Nigeria

<table>
<thead>
<tr>
<th>Internet Freedom Status</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partly Free</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obstacles to Access (0-25)</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Limits on Content (0-35)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Violations of User Rights (0-40)</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td>TOTAL* (0-100)</td>
<td>31</td>
<td>33</td>
</tr>
</tbody>
</table>

* 0=most free, 100=least free

Population: 173.6 million
Internet Penetration 2013: 38 percent
Social Media/ICT Apps Blocked: No
Political/Social Content Blocked: No
Bloggers/ICT Users Arrested: Yes
Press Freedom 2014 Status: Partly Free

Key Developments: May 2013 – May 2014

- Mobile phone services were shutdown in three northern states from May to December 2013 following the announcement of emergency rule in the region as part of a military strategy against the Boko Haram terrorist group (see Obstacles to Access).

- In November 2013, progovernment trolls were accused of blocking links to articles posted on the Facebook page of the well-known investigative online news outlet, Premium Times (see Limits on Content).

- Two individuals were arrested for posts on social media platforms: one in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page; the other in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service (see Violations of User Rights).

- The regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers (see Violations of User Rights).

- Suspicions of government surveillance increased following a November 2013 report about the installation of a mass surveillance system and revelations that the 2014 budget contained various earmarks for the purchase of specialized surveillance equipment (see Violations of User Rights).
Introduction

In 2014, access to the internet and other information and communications technologies (ICTs) continued to spread across the country due to the growth of mobile phone usage and data services. Public and private sector investments in ICT infrastructure and increased competition between service providers also played a key role. In May 2013, the Nigerian government approved a National Broadband Plan that aims to increase Nigeria’s broadband penetration five-fold by 2018. Nonetheless, the government deliberately impeded access to mobile phone networks in the northeastern states of Borno, Adamawa, and Yobe as part of a military strategy against the Boko Haram terrorist group in May 2013, imposing emergency rule and cutting off telecommunications in the region through December.

Compared to the traditional media sphere in Nigeria, online media is relatively free from restrictions, and no blocking or filtering of online content was reported during the coverage period. Self-censorship has noticeably declined since the January 2012 Occupy Nigeria protests, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights, in spite of the controversial anti-homosexuality law that passed in February 2014. Hashtag activism through social media campaigns such as #BringBackOurGirls in 2014 become a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability.

Nevertheless, observers suspected the government of trying to manipulate the online information landscape, pointing to the growing number of suspicious Twitter users who actively attack critical voices as evidence. 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 articles’ links as abusive. The news outlet also reported experiencing a massive DDoS attack against its website in January 2014.

Arrests of internet users increased in the past year, with two individuals arrested for posts on social media platforms. One individual was arrested in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page. The other was arrested in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service.

Meanwhile, Nigerian users became increasingly suspicious of online surveillance during the coverage period, even as the government continued its push to make ICT tools more available to citizens. Various legislative proposals were drafted in 2013 and 2014 that involve the interception of user communications, while the regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers. Suspicions of government intentions to monitor ICTs increased further following a November 2013 news report revealing the government’s contract with the Israel-based Elbit Systems to install a mass surveillance system by 2015.1 The publicly available summary of the federal government’s 2014 budget proposal also included various earmarks for the procurement of specialized surveillance equipment.

---

Obstacles to Access

The internet in Nigeria has continued to spread rapidly, particularly with the proliferation of mobile phone data and Fixed Wireless Access (FWA) services. In 2013, internet penetration stood at 38 percent, up from 33 percent in 2012, according to the International Telecommunication Union (ITU). Mobile phone teledensity also increased from 86 percent in May 2013 to 92 percent in April 2014, as reported by the Nigerian Communications Commission (NCC), while the ITU indicated a mobile phone penetration rate of 73 percent in 2013, up from 67 percent in 2012.

