

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	540
Land:	Nigeria
Kilde:	Freedom House
Titel:	Freedom of the Net 2020
Udgivet:	2020
Optaget på baggrundsmaterialet:	2. februar 2021



Nigeria

PARTLY FREE

60
/100

A. <u>Obstacles to Access</u>	16 /25
B. <u>Limits on Content</u>	26 /35
C. <u>Violations of User Rights</u>	18 /40

LAST YEAR'S SCORE & STATUS

64 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free)



Overview

Nigeria's online environment continues to decline in the aftermath of the February 2019 elections, with print, radio, and broadcast media

increasingly spreading false and misleading information that originates online. The government continued its consideration of legislation that would restrict online speech during the coverage period, though internet users and civil society mobilized to oppose the bill. Numerous bloggers and internet users were arrested for their online activities, with charges that included spreading false information about COVID-19 and insulting government officials.

Nigeria's vibrant media landscape is impeded by criminal defamation laws. Meanwhile, the country has made significant improvements in the competitiveness and quality of national elections in recent years, though irregularities persist. Corruption remains endemic, particularly in the petroleum industry, a key economic sector. Security challenges, including the ongoing insurgency by the Boko Haram militant group, as well as communal and sectarian violence in the restive Middle Belt region, threaten the human rights of millions of Nigerians. The response by the military and law enforcement agencies to the widespread insecurity often involves extrajudicial killings, torture, and other abuses.

Key Developments, June 1, 2019 - May 31, 2020

- A January 2020 cable break resulted in slow internet speeds and connectivity interruptions that primarily affected customers of mobile service provider and internet service provider (ISP) MTN (see A1).
- Broadband right-of-way (RoW) charges, tariffs levied on telecommunications companies for cable built along government-owned roads, fluctuated wildly in some states between January and May 2020, potentially leading to price increases and decreases for internet users (see A4).
- The majority of the 21 pro-Biafra websites originally blocked in 2017 were accessible by February 2020 (see B1).
- In October 2019, a law enforcement agency disclosed the use of sophisticated spyware that can forensically search electronic devices, including on devices belonging to journalists (see C5).

- A February 2020 report revealed how police also accessed call records from service providers to arrest journalists, by accessing contacts and compelling those individuals to call targeted journalists into police stations (see C6).
- Journalists and media websites reported cyberattacks during the coverage period, including multiple distributed denial-of-service (DDoS) attacks against the *Premium Times* website and NewsWireNG, an online newspaper (see C8).

A. Obstacles to Access

Internet penetration rates are high, but sporadic access to electricity continues to pose a barrier to consistent connectivity. An undersea cable break in January 2020 slowed speeds and interrupted connectivity. A significant gender gap in internet usage persists.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

2 / 6

Score Change: The score declined from 3 to 2 because malfunctions in undersea fiber-optic cables caused Nigerian internet users to experience slow internet speeds and connectivity interruptions.

Infrastructural challenges, including unreliable access to electricity, hampers both access to the internet and internet speeds. Despite these drawbacks, Nigeria has one of the largest populations of internet users in sub-Saharan Africa, with over 89 million people online. According to the latest data from the International Telecommunication Union (ITU), Nigeria's internet penetration rate was 27.7 percent in 2018. ¹

The government's new National Broadband Plan (2020–25) (NBP), which is set to replace the 2013–18 plan, has a goal of expanding broadband penetration to 70 percent by 2025. ² The previous NBP set a 30 percent target for broadband penetration, which the country has made incremental progress toward achieving. However, at the end of 2018, the Nigerian

Communications Commission (NCC), the sector regulator, reported that the broadband penetration rate was 22 percent.³ The new NBP was launched by President Muhammadu Buhari in Abuja in March 2020.⁴ Most of the growth in internet use can be attributed to the proliferation of mobile phone services. In January 2019, the NCC reported a mobile phone teledensity of 124 percent and nearly 174 million active mobile internet subscriptions.⁵ The ITU documented a lower mobile phone penetration rate of 75.9 percent in 2018.⁶

Reports of vandalism and destruction of communication infrastructure persisted through the coverage period.⁷ In 2018, the NCC warned against vandalism of telecommunications infrastructure and stressed that vandalism interferes with the federal government's plan to improve broadband penetration.⁸ News reports suggest there were over 33,000 cases of vandalism and theft of facilities between June 2017 and August 2018.⁹

Power cuts frequently disrupt service and access. Nigerian households reported slight improvements in electricity access in recent years, receiving an average of 10 hours of power supply per day in 2017, up from less than 6 hours the previous year.¹⁰ However, more recent data from the polling service NOI Polls showed a slight decline in the average daily power supply from 9.7 hours in the fourth quarter of 2018 to 9.2 hours in March 2019.¹¹ Data from the second and third quarters of 2019 showed an average power supply of 9.2 hours and 9.6 hours respectively.¹²

Shortfalls in the 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.¹³ Separately, the need to pay for expensive backup generators has accelerated the closure of cybercafés that were already struggling to compete with increasing mobile internet access.

