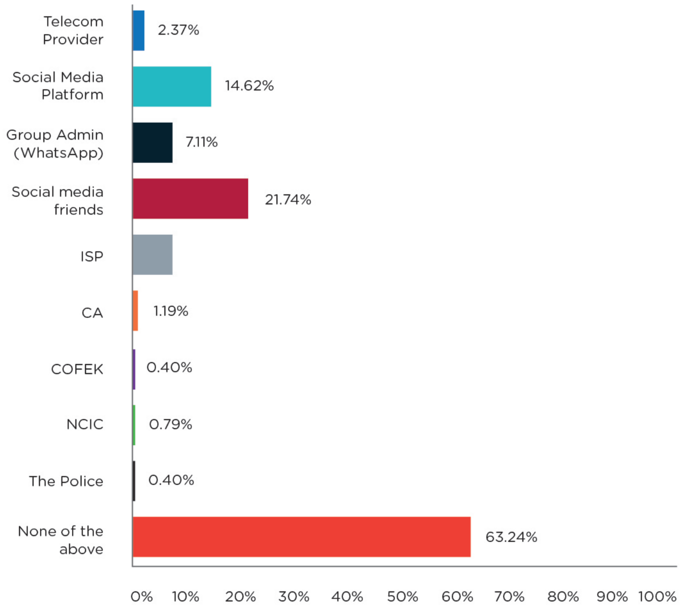
71.77% had encountered a fake news story being circulated on social media. 58.06% had encountered hate speech being circulated on social media. Censorship levels were generally lower than instances of fake news and hate speech. However, the high levels of fake news and hate speech online indicate a need to address the two categories of expression, while still upholding citizens' right to free discussion of issues during the election period. It is notable that the election period under study came before the enactment of the Computer Misuse and Cybercrimes Act, which criminalizes fake news and hate speech online.

Q8: Who were these fake news stories/hate speeches from?



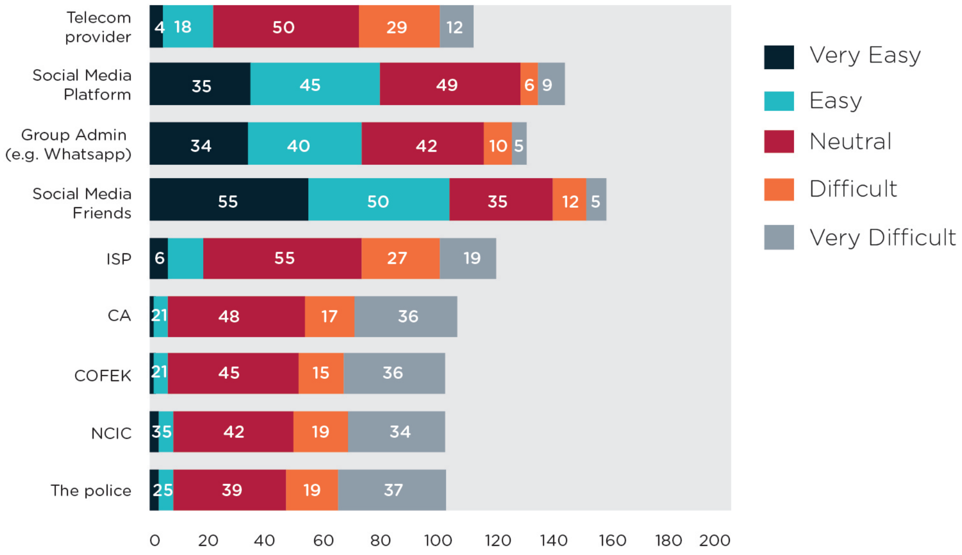
Kenyans perceived fake news and hate speech stories during the election period to have had a wide range of sources. Unknown sources were prevalent, a testament to the anonymity that the internet can provide to users. Bloggers were also a significant source of fake news stories and hate speech. Both sides of the political divide seem to have participated in spreading fake news stories and hate speech. The respondents also noted that social media users from the general public also disseminated these stories.