Increasing access to the internet has been driven in large part by internet-enabled mobile handsets that provide affordable bundled data services to mobile subscribers. For example, as of January 2014, BlackBerry service packages cost as low as US$17 a month, an option that attracts many young Nigerians. Competition, helped by the Mobile Number Portability initiative launched in April 2013, has forced service providers to offer cheaper plans based on time (daily, weekly, or monthly) or use (for social media or messaging). According to the NCC's Internet Subscriber Data reports, there were about 66 million active internet subscriptions on GSM and CDMA networks in Nigeria in April 2014, while the ITU noted a mobile-broadband penetration rate of 10 percent in 2013. Nevertheless, the quality of service remains poor, with users frequently complaining about their inability to enjoy seamless data services.

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. Internet speeds are still slow, however, averaging 1.9 Mbps (compared to a global average of 3.9 Mbps), according to May 2014 data from Akamai’s “State of the Internet” report. In addition, Nigeria’s broadband adoption (characterized by connection speeds greater than 4 Mbps) was about 5 percent, while the country’s narrowband adoption (connection speed below 256 kbps) was 4 percent. Although many providers use the word “broadband” in their promotional materials, in practice there is limited broadband service.
available in Nigeria. A mere 0.1 percent of Nigerians had access to fixed-broadband internet in 2013, representing just over 15,000 subscriptions.\textsuperscript{12}

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed ISPs rising from 18 in 2000 to 156 (55 of which have licenses in need of renewal\textsuperscript{13}) by the end of 2013. There are also 11 FWA providers,\textsuperscript{14} and five GSM mobile phone operators that provide internet access to their subscribers.\textsuperscript{15} Nevertheless, the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access. As of September 2013, the four privately-owned GSM companies—MTN, Globacom, Airtel, and Etisalat—had a total of over 118 million subscribers among them.\textsuperscript{16}

Recognizing the importance of ICTs for economic development, the communication ministry released the National Broadband Plan (2013-2018) in May 2013, which was approved by the president shortly thereafter.\textsuperscript{17} In accordance with the National Broadband Plan, the telecommunications regulator announced that it planned to auction a 2.5 GHz frequency spectrum by March 2014\textsuperscript{18} and license seven Infrastructure Companies (InfraCos) by December 2014.\textsuperscript{19}

In the meantime, access to ICTs in Nigeria is characterized by a large urban-rural divide. According to a May 2014 Gallup survey of 4,000 adults across the country, 34 percent of urban Nigerians had used the internet in the last week, compared to 22 percent of rural Nigerians.\textsuperscript{20} Similarly, 89 percent of urban Nigerians reported owning a mobile phone, compared to 79 percent of rural Nigerians, though the gap between urban and rural mobile phone owners is narrowing. In 2012, the same Gallup survey in Nigeria found that 70 percent of rural Nigerians owned a mobile phone, compared to 85 percent of urban Nigerians.

High costs are another major impediment to internet access. While increased competition among service providers has made the cost of access more affordable, the country's median annual per capita income stood at US$493 in 2013.\textsuperscript{21} FWA services cost an average of US$63 per month, while the price for internet use in a cybercafe can cost about US$0.63 per hour. As technologies expand, however, prices are continuing to decrease; in 2013, for example, the average cost of a GSM plan cost US$0.05 per megabyte of data, compared to US$1 per megabyte in 2011.

\begin{enumerate}
\item International Telecommunication Union, “Fixed (Wired)-Broadband Subscriptions, 2000-2013.”
\item 55 Internet service providers have expired licenses 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 December 31, 2013, http://bit.ly/1dO6p5e.
\end{enumerate}
In addition to cost, power cuts continued to disrupt service and access, with many users reporting the need to use private generators to stay online during outages. The country’s electricity supply saw major disruptions 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. To address the country's inadequate power supply, the federal government took an unprecedented step in November 2013 and handed over its state monopoly of the power sector to private investors. The private sector is expected to revitalize the nation's power supply, though the impact of this endeavor will take years to come into effect.

