FREEDOM
ON THE NET
2015

Freedom
House

Nigeria

	2014	2015
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	15	15
TOTAL* (0-100)	**33**	**33**

* 0=most free, 100=least free

Population:	**177.5 million**
Internet Penetration 2014:	**43 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2015 Status:	**Partly Free**

Key Developments: June 2014 – May 2015

- The regulator shut down an SMS shortcode used by the All Progressives Congress opposition party to fundraise during the electoral campaign season in February 2015, which critics saw as politically motivated (see **Content Removal**).

- Digital activism played a significant role during the March 2015 general elections, helping candidate Muhammadu Buhari defeat incumbent President Goodluck Jonathan, who was widely criticized on social media for his inefficacy (see **Digital Activism**).

- In February 2015, a local Reuters correspondent was arrested on trumped-up allegations of espionage and planning to "send negative reports to the outside world," which observers believe was part of the government's efforts to obstruct international media from covering the general elections (see **Prosecutions and Detentions for Online Activities**).

- The Cybercrime Act 2015 signed into law in May 2015 includes provisions that threaten to violate citizens' rights to privacy (see **Surveillance, Privacy, and Anonymity**) and freedom of expression (see **Legal Environment**).

- The independent news outlet *Premium Times* experienced a DDoS attack during its presidential election coverage (see **Technical Attacks**).

Introduction

In 2014 and 2015, a growing number of Nigerians had access to the internet and other information and communications technologies (ICTs) due to an increase in mobile phone data services and improved broadband. Compared to the environment for traditional media in Nigeria, online media was relatively free from restrictions, with no blocking or filtering of online content reported during the coverage period.

Social media played a significant role during the general elections held in March 2015, providing a platform for digital activism that drew widespread attention to President Goodluck Jonathan's inefficacy. In response, government authorities tried to limit internet freedom in haphazard ways. In February 2015, for example, the regulator shut down an SMS shortcode used by the All Progressives Congress opposition party to fundraise during the electoral campaign season, which critics saw as politically motivated. Also in February, a local Reuters correspondent was arrested on trumped-up allegations of espionage and planning to "send negative reports to the outside world," which observers believe was part of the government's efforts to obstruct international media from covering the general elections. And in March, the independent news outlet *Premium Times* experienced a massive DDoS attack during its presidential election coverage. Meanwhile, an alarming number of violent attacks against traditional media journalists by both the Nigerian security forces and militant groups led online journalists to be more cautious than usual in their coverage of the elections.

Nigerian users remained concerned about growing online surveillance in the past year, even as the government continued its push to make ICT tools more available to citizens. Suspicions of the government's surveillance capabilities increased following the publication of leaked emails from the Italian surveillance company Hacking Team in July 2015, which revealed that the government of Bayelsa state had an active contract with the company from 2012 to November 2013. In May 2015, outgoing President Goodluck Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a long-awaited framework for addressing the country's notorious cybercrime epidemic. The law, however, includes provisions that threaten to violate citizens' rights to privacy and freedom of expression.

Obstacles to Access

Access to ICTs continued to grow, despite high costs and frequent power cuts that disrupt network services. There were no restrictions on connectivity, in contrast to the previous coverage period when mobile phone networks were cut off in three northeastern states due to emergency rule.

Availability and Ease of Access

The internet in Nigeria has continued to spread rapidly, particularly with the proliferation of mobile phone data and Fixed Wireless Access (FWA) services.[1] According to the Nigerian Communications Commission (NCC), the sector regulator, there were over 83 million active mobile internet subscriptions on GSM and CDMA networks as of February 2015.[2] The International Telecommunication Union

[1] Fixed Wire Access (FWA) is a type of high-speed internet access that uses radio signals as a connection to service providers instead of cables, enabling areas that lack fiber optic cables or DSL to access broadband internet.

[2] Nigerian Communications Commission, "Active Internet Subscriptions (GSM) and (CDMA)," accessed March 31, 2015, http://

(ITU) estimates that 43 percent of Nigerians had access to the internet in 2014, up from 38 percent in 2013,[3] while 78 percent had access to mobile phone services, increasing from 73 percent in 2013.[4] By contrast, the NCC reported a mobile phone teledensity of 102 percent as of February 2015.

