Reality Check

Status of Internet Freedom in Nigeria

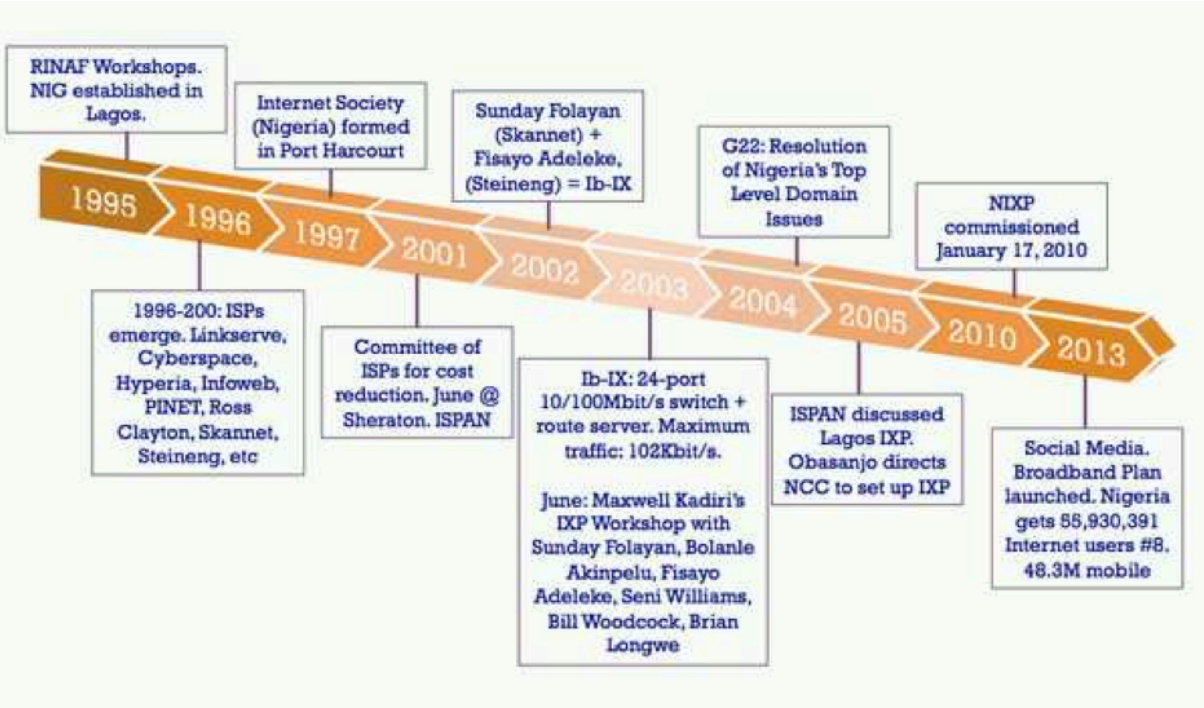
PARADIGM INITIATIVE NIGERIA

'Gbenga Sesan and Femi Abikoye
Paradigm Initiative Nigeria

This report is part of the output for the Cyber Stewards Network project of The Citizen Lab, Munk School of Global Affairs, University of Toronto, and supported by IDRC.

Reality Check: Status of Internet Freedom in Nigeria

1.0 Introduction



Pictorial representation of Internet development timeline for Nigeria

Internet access in Nigeria has grown exponentially in recent years, particularly after the introduction of mobile phone data and Fixed Wireless Access (FWA) services in July 2007. In 2013, internet penetration stood at 33% up from 28% in 2011 according to the International Telecommunications Union (ITU). The number of active mobile phone subscribers also increased from almost zero in 2000 to over 128.6 million subscribers or 91.9% penetration in February 2013 as reported by the Nigerian Communications Commission (NCC). The latest ITU data notes nearly 113 million mobile phone subscriptions and a mobile phone penetration rate of 68% in 2012, up from 57% in 2011. Mobile Internet subscriptions have also steadily increased in the past few years, reaching a penetration rate of 26% in 2012 according to an October 2012 report published by iHub Research. Nigerian Communications Commission reported 63,474,364 mobile Internet subscriptions in February 2014.