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. 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 via mobile devices.

The government deliberately cut off access to mobile phone networks in the northeastern states of Borno, Adamawa, and Yobe in May 2013, ostensibly as part of a military strategy against the Boko Haram terrorist group in the region. Residents complained of hardship due to the lack of telecommunications services and argued that the imposed shutdown did not help the government stop the terrorist threat. Instead, the shutdown at times put citizens in harm's way. In September, for example, residents travelling to another city in search of mobile phone connectivity were reportedly ambushed and killed by Boko Haram militants.

Phone lines were restored months later in December but were cut off again in March 2014 for about 20 hours.

Internet services are managed by the 2003 Nigerian Telecommunications Act, which vests regulatory responsibilities 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. 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 challenges in their operations due to competition from larger ISPs and investor focus on the mobile sector. Meanwhile, the process of issuing GSM licenses has been regarded as transparent. Unlike similar auctions that have been subject to political...

---

interference, most stakeholders found the first and subsequent GSM license auctions to be fair, as friends of prominent politicians, who are usually recipients of such licenses, lost out in the process.

**Limits on Content**

No blocking or filtering of online content was reported during the coverage period, though progovernment trolls were suspected of manipulating the information landscape on social media networks. Hashtag activism became a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability.

Online media is generally free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or filtering of content, mainly due to the complex nature of Nigeria’s internet infrastructure, which makes it difficult to carry out systematic filtering or censorship. Some ISPs have been known to block access when users infringe on laws by downloading copyrighted content, but this has often been done to manage network traffic rather than to protect intellectual property. 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, which was disconcerting to observers given the use of Blue Coat’s monitoring and filtering equipment in authoritarian countries such as China, Bahrain, and Russia.

The video-sharing website YouTube, social-networking site Facebook, microblogging application Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. According to the website rating company Alexa, the ten most popular websites in Nigeria in 2013 were Google, Google Nigeria, Facebook, Yahoo, YouTube, Blogspot, Nairaland, Twitter, the **Vanguard** and LinkedIn. Five other Nigerian websites were cited in the top 20, including **Lindaikeji**, a gossip news site; **Punch** newspaper; and **Jumia**, an eCommerce website.

Meanwhile, websites, blogs, and online commentators are generally divided among those with antigovernment, progovernment, and neutral leanings. Web commentary is generally balanced, with online commentators having more discussions on socioeconomic issues than polarized debates. Online self-censorship has declined notably in the past few years, and people now freely discuss issues that were previously unpopular or taboo, such as gay rights, in spite of the repressive anti-homosexuality law passed in February 2014. Criticism of the government on social media has also increased, as have responses from government representatives.

Government efforts to manipulate online content are sporadic in Nigeria, though observers have noted a sharp increase in the volume of progovernment responses to citizen comments on social

---


31 Discussion between a Freedom House consultant and Citizen Lab.

32 As of December 2013, there were over eleven million Facebook users. Based on Facebook advertising data accessed by author on December 31, 2013.

media in recent years. In addition, the growing number of suspicious Twitter users who 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, pro-government 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 articles’ links as abusive. Efforts to unblock the *Premium Times*’ links succeeded months later in January 2014.  

Another case of suspected pro-government manipulation surfaced in March 2014 when it was discovered that the president’s special adviser on new media, Reno Omokri, had tried to plant a story in the media with the pseudonym Wendell Simlin. According to reports, Simlin had sent an email to journalists with a Microsoft Word attachment that accused the suspended governor of the Central Bank, Lamido Sanusi, of sponsoring the terrorism group Boko Haram, shortly after Sanusi accused the government of corruption, which led to his subsequent suspension. Digital activists linked the random Wendell Simlin to the president’s new media adviser when Reno Omokri’s name was found listed as the email’s author in the attached document’s properties.