Increasing access to the internet is driven by internet-enabled mobile handsets that provide affordable bundled data services to mobile subscribers. For example, as of April 2015, BlackBerry service packages cost as low as US$7.50 a month, an option that attracts many young Nigerians. As technologies improve, prices are continuing to decrease; in 2015, for example, the average cost of a GSM plan cost US$0.26 per megabyte of data, compared to US$1 per megabyte in 2011, while FWA services cost an average of US$37 per month, down from US$63 per month in 2014. Accessing the internet at a cybercafe costs about US$0.55 per hour, down from US$0.63 per hour. Nevertheless, these costs are still a major impediment to internet access for many Nigerians, particularly those in rural areas. In addition, the quality of service remains poor, with users frequently complaining about their inability to enjoy seamless data services. Internet speeds are slow, averaging 2.8 Mbps (compared to a global average of 4.5 Mbps), according to May 2015 data from Akamai's "State of the Internet" report.[5]

Power cuts frequently disrupt service and access, with many users reporting the need to use private generators to stay online during outages, despite the country's status as an oil-rich country.[6] In the first quarter of 2015, Nigerian households reportedly received an average daily cumulative power supply of between five and seven hours per day, leading over 77 percent of Nigerians to rely on alternative electricity sources.[7]

Telecommunication companies also depend on diesel-powered generators to maintain consistent service amid sporadic power cuts, spending an estimated NGN 177 billion (US$1.14 billion) annually on fuel for the generators needed to provide back-up power for the country's 22,000 base stations.[8] Moreover, the need to pay for expensive backup power generators has accelerated the closure of cybercafes that were already struggling with competition against the growing popularity of internet access on mobile devices.

Restrictions on Connectivity

Nigeria is connected to the international internet via a number of submarine fiber-optic cables, and there are several competing national fiber-optic backbone networks in place, representing a vibrant and competitive telecommunications market that is not highly vulnerable to government interference.[9]

Nevertheless, as part of an emergency directive imposed to fight Boko Haram in the northeastern

bit.ly/1kAqyVk.

[3] International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2013, http://bit.ly/1cblxxY.

[4] International Telecommunication Union, "Mobile-cellular subscriptions," 2000-2013, http://bit.ly/1cblxxY.

[5] Akamai, "Average Connection Speed: Nigeria," map visualization, *The State of the Internet Report Q4 2014*, http://akamai.me/1OqvpoS.

[6] Clara Nwachukwu, "Nigeria maintains lead in generator imports in Africa...," *Vanguard*, January 10, 2011, http://bit.ly/1RKDVPI.

[7] Andrew Airahuobhor, "67 percent Nigerians saw no power supply improvement in 2 years," *Daily Independent*, April 8, 2015, http://bit.ly/1EUlsvT.

[8] Amaka Eze, "Base Stations Gulp N178bn Worth of Diesel Annually," *This Day Live*, August 27, 2012, http://bit.ly/1eCdTdf.

[9] Henry Lancaster, *Nigeria – Broadband and Internet Market, Digital Economy*, BuddeComm, last updated July 8, 2014, http://bit.ly/1RdcXPL.

states of Borno, Adamawa, and Yobe, the former government under President Goodluck Jonathan deliberately cut off access to mobile phone networks between May and December 2013 and again in March 2014 for about 20 hours.[10] Residents complained of hardship due to the lack of telecommunications services and argued that the shutdown did little to stop the terrorist threat.[11] Instead, the shutdown at times put citizens in harm's way. For example, residents travelling to another city in search of mobile phone connectivity were reportedly ambushed and killed by Boko Haram militants.[12] In November 2014, the government sought a six-month extension for emergency rule in the region[13] but was rejected by both chambers of the National Assembly.[14]