Q9: Did you report your experience to any of the following?

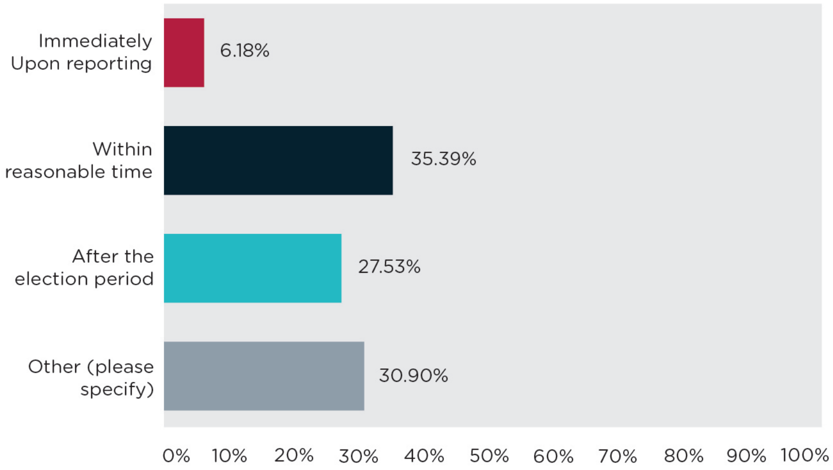


There was very little reporting of incidents: A significant number of respondents (63%) did not report the incidences experienced to any authorities. A fifth of them shared the stories with their friends which is reflective of the viral nature of this phenomenon. About a sixth (15%) reported to their respective social media platforms.

Q10: What was the ease of reporting your experience to any of the parties in question 9 above?



This graph shows that generally, it was difficult to report incidents to the different authorities. However, it was more difficult to report to the police, the national cohesion and Integration Commission, COFEK and CA. It was easier for respondents to report directly to group admins e.g. on WhatsApp and social media.



Only 7% of the respondents had their issue resolved immediately. About a third (35%) had the issue was resolved within reasonable time while another third (28%) had issue had been resolved after the election period. The final third (31%) of the respondents had varying experiences, there was no eventual resolution, or the agency did not even give an initial response.

Conclusion

Were Kenyans able to participate in the electoral process through accessing and sharing information online?

Majority of Kenyans had access to the Internet, with mobile phones and mobile phone networks providing Internet access for many people. However, there were challenges to this access which interfered with some citizens' ability to participate in the electoral process through online discussions. The instances of slower speeds experienced by some respondents, sometimes barely allowing the user to browse, show that some people were on occasion unable to access and share information online. There were also some blocked websites and blogs, indicative of censorship whose legitimacy is not clear.

Fake news stories and hate speech were rampant and from multiple sources. These two categories affect the participation of citizens in the democratic process as they involve information that has been distorted for the benefit of a few; but with serious ramifications on the population. Kenya has been prone to violence precipitated by hate speech and fake news during election periods. Despite this, there seems to be little confidence in the various agencies to address these issues. This is buttressed by the difficulty faced by those who reported fake news stories and hate speech to the agencies. There also arose a strong fact-checking community with a number of institutions now investing in civic tech and other initiatives to improve the verification of information online such as Africa Check in based in Kenya, Nigeria , Senegal, South Africa and the UK, Zimfact in Zimbabwe Pesa Check in Kenya and Dubawa in Nigeria. In a similar vein, BBC Africa have also begun a weekly program called Factfinder to analyze fake news on the continent; they show how journalists put the story together.

The survey results have also revealed several insights. We have been able to confirm that majority of our respondents considered the Internet as very important or even essential in helping them access, publish or share information during the 2017 elections period. Most of them did so on their mobile phones. However, only a fifth of the respondents thought the Internet was occasionally slow during this period. On the other hand, majority of the respondents experienced fake news and hate speech during the elections period with the most attribution going to bloggers and social media bots. A third of the respondents did not know who was publishing this information. Most of the respondents did not report these incidences, which may be indicative of apathy or helplessness as to where to report the matter. We therefore recommend a stronger policy framework to ensure an effective reporting mechanism within the telecom ecosystem.

