Nigeria

Key Developments: June 2016 – May 2017

- Digital activism was vibrant, with one campaign succeeding in increasing the National Assembly’s budgetary transparency (see Digital Activism).

- The Digital Rights and Freedom Bill passed a second reading in June 2016 and is one step closer to becoming law (see Legal Environment).

- Numerous bloggers, online journalists, and ordinary users were arrested for their online activities in the past year, most of whom were charged for “cyberstalking” under Section 24 of the cybercrime law, though no cases led to convictions (see Prosecutions and Detentions for Online Activities).

- Online journalists and internet users in Nigeria were subject to increasing extralegal harassment and intimidation for their activities (see Intimidation and Violence).
Introduction

Internet freedom in Nigeria remained stagnant in the past year amidst an ongoing trend of intimidation and arrests for online criticisms against government officials. Online censorship was not an issue, and digital activism pushed for greater government transparency.

Nigeria has a vibrant, savvy, and growing internet user population, enabled by a strong and innovative technology sector. Compared to the environment for traditional news media in Nigeria, online media is relatively free from restrictions, with no blocking or filtering of online content reported during the coverage period. A robust civil society has helped protect and enhance internet freedom for Nigerians, as demonstrated by significant advocacy efforts to codify protections for Nigeria’s internet freedom in the Digital Rights and Freedom Bill 2016, which as of 2017, is one step from passage at the House of Representatives.

Despite the progress observed, a cybercrime law passed at the end of former President Goodluck Jonathan’s tenure in May 2015 led to the arrest of several bloggers and online journalists on charges of “cyberstalking” for online writings that criticized government officials and powerful businesspeople. At least seven arrests were documented during this report’s coverage period with no indication of subsiding throughout 2017. Intimidation and harassment for online expression also became more common.

Obstacles to Access

Access to information and communications technologies (ICTs) continued to grow, despite high costs and frequent power cuts that disrupt network services. The government continued to work towards achieving its 30 percent target for broadband penetration in its National Broadband Plan (2013-2018).

Availability and Ease of Access

<table>
<thead>
<tr>
<th>Key Access Indicators</th>
<th>2016</th>
<th>2015</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet penetration (ITU)(^a)</td>
<td>25.7%</td>
<td>47.4%</td>
<td>13.8%</td>
</tr>
<tr>
<td>Mobile penetration (ITU)(^b)</td>
<td>82%</td>
<td>82%</td>
<td>58%</td>
</tr>
<tr>
<td>Average connection speeds (Akamai)(^c)</td>
<td>3.9 Mbps</td>
<td>3.3 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

\(^c\) Akamai, “State of the Internet - Connectivity Report, Q1 2017,” https://q0o.qi/TQH7L7

The government’s National Broadband Plan (2013-2018) has set a 30 percent target for broadband penetration, which the country has made incremental progress toward achieving. With over 89 million citizens online, Nigeria has one of the largest internet user populations in sub-Saharan Africa. According to latest data from the International Telecommunications Union (ITU), Nigeria’s internet...
NIGERIA

penetration rate was 26 percent in 2016, up from 25 percent in 2015. Most of the growth in internet use can be attributed to the proliferation of mobile phone services. According to the Nigerian Communications Commission (NCC), the sector regulator, mobile phone teledensity in Nigeria stood at 108 percent, while there were almost 90 million active mobile internet subscriptions on GSM networks as of March 2017. The ITU documented a lower mobile phone penetration rate of 82 percent in 2016. Internet speeds are still slow, averaging 4.1 Mbps (compared to a global average of 7.0 Mbps), according to Akamai’s “State of the Internet” report.

Increasing access to the internet is driven by affordable data services for mobile subscribers. The Alliance for an Affordable Internet ranked Nigeria the 13th most affordable internet environment among 58 developing and emerging countries assessed in its 2017 Affordability Drivers Index. As of May 2017, mobile internet plans have become very popular, with 1.5 gigabyte of data available for USD $3.28. In 2017, the average cost of a GSM plan was USD $0.02 per megabyte of data, compared to $0.05 per megabyte in 2016, $0.26 per megabyte in 2015, and $1.00 per megabyte in 2011. Nevertheless, costs are still a major impediment to internet access for many Nigerians in rural areas.

In March 2016, the government introduced the Communication Service Tax Bill 2015 which, if passed, will decrease the affordability of internet access by imposing a 9 percent tax on consumers for communications services, such as SMS, data, and voice services. The bill was still under consideration in 2017 despite its unpopularity among various stakeholders.

Power cuts frequently disrupt service and access, despite Nigeria’s status as an oil-rich country. Nigerian households reported slight improvements in electricity access the past year, receiving an average of ten hours of power supply per day in February 2017, up from less than six hours the previous year. Those with the financial wherewithal are able to rely on private generators and standby battery-powered inverter systems to stay online during outages.