There has not been a more opportune moment to talk about the state of Internet freedom in Nigeria. The year 2013 saw the world waking up to the reality that not only have many citizens been under clandestine watch for a long time by their governments, but also to the worrying depths of the amounts of access that State actors have to the private lives of billions.

As the global surveillance debate escalated, more and more governments have been implicated in acts of unmitigated violation of the privacy of their citizens. Those who

haven't already begun to pry into the lives of their citizens are planning to do so. Millions of dollars are being invested to acquire domestic surveillance capabilities. These developments have significant portents for Internet freedom and cannot be ignored.

2.0 The State of Access

As earlier mentioned, Internet access in Nigeria has grown through incredible leaps, especially with the infrastructural challenges the nation faces. For Internet freedom to truly be examined, access to the Internet must first be discussed.

The latest statistics reported by the Ministry of Communication Technology puts broadband penetration rate at 6% as of December 2012, with average broadband download speed of 2.26 Mbps and upload speed of 1.57 Mbps. Recognizing the importance of ICTs for economic development, the Communication Technology ministry set up a Presidential Committee in August 2012, tasked with the creation of a National Broadband Plan that aims to increase Nigeria's broadband penetration seven-fold by 2018.

One of the major achievements of the committee is the successful auction of 2.3GHz band and the planned licensing of Infrastructure Companies that will provide a national broadband network on a non-discriminatory, open access and price-regulated basis to all service providers. There is also a plan to license 2.5GHz and 2.6GHz bands sometime in 2014. The proposed switch to digital broadcasting planned for 2015 will also free up broadband for increased Internet penetration.

Nevertheless, a large urban-rural divide characterizes access to ICTs. According to a Gallup poll published in August 2012, 39% of urban dwellers in Nigerian said that they had used the Internet in the last week, compared with only 16% of those living in rural areas. High costs are another major impediment to Internet access, although increased competition among service providers has made the cost of access more affordable for many Nigerians.

In addition to cost, power cuts continue to disrupt service and access, with many users reporting the need to use private generators to stay online during outages. While the country's electricity supply improved notably in 2012, it saw a huge decline in 2013 and Nigeria is still reportedly the largest importer of private power generators in Africa despite the country's status as an oil-rich country.

3.0 Internet Freedom Regulation: Policies and Laws

Some governments around the world are drafting new legislation, to come to terms with the new reality of the Internet and its many provisions. Some do this to legalise their existing polices on Internet regulation while others do so in a fresh effort to regulate the

Internet. While some legal frameworks can be easily applied in an online context, others require substantial adaptation. It is thus critically important to ensure that any legislation, which impacts on freedom of expression, is consistent with recognised international human rights standards. This is particularly important since a significant part of the Internet's value, as a medium of expression, is its open and borderless nature. This value can only be preserved through a regulatory framework that balances issues of security (or protection) with those of privacy (and rights). In order to fully harness the empowerment benefits of the Internet, people must be allowed to communicate freely online.

We looked at various documents at different stages of the legislative process in the course of preparing this report – Bills, Acts and amendments. Our focus was on policy documents, administrative regulations, National Assembly bills and laws that contain provisions with potentially far reaching implications for Internet Freedom in Nigeria.

Any conversation about Internet freedom in Nigeria must start first of all with the Nigeria's *grundnorm*, the core from which all laws derive their legality, the 1999 Nigerian Constitution (as amended) that embodies the inalienable rights of its citizens and is the wellspring from which all other legislation derive their authority. Chapter 4 of the Constitution of The Federal Republic of Nigeria, 1999 (as amended) contains the fundamental rights of Nigerians.

The specific provisions relevant to Internet freedom are sections 36, 37 and 39, which grant rights to fair hearing, privacy and freedom of expression, respectively. As the Internet is first and foremost a means of communication between systems through a network, it is at its core a medium of expression thus the privacy of this medium of communication must be protected and valued.