5. HOW CAN WE MITIGATE THE IMPACT OF INFORMATION CONTROLS DURING FUTURE ELECTIONS?

As we have seen, governments are warier of controlling the Internet particularly where there have been continued investments to integrate the Internet in the economy. Nevertheless, they will not hesitate to interrupt the Internet when it serves their best interests. This is evident in the case of Zimbabwe which did not shutdown the Internet following the post-election protests but did so following the protests against rising fuel prices. Several efforts can be applied to mitigate the impact of information controls on today's cyberspace. Besides policy recommendations, CIPIT has worked to begin to define the scope of five digital rights that will be included in a handbook on Internet freedoms. These rights are:

a) **The digital right to privacy:** A digital right to privacy will be assured where the data subject can determine: a) who can collect their data, b) what data is collected, c) what data is not collected, and d) the nature of consent required to collect certain kinds of data. This criterion derives from the legal doctrine of the right to informational self-determination in respect of right to privacy. It is the right of a person to determine the disclosure, and the use of their personal data. The doctrine is in line with Westin's definition of the right to privacy which he succinctly defines as 'the right of the individual to decide what information about himself should be communicated to others and under what circumstances'.

b) **The right to assembly:** Online assembly refers to the gathering of people on virtual platforms in groups so as to express their views and at times for the purpose of criticizing the government. The nature of online assemblies is unique as it involves the sharing of information across a digital platform in order to mobilize Internet users to take part in virtual protests. As such, online assembly has various elements unique to it: the online platform, the role access of information plays, and the viral effect brought about by the network.

c) **The right to associate:** As the right to voluntarily join with others through collective action based on a common purpose through the use of modern communication technology without interference. Perhaps an interpretational challenge in defining the subject right also owes to its confusion with the related freedom of assembly. Freedom of assembly secures the right of people to meet for any purpose connected with government whereas associational freedom protects the activities and composition of such meetings.

d) **The right to speech:** This is the freedom to express a factual representation or opinion on an online platform. The right precludes the following: defamatory statements, hate speech, cyber-bullying, or misrepresentations. The custodians of the right include the government and at initial phases, administrators of online platforms. These custodians are obliged to respond expeditiously to any reports of illegal activity or activity flouting platform policies.

e) **The right to access:** The freedom or right to access refers to the right for all citizens of a country to access the communication networks that connect their devices onto the Internet. This is a facilitative right that allows such citizens to then exercise the foregoing rights to assemble, associate, express and remain private and secure online.

6. CONCLUSION

Documenting this research helped us document and understand the explicit forms of Internet control. OONI's methodology allowed us to conduct network measurements to find out whether a certain number of websites were blocked. We however found it difficult to use this methodology to measure other forms of information controls such as Internet throttling. We are contributing towards OONI developers' efforts to develop a more robust tool. Even then, a significant impact of this research was to raise further research questions key among them being, how to measure the subtle forms of Information Controls such as Internet throttling and particularly how to distinguish business-driven throttling from censorship-driven throttling., This is the main question to be explored in future work to bring forth a deeper understanding of covert forms of information controls in the African region during political processes and how this affects public policy on elections and freedom of expression and human rights in general.

7. RECOMMENDATIONS

We now conclude the report by reiterating the main findings followed by the subsequent recommendations for each finding.

Key Learnings

A) **There were no Internet shutdowns in Kenya and Zimbabwe in the electioneering period – we applaud the governments for defying the growing trend by African governments to shut down the Internet during elections:** There was no express shutdown of the Internet during the electioneering period in the countries under study. We were however not able to verify other alleged forms of control including throttling Internet connection speed and targeted localized and timed electricity supply disruption in restive zones. The collective experience while monitoring the Internet in Kenya and Zimbabwe during the elections shows that, as the Internet is integrated deeper into the economy, governments are wary to disrupt it. This is a rational decision based on anticipated losses, both political and economic. This was evident in Kenya, which did not explicitly shut down the Internet despite a contested general election and repeat election. Zimbabwe's Internet was considerably stable in the run up to the election on 30 July 2018. However, the resulting challenge of the electoral results led to the suspension of the electoral management body's website. Notably, this was control exerted by a private entity with the twitter account @ zim4thewin a digital activist that was protesting the military actions during the riots that followed the announcement of election results in Zimbabwe. In January 2019, Zimbabwe shutdown all Internet services following protests against a Government announcement that it would double fuel prices in that country. The shutdown occurred between 14 and 21 January 2019.