Shortfalls in power supply also undermine the quality of internet service offered by providers. Telecommunications base stations in Nigeria are typically powered by diesel generators, which reportedly account for 80 percent of their operating expenses. Separately, the need to pay for expensive backup power generators has accelerated the closure of cybercafés that were already struggling with competition against the growing popularity of internet access on mobile devices.

Nigeria’s internet user landscape is characterized by a significant digital gender divide: October 2015

NB: The ITU’s dataset in 2016 retroactively revised the timeseries internet penetration data for Nigeria with no explanation. Penetration for 2015 was recorded at 47 percent.
6 Sharp reduction of average cost of GSM plan reduced only in dollar terms because of currency devaluation.
9 Compared to a mere 5% in Malawi where power from the grid is stable. See, Association of Telecommunication Companies of Nigeria: http://bit.ly/1Uc58Pb.
research by the Web Foundation and Paradigm Initiative found that poor women in Nigeria’s largest city, Lagos, were 50 percent less likely to have access to the internet than men of the same age, education, and income level.\textsuperscript{10}

Another major obstacle to internet access in Nigeria is language literacy. Home to over 500 local languages,\textsuperscript{11} most internet content is in English, and local language content is vastly underrepresented. For example, the Wikipedia pages in the three major Nigerian languages of Yoruba, Hausa, and Igbo are sparsely developed, and in many instances, Wikipedia entries on Nigerian topics are edited by editors not residing in Africa.\textsuperscript{12} Local language resources, such as audio and video health and educational material, come with higher data requirements, potentially limiting access for users who can afford less data yet who stand to benefit the most from educational materials online.

Restrictions on Connectivity

There were no restrictions on connectivity to the internet or mobile networks during the coverage period. Mobile network restrictions were last reported in 2014 and 2015 in three northern states of Nigeria during a state of emergency in the fight against Boko Haram.

The backbone connection to the international internet is decentralized, resulting in a climate of healthy competition with little government interference. Multiple players have built fiber networks that crisscross the country, including Phase 3, Glo 1, Suburban Telecom, Multilinks and MTN. There are three active Internet Exchange Points (IXPs).\textsuperscript{13}

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 82 as of May 2017, though the growth of ISPs and Fixed Wireless Access (FWA) providers has slowed in recent years with the rise in mobile access.\textsuperscript{14} Five privately owned GSM mobile phone operators also provide internet access: MTN, Glocom, Airtel, Etisalat, and NTEL, which began operations in February 2016 after acquiring the license of the defunct First National Operator, NITEL.\textsuperscript{15} In January 2016, MTN acquired Visafone, securing access to its 800MHz spectrum as a possible precursor to the launch of 4G LTE service.\textsuperscript{16} Cybercafés (or telecentres) are required to obtain licenses, but the large number of unlicensed cybercafés in operation suggest that the regulator has not enforced the requirement.\textsuperscript{17}

\textsuperscript{11} Nigerian languages, http://www.onlinenigeria.com/languages/languages.asp
\textsuperscript{14} 205 licenses are listed but only 82 of them have licenses that are valid as at May 24, 2017. See: Nigerian Communications Commission, “Internet Services,” accessed May 24, 2017, http://bit.ly/1U0Khi4
\textsuperscript{17} National Communications Commission, “Class License Register: Telecenter/Cybercafe Category,” NCC, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=718&Itemid=
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. The regulator’s current CEO and Executive Vice Chairman was appointed in August through a process that was viewed as fair, particularly considering the CEO’s background as a leading academic and industry expert.18

Limits on Content

Online censorship was not reported during the coverage period. Digital activism remained vibrant, with one campaign succeeding in increasing the National Assembly’s budgetary transparency.

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. YouTube, Facebook, Twitter, WhatsApp, and other communications platforms are freely available and among the most popular websites in the country.19 The complex nature of Nigeria’s internet infrastructure makes it difficult to carry out systematic filtering or censorship.

In the past few years, however, a few high-level government officials have called for a clampdown on social media in response to the growing influence of critical commentary on the internet, sparking fears of impending online censorship.20 Legislative proposals have added weight to those fears. The Frivolous Petitions Prohibition Bill introduced in 2015 sought to penalize expression on social media, though it was withdrawn in May 2016. Meanwhile, the Cybercrime Act, which was signed into law in May 2015, has been used to arrest bloggers for critical content in the past year (see Legal Environment and Prosecutions and Detentions for Online Content).

Content Removal

The government did not issue any takedown requests, or force legitimate content to be removed from the internet during the coverage period.