ICT Market

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed internet service providers (ISPs) rising from 18 in 2000 to 189 as of the end of March 2015.[15] There are also 11 FWA providers[16] and 4 GSM mobile phone operators that provide internet access to their subscribers.[17] Nevertheless, the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access. As of February 2015, the four privately owned GSM companies—MTN, Globacom, Airtel, and Etisalat—had a total of over 136 million subscribers between them.[18]

Regulatory Bodies

The 2003 Nigerian Telecommunications Act vests regulatory responsibilities over the ICT sector in the Nigerian Communications Commission (NCC). Although the government nominates the NCC's nine-member board of commissioners, the regulator's decisions have been viewed as relatively independent. However, recent incidents—namely, the suspension of an SMS shortcode used for opposition fundraising during the election (see "Content Removal")—has called the regulator's independence into question.

All ISPs must obtain a license from the NCC to operate, and there have been no reports of any ISP being denied a license or registration renewal. However, new ISPs seeking to enter the market have faced stiff competition from larger ISPs and investor focus on the mobile sector. Meanwhile, the process of issuing GSM licenses is regarded as transparent. Unlike other auctions that are usually subject to political interference, most stakeholders have found GSM license auctions to be fair after those with political connections lost out in the process.

[10] "Nigeria Military Shuts Down Telephone Lines in Borno State," *CIO East Africa*, March 13, 2014, http://bit.ly/1RKEfOa; Ola' Audu, "Mobile networks restored in Borno," *Premium Times*, March 24, 2014, http://bit.ly/1q770VB; "Telecoms shutdown in Borno, Yobe, Adamawa disrupts Trade," *Daily Trust*, June 12, 2013, http://bit.ly/1k7YIkQ.

[11] "Military's shutdown of NE Nigeria telecoms disrupts trade," *IRIN News*, June 11, 2013, http://bit.ly/1NJVbWC.

[12] Ola' Audu, "Borno residents want phone network restored as Boko Haram gets deadlier," *Premium Times*, September 29, 2013, http://bit.ly/KhC8DS.

[13] "Jonathan writes National Assembly, requests extension of emergency rule in Borno, Adamawa, Yobe," *Premium Times*, November 18, 2014, http://bit.ly/1Hgzdp8.

[14] Chinenye Ugonna, "Nigerian Senate fails to extend emergency rule in northeast; summons military chiefs," *Premium Times*, November 19, 2014, http://bit.ly/1HGL7ry.

[15] 75 of which have licenses in need of renewal, according to the NCC website, which could mean that renewed license details have yet to be uploaded to the website, or that the regulator is in the process of renewing licenses. See: Nigerian Communications Commission, "Internet Services," accessed March 31, 2015, http://bit.ly/1bc1Urw.

[16] Nigerian Communications Commission, "Fixed Wireless Access," accessed December 31, 2013, http://bit.ly/1ckuLCB.

[17] Nigerian Communications Commission, "Digital Mobile License," accessed March 31, 2015, http://bit.ly/1HC9Z4Q.

[18] Nigerian Communications Commission, "Operator Data," accessed April 1, 2015. http://bit.ly/1Op2w9o.

Limits on Content

No blocking or filtering of online content was reported during the coverage period, though the communications regulator shut down an SMS shortcode used by an opposition party to fundraise during the elections period. The campaign season also saw an uptick in progovernment commentators who were suspected of deliberately manipulating the information landscape on social media networks. Hashtag activism became a highly influential tool for citizens to draw attention to important issues and demand government accountability.

Blocking and Filtering

Online media is generally free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or filtering of content. The complex nature of Nigeria's internet infrastructure makes it difficult to carry out systematic filtering or censorship.[19] Nonetheless, Blue Coat's PacketShaper appliance—a device that can help control undesirable traffic sent via online applications by filtering according to content category—was discovered in January 2013 on a private ISP in Nigeria,[20] which was disconcerting to observers given the use of Blue Coat technology by the authorities in countries such as China, Bahrain, and Russia. No abuses of the filtering device have been reported.