B) **There is a need for broader definitions of information controls beyond technical controls:** Information controls online cannot be understood adequately without bringing in their relationship with traditional media (television and radio). Internet penetration and usage is significantly below that of television and radio, and as such government controls may target such media over the Internet. While Kenya did not shutdown the Internet, they eventually shut down four mainstream media channels for 7 days. Also, in the aftermath of the 2017 elections, Kenya passed The Computer Misuse and Cybercrimes Act which represented the Kenyan parliament's fourth attempt to criminalize libel. The Bloggers Association of Kenya challenged the constitutionality of this Act in in the case of *Bloggers Association of Kenya (BAKE) v Attorney General & 5 others.* Subsequently, 26 sections of the Act are currently suspended pending the full hearing and determination of the case.

C) **Internet integration is likely to determine the nature and level of information control:** Information controls online cannot be understood adequately without bringing in their relationship with traditional media (television and radio). Internet penetration and usage is significantly below that of television and radio, and as such government controls may target such media over the Internet. While Kenya did not shutdown the Internet, they eventually shut down four mainstream media channels for 7 days. Also, in the aftermath of the 2017 elections, Kenya passed The Computer Misuse and Cybercrimes Act which represented the Kenyan parliament's fourth attempt to criminalize libel. The Bloggers Association of Kenya challenged the constitutionality of this Act in in the case of *Bloggers Association of Kenya (BAKE) v Attorney General & 5 others* [2018] eKLR. Subsequently, 26 sections of the Act are currently suspended pending the full hearing and determination of the case.

D) **Other actors besides government can exert information controls:** This report maps the actors concerned with Information Controls. Interview questions were conceptualized, and the research team interviewed the relevant officers. Besides the finding that no websites were blocked in Kenya during the elections, ISPs acknowledged that they block some websites using globally acceptable standards. Such websites include sites with child pornography content among others. These standards were, however, not provided and further research is needed to establish the nature of such standards. We should also highlight that it has proven challenging to secure interviews with most of the relevant legal or technical officers; it is likely that such individuals are shying away from engaging, possibly from fear of being quoted or otherwise put on record.

E) **Elections manipulation and foreign interference, a rising form of control:** Dis- and mis-information during the elections was the most used form of information control according to our observations. The project did not originally identify this area of focus, but it soon became clear that it may be the preferred option by political actors to control narratives during political campaigns. This is now a global phenomenon: particularly, Cambridge Analytica was alleged to have attempted to control narratives in Kenya, Nigeria, the Brexit campaigns, and the 2016 US elections. The alleged involvement of Cambridge Analytica in the Kenyan elections raises significant questions on the impact such interference had in that elections. We collected some relevant data from Social Media platforms for exploratory analysis on the possible impact of such control on democratic processes.

F) **Election manipulation seeks to control not access, but the narrative:** Following closely from the previous point E, various actors apart from governments can initiate information controls towards various ends. As Kenyans reflect on the 2017 elections, we continue to witness a lot of attention to fake news and the role of social media in the Kenyan elections. This sort of information control was not designed to deny citizens access to information, but to control narratives online. International media such as Channel 4 interviewed CIPIT in this regard and that research was reported in a number of international media outlets.

G) **Anonymity was crucial for election manipulation to thrive:** From the survey conducted to understand citizens perceptions to information controls, a majority of our respondents considered the Internet as very important or even essential in helping them access, publish or share information during the 2017 elections period. Most of them did so on their mobile phones. However, only a fifth of the respondents thought the Internet was occasionally slow during this period. On the other hand, a majority of the respondents experienced fake news and hate speech during the elections period with the most attribution going to bloggers and social media bots. A third of the respondents did not know who was publishing this information. Most of the respondents did not report these incidences, which may be indicative of apathy or helplessness as to where to report such matters.