Media, Diversity, and Content Manipulation

Nigeria is home to a diverse blogosphere, which has become a source of reliable news for many users, and provides space for lengthy debate on a broad array of political and social issues. Popular

---

blogging platforms include Medium, Blogger, and WordPress. Diverse political viewpoints are represented on Nigerian websites and blogs, though some independent online media outlets faced a backlash under previous governments.

Government manipulation was not reported during the period but as the 2019 elections approach, observers worry that online propaganda and manipulation could be employed to gain a political advantage among voters.

The ongoing prevalence of arrests for online commentary under the 2015 Cybercrime Law has resulted in increasing self-censorship, particularly among professional journalists who also publish content online (see Prosecutions and Detentions for Online Activities). Nigeria’s LGBTI (lesbian, gay, bisexual, transgender, and intersex) community is marginalized, and many LGBTI individuals report feeling unsafe using their real names online, preferring to engage anonymously.22

Digital Activism

As active social media users, Nigerians have become prolific digital campaigners, innovatively using social media and communications apps to call for social or political change. The savviness of Nigeria’s digital activists led to significant internet freedom success stories in the past, including the defeat of the Frivolous Petitions Prohibition Bill, or the so-called social media bill, in 2016. Among its goals, the bill sought to constrain critical expression on social media.23

During this report’s coverage period, activists led an online campaign tagged #OpenNASS that called on the country’s National Assembly to increase the transparency of its hitherto opaque budget. The social media campaign successfully pushed the assembly to present its legislative budget as line items with detailed allocations for budget items.24

Violations of User Rights

Numerous bloggers, online journalists, and ordinary users were arrested for their online activities in the past year, most of whom were charged for “cyberstalking” under Section 24 of the cybercrime law, though no cases led to convictions. Online journalists and internet users in Nigeria were subject to increasing extralegal harassment and intimidation for their activities. The Digital Rights and Freedom Bill passed a second reading in June 2016 and is one step closer to become law.

Legal Environment

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

---


Before leaving office in May 2015, former President Goodluck Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a framework for addressing the country’s notorious cybercrime epidemic.\(^{25}\) The law, however, includes provisions that violate citizens’ rights to privacy (Section 38, see Surveillance, Privacy, and Anonymity) and freedom of expression. Duplicating existing libel laws, Section 24 of the law penalizes “cyberstalking” or messages that are “false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another” with up to three years in prison, a fine, or both. Section 26 penalizes distribution of “racist or xenophobic 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.\(^{26}\)

A coalition of civil society organizations led by the digital rights organization, Paradigm Initiative, filed a suit to challenge the constitutionality of Sections 24 and 38 of the cybercrime law in May 2016,\(^{27}\) however, a judge threw out the case in a January 2017 ruling. The coalition filed an appeal on May 3, 2017 challenging the judge’s decision.

Paradigm Initiative has also led efforts to codify protections for internet freedom through the introduction of the draft Digital Rights and Freedom Bill in April 2015, which has made considerable headway since. Sponsored by lawmaker Chukwuemeka Ujam, the bill passed a second reading at the House of Representatives in June 2016,\(^{28}\) and was referred to the Committees on Telecommunications and Human Rights for further deliberation. As of May 2017, the committees have hosted a public hearing but have yet to complete and/or release their report. If the bill reaches a third reading, it will be considered fully passed by the House, then will require concurrence by the Senate and the President’s assent before becoming law.

**Prosecutions and Detentions for Online Activities**

Numerous bloggers, online journalists, and ordinary users were arrested for their online activities in the past year, most of whom were charged for “cyberstalking” under Section 24 of the cybercrime law, though no cases have led to convictions:

- In August 2016, blogger Abubakar Usman was arrested and held for two days for a report accusing the Economic and Financial Crimes Commission of corruption.\(^{29}\)

- Musa Azare was also arrested by police in August after he allegedly criticized the Bauchi state governor on social media, though the governor himself demanded Azare’s release, citing his support for freedom of expression.\(^{30}\)

- In September 2016, blogger Jamil Mubai was arrested for using Twitter to criticize the

---


Katsina state governor’s purchase of coffins instead of paying the outstanding salaries of civil servants.31

- Also in September, State Security Service (SSS) agents arrested blogger Emenike Iroegbu, who runs the Abia Facts online outlet, for allegedly harassing Abia State officials in his articles.32

- In November 2016, SSS agents arrested activist Aku Obidinma for critical comments he posted on Facebook about the Deputy Governor of Imo state.33

- In February 2017, authorities in Kaduna State arrested Audu Maikori for “inciting” tweets about citizen killings by herdsmen in Southern Kaduna that had been proven false.34 Upon realization, Maikori apologized for tweeting the false information, but the authorities continued to carry out his arrest. Released a day later on bail, he was arrested again in March, reportedly for the same issue out of insistence of the Kaduna State Governor.35 Maikori filed a countersuit for the “undue harassment and intimidation by the Kaduna State government, the State Governor and the Nigerian Police” in May,36 which he ultimately won in October.37 A Federal High Court judge ruled that Maikori’s fundamental rights had been violated by the unlawful arrests.