YouTube, Facebook, Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. In the past few years, however, a few high-level government officials have made statements calling for a clampdown on social media,[21] ostensibly as a response to the growing influence of critical commentary on the internet. Some citizens have viewed these statements as signs of impending online censorship.[22]

Content Removal

The government did not issue any takedown requests, nor did it force content to be removed from the internet during the coverage period. Nevertheless, with the rise of anti-gay sentiments following the passage of the repressive Same Sex Marriage (Prohibition) Act in January 2014, LGBTI individuals reported increasing concerns over having content related to sexual orientation and gay rights targeted for removal by the NCC. As such, many LGBTI content creators have opted to host their websites on platforms based in the United States and Europe to avoid potential censorship.[23]

[19] According to the last study by the OpenNet Initiative (ONI) conducted in 2007, several websites were inaccessible surrounding the 2007 presidential elections due to technical problems, not government intervention. OpenNet Initiative, "Nigeria," October 1, 2009, http://bit.ly/1j6ff5u; OpenNet Initiative, *Internet Watch Report: The 2007 Presidential Elections in Nigeria*, November 2007, http://bit.ly/L1rWjs.

[20] Discussion between a Freedom House consultant and Citizen Lab.

[21] On July 26, 2012, the President of the Senate of the Federal Republic of Nigeria, third in command after the president and vice president, called for a clampdown on the use of social media in Nigeria while speaking at a media retreat. Government representatives from the Oyo State House of Assembly made similar declarations in 2012. Phillip Eta, "Clamp down on Social Media now! "It is now an avenue for abusing government," – David Mark," *Daily Post,* July 28, 2012, http://bit.ly/1NeOwR3.

[22] Hauwa Gambo, "Get ready, guys: Legislator wants law against "abuse" of social media," *Naija,* November 2, 2012, http://bit.ly/1GfDV8T.

[23] "Publishing LGBTI content online is somewhat easier than in print media, but still poses challenges. Rashidi Williams explained, "If we want a website that talks about sexual orientation and gender identity, we can't find a local host for it because the Nigerian Communications Commission has a problem with it, so we have to have the website hosted by a U.S.-based platform that is outside the NCC's jurisdiction. If it is hosted in Nigeria, the NCC can find that host and tell them to take it down." PEN Nigeria, PEN America, Leitner Center, *Silenced Voices, Threatened Lives: The Impact of Nigeria's Anti-LGBT Law on Freedom of Expression,* June 29, 2015, http://bit.ly/1RddOjq.

In a murky case, the communications regulator in February 2015 shut down an SMS shortcode—a phone number with fewer digits to make it easier for users to remember—used by the All Progressives Congress opposition party to fundraise in the lead-up to the March 2015 general elections, claiming a violation of its established guidelines.[24] Though there was no evidence that the SMS shortcode block was politically motivated, Nigerian government agencies are known to align with the sitting president in order to retain the administration's favor. In a positive step, a Federal High Court ruled in favor of the opposition party in March and awarded NGN 500 million (US$ 2.5 million) as damages against the regulator "for unlawfully banning the party's presidential campaign fund-raising platform."[25]

Media, Diversity, and Content Manipulation

Nigeria is home to a diverse blogosphere, which has become an important platform for discussion and a source of reliable news for many users, providing a space for lengthy debate on a broad array of political and social issues among online commentators. Popular blogging platforms include Global Voices, Blogger, and WordPress.

Diverse political viewpoints are represented on Nigerian websites and blogs. Government efforts to manipulate online content are sporadic, though observers have noted a sharp increase in the volume of progovernment responses to citizens' comments on social media in recent years. In addition, the growing number of suspicious Twitter users that actively attack critical voices has led some to believe that the government may be financing an army of online trolls to influence the online information landscape. In November 2013, progovernment trolls were suspected of blocking links to articles posted on the Facebook page of the well-known investigative online news outlet, *Premium Times*, by repeatedly reporting the links as abusive. Efforts to unblock the *Premium Times*' links succeeded months later in January 2014.[26]