In the past few years, high-level government officials have made numerous statements calling for a clampdown on social media, ostensibly as a response to the growing influence of critical commentary on the internet, which drew reactions from citizens who viewed these statements as signs of impending online censorship. While the government denied any intent to restrict social media, it seems determined to create its own social media tools, as indicated by Nigeria’s 2013 budget proposal in which the information ministry had made provisions to spend NGN 100 million (US$623,000) for “developing social media platforms and networking with other platforms.” The information ministry proposed NGN 50 million (US$312,500) for the same project in 2014, along with an additional NGN 7 million (US$43,750) for the “integration of social media platform collaboration including secured WAN.”

There has also been some government interference in the economic aspects of online news publishing, though overt incidents have not been recorded in the past few years. In 2011, the

---

leading critical online newspaper, 234Next, folded in part due to a refusal to provide advertising by government or progovernment businesses. As the country gears up for national elections in 2015, government patronage is still evident and reputed to be the largest source of business contracts that companies depend on for financial sustainability.

Nonetheless, Nigeria is home to a diverse blogosphere, with entertainment blogs drawing the most readers and a growing number of Nigerians blogging about their personal lives or social issues. Blogs have gradually emerged as an important platform for discussion and a source of reliable news for many users, providing a space for lengthy debate among online commentators. Readers often leave comments on popular news-oriented blogs to express frustration with societal issues. The Nigerian blogosphere includes both expatriates and locally-based writers, and popular platforms on which Nigerian bloggers interact and learn from one another include Global Voices, Blogger, and WordPress. The president's Facebook page is a major platform on which citizens comment on public issues, and Twitter plays a prominent role in debates around events as they happen, with government ministers often hosting Twitter chats with the public. The formal chats were less frequent in 2013 and 2014, but ministers continued to use social media directly, employing media aides to comment on issues that concern them.

In addition, ICTs are playing an increasingly important role in mobilizing people for protests and providing updates on unfolding events. Citizens are more active on social media and increasingly believe that campaigns initiated on social media can lead to change. Online citizen activism in Nigeria was particularly evident in 2013-2014, as demonstrated by an incident involving allegations of corruption against a serving minister. On October 28, 2013, Punch newspaper published an editorial that criticized the president for not acting on the widespread calls for the dismissal of aviation minister Stella Oduah, who had allegedly used public funds to purchase bullet-proof vehicles for her personal use. The allegations elicited nationwide outrage to the story, especially on social media where “Oduah-gate” became a popular topic. While many assumed that the scandal would join the growing list of unresolved corruption cases in Nigeria, social media users kept the discussion alive, which played a large part in the government's decision to indict Oduah in January 2014.

In another showcase of online activism in Nigeria, the governor of Edo State was compelled to act upon criticisms against him on social media when a video of him insulting a woman selling wares on the roadside was posted online in November 2013. The video, which depicted the governor telling the woman to “go and die” in response to her plea against his inspection of her sale of allegedly illegal wares, became popular on social media and sparked an online campaign on the subject of human dignity. The ensuing online discussions and fundraising for the widow led the governor to issue a formal apology, invite the woman to his office, offer her a job, and donate NGN 2 million to her family—gestures that were all publicized on social media.

The most notable social media activism in 2014 was spurred by the horrific kidnapping of over 200

---

schoolgirls by the Boko Haram terrorist group in April. The hashtag #BringBackOurGirls became an international social media campaign that put a spotlight on the Nigerian government and its inadequate efforts to take action. Foreign governments eventually pledged support to help locate the girls, but as of this report's writing in mid-2014, the rescue mission was still ongoing.

Nonetheless, the #BringBackOurGirls campaign illustrated how hashtag activism has become a highly influential tool for citizens to draw widespread attention to important issues and demand government accountability. In April 2014, one hashtag campaign, #FreeCiaxon, launched following the disappearance of a man who had live-tweeted the scene of an attempted jailbreak in Abuja (using the Twitter handle @ciaxon), led to the man’s eventual release by the authorities who had covertly detained him (see “Violations of User Rights”).