Key Messages (Recommendations)

A) **More technical resources need to be channeled towards studying subtle forms of information control:** CIPIT lauds the Kenyan and Zimbabwean governments for not implementing a complete shutdown of the Internet in the run up to and during their respective elections. That said, it was challenging to verify reports of more subtle forms of control such as the deliberate throttling of Internet speeds and targeted localized and timed electricity supply disruption in restive zones. Current evidence gathering methods cannot distinguish such observations from legitimate network management behavior. We call on the research community to build robust methodologies that can differentiate business-driven throttling from censorship-driven throttling.

B) **More research resources need to be dedicated to studying the information controls ecosystem:** Broader definitions help define the information control ecosystem, which will be more illuminating than individual studies of technical, regulatory, economic, social and political controls. This also ties in subject matter areas and attracts the relevant expertise so that African governments can shed the techno-determinism tag and build confidence in their citizenry while advocating for the adoption of proposed systems. A highlight here is the Social Science One initiative which has partnered with Facebook on a project dubbed 'the effects of social media on democracy and elections', to offer selected researchers privacy-preserving access to Facebook's data.

C) **More legal resources need to be channeled to define the scope and limits of digital rights.** The continued attempt in Kenya to criminalize libel is a form of control, which mis-appropriates the legislative process. This has been used in the past against traditional media but was declared unconstitutional by the Kenyan courts. 26 sections of the said Cybercrimes Act are currently suspended pending the hearing and determination of the issue in court. African parliamentarians need to be more vigilant when dealing with new legislative proposals that are comparable to provisions that have previously been declared unconstitutional by the courts. This will avoid expensive and elaborate proceedings in court. Where courts are not independent enough, as is the case in many African states, a new form of information control is then entrenched. Instead, more investment should be made on studies for how best to balance fake news and national security concerns on one hand, with existing guarantees on digital rights on the other.

D) **All actors should be transparent and have defined standards upon which they block websites:** ISPs, communication authorities and related institutions play a pivotal role in the citizen's ability to receive information online. Therefore, any standards upon which any such actor involved with Internet connectivity applies to block a website, or throttle Internet connectivity for business purposes or otherwise, should be clearly defined and explained to the public. Moreover, it should not be a decision taken by a single individual, but rather by a consensus e.g. by a national security council and even then, with proper judicial oversight. A proper legal framework should be developed in this regard. That said, more technical and legal research is needed here as we are yet to develop the appropriate legal theory to balance very critical interests.

E) **More research resources need to be dedicated to understanding fake news and disinformation campaigns:** There is little investigation into the alleged disinformation campaigns Cambridge Analytica ran in Kenya, Nigeria, and Britain. The Mueller report in the U.S. is the only comprehensive investigation into a disinformation campaign that indicted 13 Russians, 3 Russian entities and one U.S. citizen. The Kenyan Government should launch a comprehensive investigation of Cambridge Analytica and the alleged interference operations during the 2018 election period. Principles are emerging on how to govern this issue. The Paris Call for Trust and Security in Cyberspace is a good start; it is endorsed by more than 50 nations, 90 non-profits and universities, and 130 private corporations and groups. One of the nine goals of the Paris Call is to ensure foreign actors do not interfere with elections. However, more ought to be done to operationalize these principles in the legal systems of the signatory states.

F) **More institutions and resourced ought to contribute to fact-checking:** Fact-checking is one of the emerging tactics against disinformation campaigns. However, few institutions are currently involved in this including: Africa Check based in Kenya, Nigeria, Senegal, South Africa and the U.K; Zimfact in Zimbabwe; Pesa Check in Kenya, Uganda and Tanzania; and Dubawa in Nigeria. In a similar vein, BBC Africa have also begun a weekly program called Factfinder to analyze fake news on the continent; they show how journalists put a story together. Further, institutions with data science resources can contribute sentiment analysis techniques to demystify, detect and expose psychographic techniques deployed in an active election scenario.