Before the advent of the internet, when letters were more commonly used as a means of communication, the value of privacy was put above all else as exemplified by Section 18(2) and 29 of the Nigerian Postal Service Act (Decree) 1992 which made it a felony offence to open a letter posted in Nigeria except with the authority of the postmaster and that law is still applicable in today Nigeria. If this law is applicable to physical mail in Nigeria, why should electronic communication be refused the same level of protection and more?

3.1 Policies of the Nigerian Government and its agencies

The current Nigerian National ICT Policy (approved in principle) supports the creation of better cybersecurity legislation for Nigeria but neglects to state the importance of civil liberties. The absence of the balance of civil liberties with cyber-security in most of the bills, that touch on the Internet and any form of regulation, has resulted in many calls for a thorough review. Another essential policy to Internet freedom is the broadband policy, which aims to prepare the ground for

better access to Internet in Nigeria. The policy focuses on access but access without freedom is incomplete.

Central to the discussion on Internet freedom in Nigeria is the *Draft Lawful Interception of Communications Regulation* by the National Communication Commission, which seeks to provide legal framework for the lawful interception of communications in Nigeria. The proposed regulation has in a general sense been seen more as a control contrivance by government authorities. It does not allow reports of interception to be available to the public and it uses fluid languages that can be interpreted arbitrarily. In a country where political power is subject to abuse in an atmosphere of impunity, this is dangerous.

The proposed regulation gives a lot of unsupervised powers to the Nigerian Communications Commission, including the manner in which communication is to be intercepted, the forceful storage of all data by telecommunication companies and many more. It also, in its application, affects the local encryption industry. The draft regulation in itself is odd as it is secondary legislation (from an agency of government) seeking to upturn rights guaranteed by the constitution. Unfortunately, this is not the only effort the Nigerian Communications Commission (NCC) is making towards interception as there is another sponsored bill seeking to amend the Telecommunications Act to give NCC as much power.

3.2 Acts, Laws and Decrees as passed by the National Assembly or its equivalent the Military Council

There are laws in Nigeria that partly protect the freedom of Internet users through the recognition of certain civil liberties. An example of such protection is that of the Advance Fee Fraud Act 2006, which demands a warrant before telecommunication data can be obtained. The National Identity Management Commission Act 2007 suggests strict protection of data. The provisions in the Evidence Act of 2011 are also significant not only because they provide for the admissibility of electronic evidence but because their existence now allows the law to address a whole new vista of human and digital communications. It breaks down the barriers between the physical and the electronic, merging both online and offline realities and reinforcing the fact that offline and online rights have equal standing in law.

3.3 Bills currently being considered at the National Assembly.

There is probably no other subject matter in the current National Assembly that has such as many bills as those touching on electronic communications and/or transactions. Looking through all these bills reveals the haphazard nature of our legislative process. Many bills are essentially trying to achieve the same thing that existing bills cover, and the sheer amount of redundancy and duplication – leading

to needless waste of man hours that would have been expended on more productive activity had bills been consolidated – is astounding. A lot of the redundancy and duplication is obvious around bills seeking to regulate electronic transactions and eCommerce, or combat cybercrime.

Though none of these bills have been passed into law, they pose a number of threats to Internet freedom. With some, the threats are in the technicalities while others are outright violations. A common example of threat is the interception of communications without a warrant, or a poorly worded draft that allows for loose interpretations, setting aside the need for warrants.

These examples are shown in bills like the bill for *An Act to Authorize Law Enforcement Agencies to Receive Oral and Written, In Form of Short Messaging Service (SMS), Communication Made by an Individual Using Telecommunication and Internet in Order to Enhance Criminal Investigations in Nigeria and for Other Related Matters*, the bill for *An Act to provide for the Regulation of Interception, Development and Protection of Communications Networks and Facilities for Public Interest and Other Related Matters,* and the Terrorism Amendment Bill 2013.

Some bills appear harmless at first glance but they threaten Internet freedom through the manner in which they seek to create oversight functions. An example is the bill for *An Act to Amend the National Communications Commission Act 2003*. Over the years, rights advocates have been vociferous about the protection of human rights in Nigeria but abuse is still commonplace. It can be argued that free speech is more of a big deal than ever as more citizens, most of them youth, have taken to social media to express their frustrations with governance and to contribute to national conversations.