- In March 2017, blogger Kemi Olunloyo was arrested for a post about a pastor’s alleged extra-marital affairs. She was granted bail in April.38

- In July 2017, police in Katsina State detained journalist Danjuma Katsina for Facebook posts deemed critical of a local parliamentarian. He was released the next day with no charges and given no official reason for his detention.39

**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. Several legal provisions may allow the government to conduct surveillance

---

without respect for the Necessary and Proportionate Principles, international guidelines that apply human rights law to monitoring technologies.40

The cybercrime law enacted in May 2015 requires service providers to retain user data and intercept electronic communications.41 Under Section 38 of the law, 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.42 The law implies a degree of judicial oversight over these requests, but the procedure involved is unclear.43

Guidelines for the Provision of Internet Service published by the regulator in 2013 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.44 The guidelines do not include oversight of that cooperation, introducing scope for abuse. The guidelines also stipulate that ISPs must retain user data and “the content of user messages or routing data” for at least 12 months.45

Data localization is mandated under the Guidelines for Nigerian Content Development in Information and Communications Technology, issued by the Nigerian National Information Technology Development Agency (NITDA) in 2013. The guidelines require ICT companies to “[h]ost all subscriber and consumer data locally within the country.”46 The stated aim was to boost local content and ICT development, but the requirement risks compromising user privacy and security, given the absence of adequate data protection laws.47 The extent to which the guidelines have been enforced remained unclear as of 2017, as there have been no reports that international ICT companies have been compelled to comply.

A draft Lawful Interception of Communications Regulation introduced by the communications regulator in February 2013 is still under discussion.48 If implemented, the regulation would enable interception both with and without a warrant under different circumstances, and require mobile phone companies to store voice and data communications for three years. It also directs telecommunications licensees to “provide the National Security Adviser and the State Security Service with the key, code, or access to...protected or encrypted communication” on demand.49

40 Necessary and Proportionate principles: https://necessaryandproportionate.org/about
42 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 38.
43 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.
45 Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission,” 3.
52 Nigeria Communications Commission, “Draft Lawful Interception of Communication Regulations.”
Critics said it bypassed the legislative process and threatens citizens’ privacy rights, since it lacks judicial safeguards against abuse or opportunities for redress.50

News of the government’s acquisition of mass surveillance equipment over the past few years has deepened suspicions of surveillance. 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 2013.51 The active period of the contract from 2012 to 2013 coincides with the state governor’s crackdown on so-called “rumormongering” online.52 Citizen Lab research from 2014 also found a FinFisher “Command and Control” server located on a private ISP in Nigeria.53 As of May 2017, the extent to which that surveillance system is operational is not known.54

The government’s intent to enhance its surveillance capabilities is reflected in its federal budget, which in 2017 allocated NGN 13.9 billion (US $45.6 million) to something called the “Stravinsky Project” for the National Security Adviser’s office 55 which observers believe is new surveillance technology. Other line items in the 2017 budget for the National Security Adviser and allied agencies include “Surveillance Equipment, IMSI catcher,” among others.56 As of mid-2017, it was not clear if those purchases had taken place, or for what purpose. Government officials frequently assert the need for technologies to fight the Boko Haram terrorist group.

SIM card registration requirements instituted in June 2009 threaten users’ rights to anonymous communication and privacy,57 particularly in the absence of a data protection law.58 User registration is also required in cybercafés. An October 2013 directive from the regulator requires cybercafés to “maintain an up-to-date database of subscribers and users, including their full names, physical addresses, passport photos, and telephone numbers.”59 Under Section 7 of the cybercrime law, cybercafés must make their registers “available to law enforcement personnel whenever needed,” with no clear requirement for judicial oversight.60

Intimidation and Violence

Online journalists and internet users in Nigeria have been subject to increasing extralegal harassment and intimidation for their activities in the past few years, particularly by local officials

54 When the author of this report asked for the state of the surveillance system during the Internet Freedom Forum 2016, the representative of the National Security Adviser said he was not aware of any such project. 55 Office of the National Security Advisor 2017 budget, http://bit.ly/2qjrrpB
60 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 7.
or powerful businesspeople who have taken issue with critical commentary posted about them on social media. Alongside the threat of arrest as an intimation tactic, police often raided the homes of targeted bloggers, seizing equipment.61

Technical Attacks

Cyberattacks against news websites, civil society, and human rights activists were not reported in Nigeria during the coverage period, although a government agency announced on Twitter that its website was under attack in May 2017.62

---

62 Ministry of Mines and Steel announced on twitter that its website was under attack on May 21, 2017, http://bit.ly/2qj3Fu4