Users practice a degree of self-censorship online but have become more open in discussing issues that were previously unpopular or taboo, such as gay rights, in recent years. In Nigeria's growing anti-gay climate, however, many LGBTI individuals have reported feeling unsafe expressing themselves online using their real names and instead engage with the internet anonymously.[27] Online journalists were also more cautious than usual in their coverage of the March 2015 elections given the alarming number of violent attacks against traditional media journalists by both the Nigerian security forces and militant groups at the time.[28]

Digital Activism

As active social media users, Nigerians have increasingly initiated campaigns on social media to call for social or political change. Following the abduction of over 200 schoolgirls by Boko Haram

[24] Emmanuel Elebeke, "NCC justifies reason for shutting APC's sms platform," *Vanguard*, January 28, 2015, http://bit.ly/1FU7PJr.

[25] "Campaign Blockage: Court orders NCC to pay N500m damages to APC," *Premium Times*, March 24, 2015, http://bit.ly/1FU7Ug2.

[26] Peter Nkanga, "Attacks on critical Nigerian website highlight vulnerability," Committee to Protect Journalists (blog), March 11, 2014, https://cpj.org/x/59a8.

[27] *Silenced Voices, Threatened Lives: The Impact of Nigeria's Anti-LGBT Law on Freedom of Expression.*

[28] Peter Nkanga, "In election year, Nigeria's press feeling the pressure," Committee to Protect Journalists (blog), March 24, 2015, http://bit.ly/18X01gI.

in April 2014, the hashtag #BringBackOurGirls became an international social media campaign that put a spotlight on the Nigerian government's haphazard and ineffectual response to the crisis. The widespread attention on the government's inaction garnered by the campaign led to a dramatic drop in President Jonathan's already waning popularity, costing him in the 2015 elections. While the Jonathan government ultimately failed to rescue the abducted girls, the campaign illustrated how hashtag activism has become a highly influential tool for citizens to draw widespread attention to important issues, demand government accountability, and punish erring governments with defeat at the polls.

Violations of User Rights

The Cybercrime Act 2015 signed into law in May 2015 includes provisions that threaten to violate citizens' rights to privacy and freedom of expression. A Reuters correspondent was arrested in February 2015, which observers believe was part of the government's efforts to obstruct international media from covering the general elections. The independent news outlet Premium Times *experienced a DDoS attack during its presidential election coverage.*

Legal Environment

Nigeria's 1999 constitution guarantees freedom of expression and the press, and the implementation of Sharia (or Islamic) law in 12 northern states has not affected internet freedom in those regions to date. Nonetheless, libel remains a criminal offense in Nigeria and may be broadly applied to online content, with the burden of proof resting on the defendant. Print media journalists covering sensitive issues such as official corruption and communal violence are regularly subjected to criminal prosecution.

In May 2015, outgoing President Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a long-awaited framework for addressing the country's notorious cybercrime epidemic.[29] The law, however, includes provisions that threaten to violate citizens' rights to privacy (see "Surveillance, Privacy, and Anonymity") and freedom of expression. Under section 26 of the law, individuals can be criminally penalized for expressing or distributing "racist or xenophonic material to the public through a computer system or network" with up to five years in prison, a fine of up to NGN 10 million (US$50,000), or both.[30]

State government officials in Nigeria have also made efforts to restrict freedom of expression within their jurisdictions. In March 2013, for example, the governor of the southern state of Bayelsa introduced a bill to the state assembly that aimed to criminalize "rumor mongering" and the spread of false information.[31] While the bill remained stalled as of mid-2015, it did not deter the state governor from cracking down against alleged rumor mongering online, arresting one individual in October 2013 for a Facebook post criticizing the governor.[32]

[29] "Nigeria's President Jonathan Sign the Cybercrime Bill Into Law," *Techloy,* May 16, 2015, http://bit.ly/1RdeipQ.

[30] Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, http://bit.ly/1LHHhTh.

[31] "Governor Dickson Proposes Draconian Law Against Rumor Mongering," *Sahara Reporters*, March 21, 2013, http://bit.ly/1jr44I0.

[32] See Freedom House, "Nigeria," *Freedom on the Net 2014*, https://freedomhouse.org/report/freedom-net/2014/nigeria.