4.0 Threats to Internet Freedom

Looking at the bills currently in the National Assembly, the following are common threats identified in many of the provisions in these legislative documents.

4.1 Unauthorised Access and Usage

While the aim of many of the provisions in these bills is presumably to combat cybercrimes, their wording criminalises enormous amounts of innocuous behaviour. Nearly every information system, including many websites, contains a terms of use agreement dictating the precise way in which the product or service is authorised to be used. These documents frequently contain binding conditions. For example, the website of a popular hotel chain contains an agreement which states that users must be at least eighteen years of age. However, by making it a criminal offence in

the bills to use an information system or access data without authorisation, or in excess of the authorisation received, users who wish to stay on the right side of the law would have to slog through pages of terms and conditions for every website they visit and any device or programme they use to ensure that they are not using the service beyond the dictates of its creator. Such principles in various bills should be more specific.

4.2 Privacy Breach through Mass Surveillance

Respect for privacy is key to preserving freedom of expression on the Internet. It is broadly recognised that privacy and the ability to communicate free from surveillance are necessary to democratic discourse. As the United Nations Special Rapporteur on Freedom of Opinion and Expression noted: "States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy... Without adequate legislation And legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights, defenders and whistle-blowers, for example, cannot be assured that their communication will not be subject to States' scrutiny".

4.3 Poorly Drafted Laws

With most of the bills that have either positive or negative effects on Internet freedom, the draft quality is where the huge problem lies. From our review, most of the bills suggest that the intention of the lawmakers includes the provision of laws that also protect the Nigerian citizens but they do not bother with the interpretation of the clauses, thus while the law appears harmless, it can lead – through interpretation – to a rightful act becoming illegal. An example of poor drafting is the Cybercrime Bill 2013. In its effort to curb hate crimes based on race, ethnicity, etc, the bill uses the word 'insult' which could apply to so many circumstances, leaving an open-ended inference on what a person might say or do that can lead to a jail term. These errors, or deliberate attempts at hurting Internet Freedom, are numerous and more importantly, they spread across too many bills.

4.4 Replication of Bills

Many of the bills carry the same themes and this is due to the efforts to adapt old bills to the current climate without editing or amending them, and probably the desire to score political points without any thorough consultation by some lawmakers. The lack of consolidation of the bills has led to the lack of attention being given to the sector and may lead to continued lack of balance in regulations being considered for the purpose of "national security".

5.0 National Assembly Bills and Internet Freedom

In this section, we provide a list of National Assembly bills that could hurt Internet freedom, those that touch on the subject but have no restrictions and those that have outright negative clauses on Internet Freedom.

5.1 Bills/Acts That Could Hurt Internet Freedom Through Interpretation

1. Cybersecurity Bill 2011
2. Electronic Transaction Bill 2011 (HB 03)
3. Electronic transfer of funds Crime Bill 2011 (SB 35)
4. Telecommunications Investigation Bill
5. Cybercrime Bill 2013
6. A Bill For An Act To Amend The Copyright Act For The Purposes Of Making Provisions For The Technological Measure Of Protecting For Technological Matters On Protecting Counterfeit And For Other Related Matters
7. Advance Fee Fraud And Other Fraud Related Offences (Amendment) Act 2006
8. A Bill To Provide For The Interception And Monitoring Of Certain Communication; To Provide For The Interception Of Postal Articles And For The Monitoring Of Communication In The Case A Of A Serious Offense Or If The Security Offense Or Other Compelling National Interests Is Threatened; To Prohibit The Provisions Of Certain In Telecommunication Services Which Do Not Have The Capacity To Be Monitored; To Regulate Authorised Telecommunication Monitoring And For Other Matters Connected Therewith
9. A Bill For An Act To Amend The National Communications Commission Act 2003 To Empower The Police And Security Agencies To Track, Intercept And Monitor Conversations And Text Messages Involving Suspected Terrorist And Other Matters (HB 13.02.470)
10. Terrorist Prevention (Amendment) Act 2013
11. Amendment Of Cap P3 Penal Code Of The Laws Of Federation Of Nigeria To Insert New Chapter Computer Misuse And Cybercrime Offences
12. A Bill For An Act To Facilitate The Use Of Information In Electronic Form For Conducting Transactions In Nigeria And For Connected Purposes (SB 248)
13. Amendment Of Criminal Code Of The Laws Of Federation Of Nigeria To Insert New Chapter Computer Misuse And Cybercrime Offences
14. A Bill For An Act To Provide For The Promotion Of Internet Safety In Nigeria And Other Related Matters (HB 673)

