Office of the High Commissioner on Human Rights

Staff Development Unit.

United Nations, Geneva, Switzerland

Online surveillance and censorship during elections and key political events:: Coffee Briefing ::: Wednesday, 21 February 2018 from 14:00 to 15:30

By Arthur Gwagwa

Senior Research Fellow- Center for Intellectual Property and Information Technology Law

Project: Sub-Saharan Africa elections and Cyber Regionalism

Collaborating with the Open Observatory for Network Interference (OONI).

Funded by the Open Technology Fund.

Topics for Discussion

- Impact of technologies on elections and human rights
- Defining Online Information Controls
- Technical controls and what OONI does
- Countries and Issues covered.
- Findings from Technical OONI Research
- Regulatory Controls of Online Spaces
- Social controls of online spaces
- Elections Security and Privacy: Safeguards in the use of election biometric technologies
- Computational Propaganda, Algorithms-based Misinformation, Intermediaries
- Social Media, Civic Space, Off and Online Freedom of Expression.

1. Impact of technologies on elections and human rights

Elections can decide the political course of nations for years and even decades, and pose critical moments for a range of human rights, including the freedoms of expression and association, and the rights to privacy and political participation. An election’s success depends on transparent and accountable protection and promotion of these rights. As voting and identification procedures become digitized, technology is increasingly inextricable – and influential – during elections, in ways that authorities have yet to address.

While modern computing methods, in particular cloud-based machine learning, which is fueled by big data technology, constitute a paradigm shift in how we interact and communicate and enhance the protection of human rights, their role in undermining has been under spotlight, especially in the conduct of elections. Some of the challenges include the use of social media for propaganda and questions around the integrity of electronic voting, as we saw in Kenya. The misuse of technology has negatively impacted on the freedom to participate in the political process. Yet, the same technologies that potentially threaten rights also provide opportunities for their enhanced protection. For example, social media has been used to provide information to voters vital for them to make informed choices.

Drawing on previous research I carried out alone and with others, this briefing considers both the opportunities for the enhanced protection of human rights by technologies, the threats they pose and approaches that need to be adapted to meet the rapidly evolving technological landscape.

2. Defining Information Controls

According to Citizen Lab at the Munk School of Global Affairs at Toronto University, information controls is utilized as a broad term to define actions that governments, the private sector, and other actors take through the internet and other information communications technologies to deny (e.g, internet filtering), disrupt (e.g., network shutdowns), monitor (e.g, network surveillance), or secure (e.g., encryption) information for political ends. Information controls can also be non-technical and implemented through legal and regulatory frameworks, including informal pressures placed on private companies.

The Citizen Lab pioneered the use of “mixed methods” in researching Internet governance and controls. Understanding how the Internet functions requires attention to both the technical aspects and the underlying social, legal, political, and economic systems and processes behind them. In order to meet their objectives, projects that utilize this approach combine field and literature research, legal and policy analyses, as well as technical measurements, to develop a holistic understanding of Internet governance and freedom of expression in the selected countries.

3. Technical-based Controls and what OONI Probes

The Open Observatory of Network Interference (OONI) is a free software project that aims to empower decentralized efforts in increasing transparency of internet censorship around the world. To this end, OONI has developed multiple software tests that are designed to measure the following:

* Blocking of websites;
* Blocking of instant messaging apps (WhatsApp, Facebook Messenger, Telegram);
* Blocking of censorship circumvention tools (Tor, Psiphon, etc.);
* Presence of systems ("middle boxes") that could be responsible for censorship and/or surveillance.

Tens of thousands of users have run OONI's software (called ooniprobe) across more than 190 countries over the last 5 years, contributing to the collection of millions of network measurements from around the world. Upon analysis, these network measurements shed light on various instances of internet censorship and traffic manipulation.

All network measurement data is published on OONI Explorer (https://explorer.ooni.torproject.org/world/), which is arguably the largest publicly available resource on internet censorship to date.

The data that is collected through OONI software can be useful to researchers, such as Freedom House, technology developers in the Internet freedom community and users at risk on the ground since such data shows exactly how censorship is implemented in a network. In other words, this data can be used as technical evidence of censorship. This will raise awareness of threats and help developers to work with users in designing appropriate privacy and security enhancing tools that enable unhindered access.

4. Countries and Issues covered.

Both traditionally repressive and even democratic governments across the world, including in Africa are responding to key political events such as elections and protests by increasing information controls when the information being targeted has the highest value (e.g., during elections or public demonstrations). This is having an effect on a wide range of rights including privacy, expression, association and assembly and to vote.

Countries examined

- Lesotho, Rwanda and Angola, DRC and the Gambia.
- Venezuela, Turkey, Catalonia, Pakistan, Uganda, Ethiopia, Malaysia & Iran.