In an effort to codify protections for internet freedom, a coalition of civil society organizations released a draft Digital Rights and Freedom Bill in April 2015 to be introduced to the 8th National Assembly in 2015.

Prosecutions and Detentions for Online Activities

The Nigerian authorities occasionally arrest online journalists and ordinary users for their online activities. One arrest was reported during the coverage period.

On February 15, 2015, state security officers broke into the home of Reuters correspondent Tife Owolabi, arresting him on allegations of espionage and planning to "send negative reports to the outside world."[33] The authorities also seized his electronic devices—including cameras, laptops, hard drives, and an iPad.[34] Though he was ultimately released and dismissed of all charges, the timing of his arrest coincided with other government efforts to obstruct international media from covering the March 2015 elections.[35]

In September 2015,[36] a blogger was arrested for a Facebook post that accused the wife of the Ogun state governor of laundering money. With a case set for late October 2015, blogger Ojo Emmanuel faces charges of criminal libel and conspiracy against the state government.[37]

Surveillance, Privacy, and Anonymity

Thus far, there has been no evidence that the Nigerian authorities proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state. News of the government's acquisition of mass surveillance equipment over the past few years has deepened these suspicions. In July 2015, leaked emails from the Italian surveillance firm Hacking Team revealed that the company had a contract with the Bayelsa state government that expired in November 2013.[38] The active period of the contract from 2012 to 2013 coincides with the state governor's efforts at the time to crackdown on so-called "rumor mongering" online that led to the arrest of one Facebook user (see "Legal Environment").[39]

Earlier in April 2013, the online newspaper *Premium Times* published a report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria.[40] While the installation of the system was reportedly expected within

[33] Arodiegwu Eziukwu, "Nigeria's secret police accuse Reuters journalist of spying," *Premium Times*, February 16, 2015, http://bit.ly/1AAmRHn.

[34] Mike Odiegwu , "DSS ransacks home of Reuters correspondent in Bayelsa," *The Nation*, February 16, 2015, http://bit.ly/1yC0EYZ.

[35] "Al Jazeera detention clouds Nigerian election," *Aljazeera*, March 27, 2015, http://bit.ly/1BAfN99.

[36] Outside of coverage period.

[37] "Court Grants Bail To Nigerian Blogger Arrested Over Facebook Post On Ogun State Governor's Wife," *Sahara Reporters*, September 29, 2015, http://bit.ly/1RKGSzF.

[38] Ibukun Taiwo, "TL;DR: The Curious Case of Hacking Team And A Southern Nigerian State," *Tech Cabal*, July 17, 2015, http://bit.ly/1J8RYg4.

[39] Ogala Emmanual, "Nigeria: Hacking Team, Bayelsa's Govt's Internet Surveillance Contractor, Hacked," *Premium Times,* July 6, 2015, http://bit.ly/1GfmXYj.

[40] Ogala Emmanuel, "EXCLUSIVE: Jonathan awards $40 Million contract to Israeli company to monitor computer, Internet communication by Nigerians," *Premium Times*, April 25, 2013, http://bit.ly/SSZ0ij.

two years,[41] there has been no further news of the system's implementation as of October 2015. In April 2013, Citizen Lab research also found a FinFisher "Command and Control" server, which communicates with malware that can be used for surveillance, located on a private ISP.[42] As of mid-2015, the extent to which such surveillance systems have been implemented is still unknown.

Other government surveillance efforts were revealed in the publicly available summary of the federal government's 2014 budget proposal, which budgeted NGN 415 million (US$2.6 million) for a "Data Retention System," NGN 359 million (US$2.2 million) for a "GSM Passive Off-the-air Interception System," and NGN 350 million (US$2.2 million) for a "Strontium Sky Diligent Recon System" under the Directorate of State Security Services.[43] While the exact purpose of these technologies is still unclear, and it remains unknown whether the systems have been purchased and installed as of mid-2015, the budgeted expenses increased suspicions of the government's intent to enhance its surveillance capabilities, particularly amid frequent assertions by government officials of the need for technologies to fight the threat from Boko Haram.