G) **Entrench transparency in campaign financing, Internet advertising and content moderation:** Kenya has a framework for managing electoral finance, the Kenya Election Campaign Financing Act. Political parties are required to report their expenditures to the Independent Electoral and Boundaries Commission (IEBC) within 3 months after the elections. However, it is not clear whether the party expenditure-reporting mechanisms are effective. For instance, because of the Federal Election Commission in the US, we know that the Trump campaign paid Cambridge Analytica $6 million between July and December 2016. Moreover, the legal frameworks for Internet advertising need to be aligned with their mainstream counterparts. It should be clear who is sponsoring the advertisement, why they are sending the message, which other messages are they promoting on a particular platform, and who is paying for it. Moreover, it ought to be easier to flag and enforce take-down orders for anonymous advertisements promoting disinformation and fake news. We therefore call on government, social media platforms, academia, and civil society to work together to develop a stronger policy framework and legal framework that is both relevant and enforceable from a technical perspective.

REFERENCES

@theRealRaila. The Real Raila [Internet]. Facebook.com. 2019. Available from: *https://www.facebook.com/pg/TheRealRaila/videos/?ref=page_internal*

Access Now. (2018). Internet Shutdowns in Context: Insights from the Shutdown Tracker Project (STOP). [online] Available at: *https://www.accessnow.org/keepiton/#take-action.*

Africa Check | Sorting fact from fiction [Internet]. Africa Check. 2012. Available from: *https://africacheck.org*

BBC World Service TV - Factfinder [Internet]. BBC. Available from: *https://www.bbc.co.uk/programmes/w13xttsw*

Bearak M. 'Shut Down Zimbabwe' protests are met with Internet blackouts and arrests [Internet]. The Washington Post. 2016. Available from: *https://www.washingtonpost.com/news/worldviews/wp/2016/07/06/shut-down-zimbabwe-protests-are-met-with-internet-blackouts-and-arrests/?noredirect=on&utm_term=.0abf19c701e1*

Castells M. Networks of outrage and hope: Social movements in the Internet age. John Wiley & Sons; 2015 Jun 4.

Castells M. The impact of the internet on society: a global perspective. F. González, ed. 2014 Sep:132-3.

Channel 4 News. Cambridge Analytica Uncovered: Secret filming reveals election tricks [Internet]. 2018. Available from: *https://www.youtube.com/watch?v=mpbeOCKZFfQ*

Channel 4 News. Cambridge Analytica: Undercover Secrets of Trump's Data Firm [Internet]. 2018. Available from: *https://www.youtube.com/watch?v=cy-9iciNF1A*

Channel 4 News. How Cambridge Analytica tried to intimidate Nigerian voters [Internet]. 2018. Available from: *https://www.youtube.com/watch?v=KOpKkgXNb50*

Channel 4 News. Kenyans bombarded with fake news in presidential election [Internet]. 2018. Available from: *https://www.youtube.com/watch?v=525TpQNmbAI*

CIPIT Research Reveals Evidence of Internet Traffic Tampering in Kenya: The Case of Safaricom's Network | CIPIT Blog [Internet]. Blog.cipit.org. 2017. Available from: *https://blog.cipit.org/2017/03/23/cipit-research-reveals-evidence-of-internet-traffic-tampering-in-kenya-the-case-of-safaricoms-network/*

CIPIT, (2018) Intentional Internet Disruptions: Estimating Impact in Observable and Shadow Economies.