5.2 Bills/Acts That Touch on Internet Freedom But Have No Restrictions

1. Electronic Transaction (Establishment) Bill 2013
2. National Identity Management Commission Act 2007
3. Data Protection Bill 2010 (HB 45)
4. Advance Fee Fraud And Other Related Fraud Offences
5. Electronic Transfer Of Funds Crime Bill 2011 (SB 35)
6. Nigeria Communication Commission Act 2003
7. Mobile Number Portability Regulation 2013
8. National Information Technology Development Act 2007
9. A Bill For An Act To Amend The Copyright Act For The Purposes Of Making Provisions For The Technological Measure Of Protecting For Technological Matters On Protecting Counterfeit And For Other Related Matters
10. A Bill For An Act To Protect Telephone Consumers From The Activities Of Telemarketers And To Provide For Adequate Sanctions Against The Business Of Telemarketing In Nigeria And Other Purpose Forthwith (HB 13.01.427)
11. Electronic Commerce (Provision of Legal Recognition) Bill 2011 (SB 09)

5.3 Bills That Have Negative Clauses On Internet Freedom

1. A Bill For An Act To Provide For The Prohibition Of And Punishment For Electronic Transaction Fraud And Crime In All Electronic Transaction In Nigeria And For Other Related Matters (SB 69)
2. A Bill For An Act To Authorize Law Enforcement Agencies To Receive Oral And Written In Form Of Short Messaging Service (SMS) Communication Made By An Individual Using Telecommunication And Internet In Order To Enhance Criminal Investigations In Nigeria For Related Matters (HB 13.03.485)
3. Electronic Transfer of Funds Crime Bill 2011 (SB 35)
4. Cybersecurity Bill 2011
5. Cybercrime Bill 2013
6. A Bill For An Act To Amend The Copyright Act For The Purposes Of Making Provisions For The Technological Measure Of Protecting For Technological Matters On Protecting Counterfeit And For Other Related Matters
7. Advance Fee Fraud And Other Fraud Related Offences (Amendment) Act 2006
8. A Bill To Provide For The Interception And Monitoring Of Certain Communication; To Provide For The Interception Of Postal Articles And For The Monitoring Of Communication In The Case A Of A Serious

Offense Or If The Security Offense Or Other Compelling National Interests Is Threatened; To Prohibit The Provisions Of Certain In Telecommunication Services Which Do Not Have The Capacity To Be Monitored; To Regulate Authorised Telecommunication Monitoring And For Other Matters Connected Therewith

9. A Bill For An Act To Amend The National Communications Commission Act 2003 To Empower The Police And Security Agencies To Track, Intercept And Monitor Conversations And Text Messages Involving Suspected Terrorist And Other Matters (HB 13.02.470)
10. Terrorist Prevention (Amendment) Act 2013
11. A Bill For An Act To Provide For The Promotion Of Internet Safety In Nigeria And Other Related Matters (HB 673)

6.0 Clandestine Government Operations that Threaten Internet Freedom

By some accounts, the federal government of Nigeria has currently started surveillance operations in Nigeria without proper legal framework or the oversight of other arms of the government whose legal duty it is to regulate executive powers. The mere refusal of the federal government to make a statement on continued accusation levelled against it that it is either already undergoing mass surveillance operations or making aggressive efforts to enable them do so has been seen as enough evidence.