Still under active discussion as of mid-2015,[44] a draft Lawful Interception of Communications Regulation, introduced by the communications regulator in February 2013,[45] has been criticized for bypassing the legislative process and lacking judicial safeguards against abuse or opportunities for redress, threatening to infringe on citizens' constitutional right to privacy.[46] If implemented, the regulation has conditions for interception both with and without a warrant and will require mobile phone companies to store voice and data communications for three years. It will also direct licensees to, on demand, "provide the National Security Adviser and the State Security Service with the key, code, or access to the Protected or Encrypted Communication."[47]

Meanwhile, requirements on service providers to retain user data and intercept electronic communications are included in the latest Cybercrime Bill, implemented in May 2015.[48] Under section 38 of the bill, providers are required to "keep all traffic data and subscriber information…for a period of two years" and comply with requests from law enforcement agencies to access this data.[49] Judicial oversight of these requirements is unclear.[50]

[41] Ogala Emmanuel, "EXCLUSIVE: Elbit Systems officials arrive; begin installation of $40 million Internet Spy facility for Nigeria," *Premium Times,* November 26, 2013, http://bit.ly/1GIOTP4.

[42] Morgan Marquis-Boire et al., *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab, April 30, 2013, http://bit.ly/1amNwJ1.

[43] Office of the National Security Adviser, "2014 FGN Budget Proposal," last accessed on January 11, 2014, http://bit.ly/1k81fLW.

[44] Paul Adepoju, "Nigeria: communications regulator to legalise interception," *Web Africa*, July 16, 2015, http://bit.ly/1RdfHN8.

[45] Nigeria Communications Commission, "Draft Lawful Interception of Communication Regulations," accessed April 15, 2015, http://bit.ly/1du7UKO; Ojo Madueke, "Revealed: SSS, Police Have Powers to Tap Phone Lines," *This Day Live*, January 30, 2013,http://bit.ly/1hH90GJ; Clement Ejiofor, "Mind That Conversation: Security Operatives To Tap Phones, Track E-mail," *Naij*, February 5, 2013, http://bit.ly/1VUWPsL; Ken Nwogbo, "SSS, Police Get Powers to Tap Phones," *Nigeria Communications Week*, January 29, 2013, http://bit.ly/1RdfTfd.

[46] Kunle Azeez, "Concerns over proposed lawful interception law," *National Mirror Online*, May 23, 2013, http://bit.ly/1kARPa1; Katie Collins, "Nigeria embarks on mobile phone surveillance project," Wired UK, September 4, 2013, http://bit.ly/1PvCpl2; John Dada and Theresa Tafida, "Online surveillance: Public concerns ignored in Nigeria," in *Communications Surveillance in the digital age 2014*, Global Information Society Watch, http://bit.ly/1PjVGXy.

[47] Nigeria Communications Commission, "Draft Lawful Interception of Communication Regulations."

[48] "Nigeria's President Jonathan Sign the Cybercrime Bill Into Law."

[49] Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 38.

[50] According to Section 38(4): "Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation ***or*** by an order of a court of competent jurisdiction" (emphasis added). Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, http://bit.ly/1LHHhTh.

The 2013 "Guidelines for the Provision of Internet Service" published by the NCC also require ISPs to cooperate with law enforcement and regulatory agencies in providing "any service-related information… including information regarding particular users and the content of their communications" during investigations of cybercrime or other illegal activity.[51] No details are provided in the guidelines regarding the oversight mechanisms required to prevent government authorities from acquiring free access to user information. The guidelines also stipulate that ISPs must retain user data and "the content of user messages or routing data" for at least 12 months.[52]