CIPIT: Strathmore Law School. Biometric Technology, Elections, and Privacy: Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process. [Internet]. 2018. Available from: *https://cipit.org/index.php/2-uncategorised/1479-biometric-technology-elections-and-privacy.*

Communications Authority of Kenya (CA). First Quarter Sector Statistics Report for the Financial Year 2017/2018 (July-September 2017) [Internet]. Nairobi; 2017. Available from: *https://ca.go.ke/wp-content/uploads/2018/02/Sector-Statistics-Report-Q1-2017-18.pdf*

Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace [Internet]. France Diplomatie :: Ministry for Europe and Foreign Affairs. 2019 [cited 1 April 2019]. Available from: *https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in*

Digital Society of Zimbabwe [Internet]. Dszim.org. 2018. Available from: *http://www.dszim.org/2018/08/10/zimbabwean-election-website-blocked-following-2018-general-elections/*

Dubawa [Internet]. Available from: *https://dubawa.org*

Gichuki D, Gwagwa A, Rutenberg I. Historical Antecedents and Paradoxes that Shaped Kenya's Contemporary Information and Communication Technology Policies. Africa Policy Journal. 2016;12:61.

Godana, G. (2019). The Digital Freedom of Association. [online] Available at: *https://blog.cipit.org/2018/09/06/the-digital-freedom-of-association/.*

Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Communications Networks, July 2017.

Ikram A. Limitations on media freedom; Are the current media laws in compliance with the constitution of Kenya?

Ipsos. Ipsos Kenya SPEC poll 17 April 2015 [Internet]. 2015. Available from: https://www.slideshare.net/ipsoske/ipsos-kenya-spec-poll-17-april-2015

Karanja M. CIPIT Research Reveals Evidence of Internet Traffic Tampering in Kenya: The Case of Safaricom's Network | CIPIT Blog [Internet]. Blog.cipit.org. 2017. Available from: *https://blog.cipit.org/2017/03/23/cipit-research-reveals-evidence-of-internet-traffic-tampering-in-kenya-the-case-of-safaricoms-network/*

Karanja M. Kenyan Elections and Alleged Hacking: A Look at the available evidence | CIPIT Blog [Internet]. Blog.cipit.org. 2017. Available from: *https://blog.cipit.org/2017/08/18/kenyan-elections-and-alleged-hacking/*

Karanja, M., (CIPIT), Xynou, M., (OONI) & Filastò, A., (OONI). Kenya: Censorship-Free Internet? 2016 Access Link

Kenya Information and Communications (Registration of SIM-Cards) Regulations, 2015.

Kenya National Commission of Human Rights, On the Brink of the Precipice: A Human Rights Account of Kenya's Post-2007 Election Violence. Nairobi: KNCHR, 2008. Print. See page 32.

La Rue F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011), p 19

Majama K. Zimbabwean election website blocked following 2018 general elections - koliwemajama.co.zw [Internet]. koliwemajama.co.zw. 2018. Available from: *https://koliwemajama.co.zw/zimbabwean-election-website-blocked-following-2018-general-elections/*

Mungai, B. (2019). Digital Right: The Freedom of Assembly. [online] Available at: *https://blog.cipit.org/2018/09/05/digital-right-the-freedom-of-assembly/.*

Muthuri R. Internet Speed Throttling Surrounding Repeat Election? | CIPIT Blog [Internet]. Blog.cipit.org. 2017. Available from: *https://blog.cipit.org/2017/10/29/internet-speed-throttling-surrounding-repeat-election/*

NodeXL | Your Social Network Analysis Tool for Social Media [Internet]. Social Media Research Foundation. Available from: *https://www.smrfoundation.org/nodexl/*

OHCHR | Human Rights Council concludes thirty-second session after adopting 33 resolutions and one decision [Internet]. Ohchr.org. 2016. Available from: *https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=20252&LangID=E*

OONI - DNS consistency [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/dns-consistency/*

OONI - HTTP Host [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/http-host/*

OONI - HTTP Requests [Internet]. Ooni.torproject.org. Available from: h*ttps://ooni.torproject.org/nettest/http-requests/*

OONI - Lantern [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/lantern/*

OONI - Meek Fronted Requests [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/meek-fronted-requests/*

OONI - Telegram test [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/telegram/*

OONI - Tor Bridge Reachability [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/tor-bridge-reachability/*

OONI - Vanilla Tor [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/vanilla-tor/*

OONI - Web connectivity [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/web-connectivity/*