### Violations of User Rights

Various legislative proposals were drafted in 2013 and 2014 that involve the interception of user communications, while the regulator announced a new directive in October 2013 requiring cybercafes to register customers and maintain an up-to-date database of subscribers. Two individuals were arrested for posts on social media platforms: one in October 2013 for allegedly criticizing the governor of Bayelsa state on his Facebook page; the other in March 2014 for live-tweeting an incident involving Boko Haram militants and the State Secret Service. Suspicions of government intentions to monitor ICTs increased further following a November 2013 news report revealing the government’s efforts to install a mass surveillance system by 2015.

Nigeria’s 1999 constitution guarantees freedom of expression and of the press, and the lack of internet-specific legislation has generally fostered an open environment for online activities. Nonetheless, the country’s legal framework was revised in 2011 to reflect the use of new media technologies through Section 84(1) of the 2011 Evidence Act, which provides for the admission of statements in documents produced by computers and electronic signatures as evidence in court. Libel also remains a criminal offense in Nigeria, 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. Meanwhile, the implementation of Sharia (or Islamic) law in 12 northern states has not affected internet freedom to date.

There are currently no laws in Nigeria that specifically restrict online speech, though a draft bill on electronic transactions and fraud detection proposed in 2011 did include a provision that sought to punish online speech regarded as “false information that could threaten the security of the country or that is capable of inciting the general public against the government through electronic message” with heavy fines, up to seven years in prison, or both. Following public backlash against the draconian provision, especially on social media, the senate announced that the controversial clause would be deleted from the proposed bill in December 2013.

---

In addition to national legislative initiatives, state government officials in Nigeria have made efforts to restrict freedom of expression within their jurisdictions. In March 2013, for example, the governor of the southern state of Bayelsa, Seriake Dickson, introduced a bill to the state assembly that aimed to criminalize “rumor mongering” and the spread of false information. While the bill is still under consideration as of mid-2014, it has not deterred Governor Dickson from cracking down against alleged rumor-mongering online.

Notably, on October 26, 2013, known businessman Tonye Okio was arrested in Abuja, blindfolded, and driven to Bayelsa State by the Nigeria Police’s Special Investigation Bureau for allegedly criticizing the governor of Bayelsa on his Facebook page. The police also reportedly seized Okio’s electronic gadgets and deleted the critical posts about the Bayelsa governor from his Facebook account. He was held for 10 days without trial and subsequently granted bail under politically-motivated conditions that were “impossible” to meet, requiring an agent of the complainant to stand as Okio’s surety for the bail. Okio later was released on January 22, 2014 after spending three months in prison. He was reportedly one of several victims of the Bayelsa state government’s proposed rumor mongering law.

In another notable incident during the coverage period, a Twitter user (@ciaxon) was covertly detained in March 2014 after he live-tweeted a series of photos depicting the attempted escape of suspected Boko Haram members who were being held at a State Secret Service (SSS) facility. His photos were picked up by media outlets covering the story, leading to suspicions that the SSS was behind his disappearance. Large-scale protests initiated by the hashtag campaign, #FreeCiaxon, elicited international attention and ultimately led to his release 12 days later.

SIM card registration requirements instituted in June 2009 impose restrictions on users’ rights to anonymous communication. In addition, a new directive announced by the regulator in October 2013 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.\textsuperscript{60} As of mid-2014, there have been no reports that the new registration requirements have been enforced, and it remains unclear whether the authorities need a court order to gain access to customer information from cybercafe records.\textsuperscript{61}

In February 2013, the NCC introduced a new draft Lawful Interception of Communications Regulation.\textsuperscript{62} Still under discussion as of mid-2014, the regulation was criticized for potentially infringing on the constitutional right to privacy, in addition to a lack of safeguards against abuse or opportunities for redress, and unclear supervisory and reporting provisions.\textsuperscript{63} If implemented, the bill 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 “provide the National Security Adviser and the State Security Service with the key, code or access to the Protected or Encrypted Communication.”\textsuperscript{64}