Addressed problems

- Restrictive Internet filtering by technical methods (IP blocking[1], DNS filtering[2], TCP[3] RST, DPI[4], etc.)
- Blocking, filtering, or modification of political, social, and/or religious content (including apps)
- Technical attacks against government critics, journalists, and/or human rights organizations (Cyber attacks)
- Localized or nationwide communications shut down or throttling (Blackouts)
- Pro-government manipulation of online discussions (propaganda, imitation content, and/or sock puppets)
- Repressive surveillance or monitoring of communication
- Policies, laws, or directives that increase surveillance, censorship, and punishment

5. Findings from Technical OONI Research

Elections

======

1. Uganda: Social media blocked during 2016 general elections: https://ooni.torproject.org/post/uganda-social-media-blocked/

OONI data shows that Smile Telecom blocked the HTTP and HTTPS versions of Facebook, Twitter, WhatsApp and Viber, whereas Orange only blocked

[1] **IP blocking** is a form of security used on mail, Web or any other Internet servers to **block** connections from a specific **IP** address or range of addresses that are considered undesirable or hostile.

[2] Domain Name System **Blocking**, or **DNS Blocking** is a strategy for making it difficult for users to locate specific domains or web sites on the Internet. It was first introduced in 1997 as a **means** to block spam email from known IP addresses. However, **DNS blocking** should not be the only line of defense against spam email.

[3] Transmission Control Protocol is one of the most used protocols in digital network communications and is part of the Internet protocol suite, commonly known as the **TCP**/IP suite. Primarily, **TCP** ensures end-to-end delivery of data between distinct nodes.

[4] **Deep packet inspection** is a form of computer network packet filtering that examines the data part of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination. **Packet injection** (also known as forging packets or spoofing packets) is a computer networking term that refers to the process of interfering with an established network connection, by means of constructing packets to appear as if they are part of the normal communication stream. The **packet injection** process allows an unknown third party to disrupt or intercept packets from the consenting parties that are communicating, which can lead to degradation or blockage of users' ability to utilize certain network services or protocols. **Packet injection** is commonly used in man-in-the-middle attacks and denial-of-service attacks.

the HTTP version of Facebook and Twitter.

2. Venezuela: Blocking of sites during 2015 parliamentary elections:
https://ipysvenezuela.org/navegarconlibertad/2016/03/29/resultados-navegables/
(IPYS Venezuela study using OONI Probe)

3. The Gambia: Internet shutdown during 2016 presidential elections:
https://ooni.torproject.org/post/gambia-internet-shutdown/ (third party
datasets)

4. Rwanda censors critical, independent media in targeted fashion leading up to and during the country's recent presidential election.
https://www.opentech.fund/article/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election

Political protests

===========

1. Ethiopia: DPI used to block Ethiopian media websites during wave of
political protests: https://ooni.torproject.org/post/ethiopia-report/

We also found WhatsApp to be blocked during the protests, as well as a
number of human rights sites, LGBTQI sites, and censorship circumvention
tool sites.

2. Ethiopia: Internet shutdown in August 2016 at the height of political
protests:
https://ooni.torproject.org/post/ethiopia-internet-shutdown-amidst-recent-protests/
(third party datasets)

3. Pakistan: Blocking of news outlets, social media sites, and instant
messaging apps during Islamist protests:
https://ooni.torproject.org/post/how-pakistan-blocked-social-media/

4. Iran: DPI blocking of Instagram and TCP blocking of Telegram during
protests: https://ooni.torproject.org/post/2018-iran-protests/ &
https://ooni.torproject.org/post/2018-iran-protests-pt2/

Other cases of politically-motivated censorship

==============================

1. Catalonia: Blocking of sites related to the Catalan Independence
Referendum:
https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/

2. Malaysia: DNS blocking of news sites covering the 1MDB scandal:
https://ooni.torproject.org/post/malaysia-report/

3. Turkey: Internet access disruptions during attempted military coup:
https://ooni.torproject.org/post/turkey-internet-access-disruption/

6. Regulatory Controls of Online Spaces: Polices, Laws and Internet Governance Frameworks

- Angola: *As Angola comes online, government has been laying a regulatory and legal framework for censorship.*

https://www.opentech.fund/article/angola-emerging-battleground-digital-rights

- Lesotho: Regulator pushes back against government attempts to shutdown social media. https://www.opentech.fund/article/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections
- Zimbabwe Cyber security ministry and Human rights

  https://www.cfr.org/blog/what-zimbabwes-cybersecurity-ministry-says-about-human-rights-country

7. Social Controls of online spaces: Third Generation Controls

- **Authority-led information manipulation-Zimbabwe**

Field research in Sub Saharan Africa reveal that authority-led information manipulation is assuming different patterns: reflecting a range of motivations, and can include efforts undertaken to open up access to information or secure privacy as much as efforts undertaken to do the opposite.

While the current focus on internet shutdowns remains of utmost importance, less discussed are instances when authorities keep the internet on, for their benefit including by seeking to control the public discourse on it to achieve political goals. This trend is increasingly seen during key political events such as elections and coups. Such controls which are often applied in highly dynamic ways often respond to events on the ground. For instance, during public uprisings, authorities view the Internet as a double-edged sword, therefore to shut it down or to keep it open is the authoritarian's biggest dilemma.