OONI - WhatsApp test [Internet]. Ooni.torproject.org. Available from: *https://ooni.torproject.org/nettest/whatsapp/*

Ooni.torproject.org. OONI - Psiphon. [online] Available at: *https://ooni.torproject.org/nettest/psiphon/.*

Opiyo, C. (2019). Free Speech in the Digital Space. [online] Available at: *https://blog.cipit.org/2018/09/03/free-speech-in-the-digital-space/.*

PesaCheck [Internet]. Available from: *https://pesacheck.org*

Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa / Press Releases / ACHPR [Internet]. Achpr.org. 2019. Available from: *http://www.achpr.org/press/2019/01/d440/*

Rouvroy A, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' 2009.

Satar, J. (2019). Defining a Digital Right to Access. [online] CIPIT Blog. Available at: *https://blog.cipit.org/?p=6957.*

Scherer S. Evgeny Morozov – The Folly of Technological Solutionism (2013) [Internet]. New Media for Social Change. 2014. Available from: *http://wpmu.mah.se/nmict142group5/index.php/evgeny-morozov-the-folly-of-technological-solutionism-2013/*

Socialscience.one. (2019). SOCIAL SCIENCE ONE: Building Industry-Academic Partnerships. [online] Available at: *https://socialscience.one.*

Socialscience.one. (2019). SOCIAL SCIENCE ONE: Building Industry-Academic Partnerships. [online] Available at: *https://socialscience.one.*

Special Counsel's Office U.S. Department of Justice. The Mueller Report: The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion. Skyhorse; 2019.

Texas Media Company Hired by Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals [Internet]. Privacy International. 2017. Available from: *https://privacyinternational.org/long-read/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack*

The cyberattack against the Zimbabwe Electoral Commission – Qurium Media Foundation [Internet]. Qurium.org. 2018. Available from: *https://www.qurium.org/alerts/zimbabwe/the-cyberattack-against-the-zimbabwe-electoral-commission/*

Tugee, L. (2019). Defining the Digital Right to Privacy. [online] Available at: *https://blog.cipit.org/2018/09/04/defining-the-digital-right-to-privacy/.*

Twitter and Facebook are blocked in Uganda as the country goes to the polls [Internet]. Quartz Africa. 2016. Available from: *http://qz.com/619188/ugandan-citizens-say-twitter-and-facebook-have-been-blocked-as-the-election-gets-underway/*

Wamathai. Justice Chacha Mwita suspends 26 sections of the Computer Misuse and Cybercrimes Act - BAKE [Internet]. BAKE. 2018 [cited 2018]. Available from: *https://www.blog.bake.co.ke/2018/05/29/justice-chacha-mwita-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act/*

Wellman B., Rainie L. Networked. MIT Press, The.; 2012.

Westin A, 'Privacy and Freedom', 25 Washington and Lee Law Review, 1968.

Xynou M, Filastò A, Karanja M. OONI - Kenya: Censorship-free internet? [Internet]. Ooni.torproject.org. 2016. Available from: *https://ooni.torproject.org/post/kenya-study/*

Zimbabwe Election 2018 [Internet]. Zimelection.com. 2018. Available from: *https://zimelection.com*

Zimbabwe Electoral Commission [Internet]. Zec.org.zw. Available from: *https://www.zec.org.zw/*

Zimbabwe Media Commission | About the Organization [Internet]. Mediacommission.co.zw. [cited 1 April 2019]. Available from: *http://mediacommission.co.zw/index.php/about-the-company/*

Zimbabwe: 2018 General elections website blocked | Association for Progressive Communications [Internet]. Apc.org. 2018. Available from: *https://www.apc.org/en/blog/zimbabwe-2018-general-elections-website-blocked*

Zimbabwean online fact-checking platform | ZimFact [Internet]. Available from: *https://zimfact.org*

CIPIT

CENTRE FOR INTELLECTUAL PROPERTY
AND INFORMATION TECHNOLOGY LAW

VT OMNES VNVM SINT

Strathmore University

Law School