Meanwhile, throughout 2013 and 2014, the National Assembly began discussing other proposed laws that also address the subject of lawful interception, such as the Oral and Written Communications Tracking Bill, Regulation of Telecommunication Facilities to Support Investigations Bill, Electronic Fraud Prohibition and Electronic Transfer of Funds Crime Bill,\textsuperscript{65} the Interception of Communications Bill, and the Cybercrime Bill.\textsuperscript{66} Though most of the draft bills—all still under discussion as of mid-2014—require security agencies to obtain a court order before they can conduct surveillance activities, warrants are generally easy to obtain in the context of Nigeria’s nominally independent judiciary.

Meanwhile, ISPs are currently required 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, according to the “Guidelines for the Provision of Internet Service” published by the NCC.\textsuperscript{67} 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.\textsuperscript{68}


\textsuperscript{64} Nigeria Communications Commission, “Draft Lawful Interception of Communication Regulations.”


\textsuperscript{67} “Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission,” accessed December 11, 2013, 2 http://bit.ly/1hVBMa2.

\textsuperscript{68} “Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission,” 3.
Thus far, the Nigerian security services have not appeared to proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state, and the government’s recent acquisition of mass surveillance equipment has deepened these suspicions. In April 2013, the online newspaper *Premium Times* published a news report revealing that the federal government had awarded a secret contract to Israel-based Elbit Systems to help monitor internet communications in Nigeria. A civil society organization working on ICT Policy, Paradigm Initiative Nigeria, made a Freedom of Information (FOI) request on the contract in May 2013, but to no avail, eliciting a lawsuit that was subsequently dismissed by a judge in a widely criticized ruling. In August 2013, a local anti-corruption organization accused the judge of bias based on his apparent pattern of opposition to rights-focused suits.

Evidence of government plans to implement a surveillance system was further corroborated by publicly available details of Nigeria’s 2013 budget, in which the Office of the National Security Adviser requested US$61 million for a “wise intelligence network harvest analyzer system, open source internet monitoring system, personal internet surveillance system.” 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. As of mid-2014, the extent to which such surveillance systems have been implemented has yet to be established, though in November 2013, *Premium Times* reported that Elbit Systems staff was in Nigeria and working to complete the mass surveillance system within two years.

Meanwhile, in the publicly available summary of the federal government’s 2014 budget proposal, the Directorate of State Security Services listed plans to spend NGN 415 million (US$2.6 million) on a “Data Retention System,” NGN 359 million (US$2.2 million) on a “GSM Passive Off-the-air Interception System,” and NGN 350 million (US$2.2 million) on a “Strontium Sky Diligent Recon System.” The Office of the National Security Adviser similarly proposed NGN 11 billion (US$68.8 million)—more than its total budget on mass surveillance equipment in 2013—on its ongoing “Enhanced and Specialized Security Equipment, Gadgets and Services” project, and another NGN 5.2 billion on an unexplained “Security Program for Federal Courts.” While the exact purpose of these technologies is still unclear, the planned 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 Boko Haram threat.

Online journalists and internet users have not been subject to significant extralegal intimidation or threats for their activities, though the state is known to target journalists in the traditional media with arbitrary and extralegal measures to suppress political criticism. The Nigerian authorities have a
history of arresting and intimidating traditional media workers, and at least ten journalists have been killed in connection with their work since 1998. In addition, there is a culture of impunity for crimes against media workers.

Cyberattacks have increased in Nigeria, though most of the attacks are against government websites and carried out by the Naija Cyber Hacktivists, a group that has claimed responsibility for almost all cyberattacks to date. One DDoS attack against an independent news outlet known for its critical coverage of the government, *Premium Times*, was reported in January 2014.

---