SIM card registration requirements instituted in June 2009 threaten users' rights to anonymous communication and privacy,[53] particularly in the absence of a data protection law.[54] Anonymity is also compromised by user registration requirements in cybercafes under the new Cybercrime Law passed in May 2015. Under Section 7 of the law, cybercafes must make their registers "available to law enforcement personnel whenever needed," with no clear measures for judicial oversight.[55] This provision follows an October 2013 directive from the regulator that requires cybercafes to register customers and "maintain an up-to-date database of subscribers and users, including their full names, physical addresses, passport photos, and telephone numbers," as part of the government's efforts to combat cybercrime.[56] The regulator was proactive in enforcing these requirements in 2014, finding 128 illegal cybercafes operating in Kano state without a license.[57]

Intimidation and Violence

Compared to print and broadcast journalists, online journalists and internet users have not been subject to significant extralegal intimidation or threats for their activities. The Nigerian authorities have a history of harassing and arresting traditional media workers, who faced greater restrictions and attacks by security forces and militant groups in the lead up to the March 2015 elections.[58] The precarious environment for Nigerian journalists is exacerbated by a culture of impunity for crimes against media workers.[59]

Online users are occasionally harassed by the authorities for their online activities. On May 5, 2014, the State Security Service visited the office of a prominent digital media freedom activist, 'Gbenga Sesan, after he had tweeted that citizens should hijack the hashtag for the 2014 World Economic Forum on Africa (#WEFAfrica) hosted in Nigeria to draw attention to the kidnapped Chibok girls and the #BringBackOurGirls campaign.[60] The authorities summoned and questioned Sesan for a few hours before releasing him in an effort that stemmed from concerns that Sesan was embarrassing the country with his tweets.[61]

[51] Nigerian Communications Commission, "Guidelines for the Provision of Internet Service," accessed December 11, 2013, 2, http://bit.ly/1hVbmA2.

[52] "Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission," 3.

[53] Nigerian Communications Commission and National Identity Management Commission, "Design, Development and Delivery of SIM Card Registration Solution," June 15, 2009, http://bit.ly/1clf91H.

[54] F. Franklin Akinsuyi, "Data Protection & Privacy Laws Nigeria, A Trillion Dollar Opportunity," Linkedin, April 15, 2015, http://bit.ly/1RdgvBs.

[55] Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 7.

[56] "NCC orders cyber cafes to register users," *Telecompaper*, October 22, 2013, http://bit.ly/1LPOk7w.

[57] Nigerian Communications Commission, *2014 Q4 Compliance Monitoring and Enforcement Report*, http://bit.ly/1G3bwyX.

[58] Nkanga, "In election year, Nigeria's press feeling the pressure."

[59] Committee to Protect Journalists, "Nigeria," *Getting Away With Murder*, October 8, 2015, http://bit.ly/1LPOGuF.

[60] "#WEFAfrica For #BringBackOurGirls," GS Speaks (blog), May 4, 2014, http://gbengasesan.com/?p=1317.

[61] Ogechi Ekeanyanwu, "SSS quizzes #BringBackOurGirls advocate," *Premium Times*, May 5, 2014, http://bit.ly/1EUFars; Bankole Oluwafemi, "Nigerian Secret Service Summons Gbenga Sesan," *TechCabal*, May 5, 2014, http://bit.ly/1EcnrNl.

Technical Attacks

Cyberattacks are common in Nigeria, though most attacks are against government websites and carried out by the Naija Cyber Hacktivists,[62] a group that has claimed responsibility for almost all cyberattacks to date. During the 2015 presidential elections, a new group calling itself the Nigerian Cyber Army hacked the website of the Independent National Electoral Commission (INEC),[63] claiming that it did so to ensure free and fair elections. One distributed denial of service (DDoS) attack against the independent news outlet *Premium Times* was reported during its presidential election coverage.[64]

[62] Daily Times, "EFCC & NCC Websites Hacked," *Naija Log* (blog), October 29, 2011, http://bit.ly/1amPau6.

[63] Micheal Abimboye, "INEC website hacked," *Premium Times*, March 28, 2015, http://bit.ly/1JSmnwX.

[64] Ogala Emmanuel, "How PREMIUM TIMES survived massive cyber attacks during presidential election coverage," *Premium Times*, April 5, 2015, http://bit.ly/1G41UH5.