6.1 Elbit Systems' $40 Million Contract[1]

In April 2013, a Nigerian online newspaper, *Premium Times*, broke the news of a $40 million Internet surveillance contract, following the global press release of the Israel-based company, Elbit Systems[2], to whom the contract was awarded by the Nigerian government. The purpose of the contract was to enable government monitor Internet communications of citizens. Following an unsuccessful request for details through a Freedom of Information letter to the Presidency, Paradigm Initiative Nigeria filed a suit at the Federal High Court, requesting an Order of Mandamus in a bid for the court to compel the Federal Government to release information concerning the contract.

On July 3, 2013, Honourable Justice G. O. Kolawole gave a ruling against the Paradigm Initiative Nigeria's plea/application for an Order of Mandamus. We are currently appealing the decision before the Court of Appeal (Abuja Judicial Division)

[1] http://www.informationng.com/tag/elbit-systems

[2] http://www.premiumtimesng.com/news/150333-exclusive-elbit-systems-officials-arrive-begin-installation-40-million-internet-spy-facility-nigeria.html

under the case number CA/A/A2013. A court date, February 4 2015, was only recently set to hear the appeal.

This exclusive action of the executive arm of government caused no small stir, especially on the floor of the Lower House at the National Assembly. Hon. Shehu Gusau, the chairman of the House of Representatives Committee on Information and Communication Technology, on May 30, 2013, called for a suspension of the contract and a probe, to fish out those who are responsible for the illegal awarding of the contract.

Despite this call, news reports from November 27, 2013, had it that the contract is still being undertaken by Elbits Systems and that its employees and equipment have arrived Abuja, Nigeria, to commence the building of facilities. It is believed that it will take two years to complete the project and training for the use of equipment. In the 2013 budget, the Nigeria National Security Agency had $60 million slated for surveillance and in its proposed 2014 budget, it has much more budgetary allocation for the same task. The types of mass surveillance carried out by the NSA are unknown, and this is a cause for concern.

6.2 Remote Control System (RCS) Product Hacking Team[3]

Hacking Team is a Milan-based company that says it's the "first to propose an offensive solution for cyber investigations". Their Remote Control System (RCS) is a suite of monitoring implants sold exclusively to government agencies worldwide. RCS can capture data that is stored on a target's computer, even if the target never sends the information over the Internet. RCS's capabilities include the ability to copy files from a computer's hard disk, record Skype calls, e-mails, instant messages, and passwords. Hacking Team advertises the RCS mechanism by which data gathered by the spyware is transmitted as "untraceable" to a specific government. The Citizen Lab through a series of tests located countries which are currently using their software to monitor its citizens and the Nigerian government is one of such.

6.3 FinFisher Command and Control Servers[4]

It has also been revealed, by Citizen Lab, that Nigeria has also joined the company of nations that have active FinFisher Command and Control servers. FinFisher

[3] Citizen lab: Mapping Hacking Team's "Untraceable" Spyware https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[4] Citizen Lab: For Their Eyes Only: The Commercialization of Digital Spying https://citizenlab.org/2013/04/for-their-eyes-only-2/

servers are designed with the sole purpose of helping governments with surveillance.

6.4 Outright Human Rights Violation

Sadly, a history of human rights violation on the use of social media already exists in Nigeria. An apt example is Tonye Okio[5], a former representative of the former governor of Bayelsa State, Timipre Sylva who was arrested and jailed over a Facebook comment he made. He was arrested and subsequently detained for 86 days without trial in a Bayelsa prison. He was later then charged under the offence "seditious publication". The matter is still in court.

7.0 Conclusion

The Nigerian government must understand the legal and socio-economic implications of the various threats to Internet Freedom and seek to, while combating security threats, find the right balance between privacy of its citizens and security of the nation. Citizen participation is needed to create a safe and free Internet, and government should not seek to intimidate individuals and organisations that bring these rights violations to the attention of all stakeholders.

[5] http://saharareporters.com/article/tonye-okio-president-jonathan's-critic-has-been-arrested-sabella-ogbobode-abidde