In Zimbabwe during the November 2017 coup which became Mugabe's end game, the military kept it open and encouraged the free flow of information as it suited its motive to clothe the coup with constitutional legitimacy. Similarly during Kenya's August 2017 election, the government only backtracked on its threats to shut down the Internet when it realised that it could benefit from fake news and disinformation that discredited the opposition. This is also seen on a global scale such as the 014 Thailand coup how Turkey's President Erdogan used Skype to appeal to his supporters to resist military takeover during the July 15, 2016 failed coup.

As was the case in Turkey, such authority-led digital information manipulation during popular uprisings can achieve short term gains based on the popular sentiment of the moment. However, controlling of discourse and opinions in such spaces can have long term ramifications to freedom to express different views in pursuit of democratic alternatives. In Africa, Ethiopia set the precedent when the ruling Ethiopian People's Revolutionary Democratic Front (EPRDF) first came to power, with the assistance of China. It heavily invested in ICTs, opened the space for debate but refused to engage with the very debates it had allowed to bloom.

https://www.academia.edu/35315190/Impact_of_Military-Led_Information_Controls_to_Democracy_in_Zimbabwes_recent_Coup

- **Computational Propaganda, Algorithms-based Misinformation, Intermediaries**

There has been a rise of propaganda and misinformation around elections, especially on social media platforms, and highlight corporate and government responses. Widespread criticism of social media platforms, who are seen as pursuing profit at the expense of democratic values, gives wide cover to policymakers for a range of restrictive measures. Rising liability for intermediaries and increased pressure on companies to enforce government policies threatens freedom of expression, and risks harming democracy in the name of free and fair elections. Drawing from his U.S. experience, Peter will offer a comparative analysis on U.S 2016 elections and its implications for political events elsewhere, with insights into specific policy and practical responses of large internet companies.

- **Social Media, Civic Space, Off and Online Freedom of Expression.**

Social media has played a crucial role in Kenya's 2017 and previous elections, from citizens' engagement, political engagement especially by female candidates. However, it has also been blamed for misinformation and for being used as a platform for fomenting violence. In turn, the government -led multi stakeholders have previously adopted the so called 'Peace at All

Costs" measures which some quarters have criticised on human rights grounds. This segment will discuss the role of social media in Kenya's elections with a particular emphasis on the 2017 elections and the implications for human rights.

8. Surveillance

A number of governments are using surveillance powers. In the case of Kenya, surveillance is preferred over censorship whereas in Ethiopia, it is used alongside censorship. Future research should try to further examine how surveillance relates to censorship. Also, an understanding of the surveillance market will help shed light on where repressive governments are obtaining their surveillance technologies from. In the case of censorship and surveillance, states are out to balance the national and individual liberty. **See: https://www.academia.edu/35814477/Sub-Saharan_Africa_Internet_Freedom_Landscape_-_2017_Conference_Report**

One problematic area here relates to the use of network middleboxes as it is not clear what they are being used for. As 'dual use' technologies, they may be used for data traffic management but also for to effect censorship.

Impact of surveillance beyond violating privacy.

In Kenya, communications surveillance is a matter of life and death: new Privacy International investigation. https://medium.com/privacy-international/in-kenya-communications-surveillance-is-a-matter-of-life-and-death-new-privacy-international-a76b5416583

9. Security and Privacy in Electronic voting

Safeguards in the use of election biometric technologies

The ruling by the Kenyan Supreme Court on the interference with the electronic transmission of election results ("hacking") and its impact on the integrity of the election raises questions on the reliability of electronic election processes and the challenges this poses to democracy at large. The elections demonstrate that voting is not simple matter of secure system defending against attacks from an external adversary like what happened in the U.S.

Technological innovation can bring great advantages, including in elections. If employed correctly, it can increase the numbers of the population able to exercise their vote by increasing access to the (virtual) ballot box, reduce the factor of human error in counting votes and help bring out conclusive election results more quickly. However, they can potentially be compromised. Technological complexity may render elections more opaque and vulnerable to manipulation—or at least the suspicion of manipulation. We should be vigilant, however, that

cyberspace does not become the next space in which states assert absolute power at the expense of the rights of its citizens, including the right to vote in free and fair elections. As Kenya prepares for another election, by drawing lessons from South Africa and other countries, this segment will discuss both human, legal and technological measures Kenya and indeed other African countries should put in place to safeguard the integrity of the vote and ultimately accurately reflect the will of the people. See my detailed analysis on the legal and technological issues on the Kenyan elections here:
https://www.academia.edu/34594658/Understanding_the_Legal_and_Technological_challenges_in_Kenyas_2017_Elections

Also see my blog on the governance issues and their impact on the technological issues:
https://www.worldpoliticsreview.com/articles/23290/is-kenya-s-election-debacle-a-failure-of-technology-or-governance