In January 2020, a break in the South Atlantic 3(SAT3)/West African Cable System (WACS) undersea fiber-optic cable interrupted internet and

voice service in Nigeria. MTN, which is the most widely used provider in Nigeria, was reportedly most affected by the cable damage. ¹⁴ The disruption, which lasted about a week, resulted in slow internet speeds for some customers, while others could not access the internet at all. Other ISPs in Nigeria rely on other fiber-optic cable systems to provide internet access, such as MainOne and Glo 1. Furthermore, at the end of March, another cut to SAT3/WACS resulted in slow internet services for end users across Nigeria. ¹⁵

The average fixed broadband download speed is 11.91 Mbps and the average mobile download speed is 16.74 Mbps. ¹⁶ In 2019, the National Information Technology Development Agency (NITDA) released its Framework and Guidelines for Public Internet Access. The framework states that “public internet access providers (PIAPs) are required to guarantee a minimum of 256 Kbps as committed information rate (CIR) in a shared connection for each connected user at a given time. Number of users at a given time can be determined by the PIAP depending on the total bandwidth size it is providing.” ¹⁷

In 2018, the Association of Submarine Cable Operators of Nigeria (ASCON) was formed to “promote, encourage, and assist in the protection of subsea cable infrastructure and ancillary equipment and facilities from marine activities, man-made and natural hazards.” ¹⁸

The 2016 acquisition of Visafone by MTN enabled it to obtain 800-megahertz clock (MHz) spectrum access.

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	1 / 3
--	--------------

Although significant digital divides around gender and language persist, affordable data services for mobile subscribers has increased internet access. In its 2019 Affordability Report, the Alliance for Affordable Internet ranked Nigeria 19th out of 61 low- and middle-income nations in the implementation of policies leading to affordable internet access. ¹ In

February 2020, the cost of at least 1.5GB of data from MTN, Glo, and Airtel, the country's most widely used ISPs, was \$2.73 ² . In February 2018, 1.5GB of mobile data, which remains very popular, cost \$3.28. In 2017, the average cost of a mobile plan was \$0.02 per MB, ³ compared to \$0.05 per MB in 2016, \$0.26 per MB in 2015, and \$1 per MB in 2011. Nevertheless, cost remains a major impediment to internet access for many Nigerians in rural areas. Due to the unreliable electricity supply (see A1), those who can afford it often rely on private generators and standby battery-powered inverter systems to remain online during power outages.

In October 2019, the Minister of Communications and Digital Economy issued a directive to telecommunications operators through the NCC to reduce the cost of data and to stop illegal data reductions from consumers. The directive was not implemented during the coverage period ⁴ .

In 2016, the government introduced the Communication Service Tax Bill 2015, which would decrease the affordability of internet access by imposing a 9 percent tax on consumers for communications services including short-message service (SMS), data, and voice services. ⁵ The bill was ultimately folded into the Telecommunications Service Tax Bill 2016, and was before the Senate as of October 2019, ⁶ despite its unpopularity among various stakeholders. The bill was later referred to the Senate's telecommunications committee for further consideration. ⁷

Nigeria's internet landscape is characterized by a significant digital gender and urban divide. A 2018 GSMA survey of 23 low- and middle-income countries, ⁸ including Nigeria, revealed that women were 26 percent less likely than men to use mobile internet services; over 90 percent of Nigerians access the internet on their mobile phones. ⁹ According to the Inclusive Internet Index, women in Nigeria are 22 percent less likely to access the internet than men. ¹⁰ The electricity gap between urban and rural areas underscores internet access issues; 86 percent of Nigeria's urban population has electricity, while 34 percent of the rural population does. ¹¹

Language also serves as an obstacle to internet access in Nigeria. While over 500 languages are spoken in Nigeria, ¹² most internet content is in English, and local language content is vastly underrepresented. For example, there are few Wikipedia entries in the three major Nigerian languages of Yoruba, Hausa, and Igbo. Wikipedia entries on Nigerian topics are often edited by individuals who do not reside in Africa. ¹³ Local language resources, such as audio and video health and educational materials, have higher data requirements, potentially limiting access for users who can afford less data, yet stand to benefit the most from educational materials online.

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?

6 / 6

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 during a state of emergency due to the Boko Haram insurgency.

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, Main One, Suburban Telecom, Multilinks, and MTN. There are three active internet exchange points (IXPs). ¹

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

5 / 6

There are no significant legal, regulatory, or economic obstacles that restrict the diversity of service providers in Nigeria.

The information and communications technology (ICT) market in Nigeria has expanded considerably over the past two decades, with the number of licensed ISPs growing from 18 in 2000 to 126 as of May 2020, though the growth of ISPs has slowed in recent years with the rise in mobile access. ¹ Despite the large number of registered ISPs, there is a high degree of market concentration. ² Five privately owned mobile service providers also provide internet access: MTN, Globacom, Airtel, 9Mobile (formerly Etisalat), and NTEL, which began operations in 2016 after acquiring the license of the defunct national telephone service provider NITEL. ³ In 2016, MTN acquired Visafone, securing access to its 800-MHz spectrum. ⁴

In May 2020, several states reduced or fully waived broadband RoW charges, tariffs levied on telecommunications companies for each meter of cable built along state roads. High RoW charges can limit the expansion of broadband and restrict the entry of new providers to the market, or result in higher costs for subscribers. The states of Ekiti, Imo, Plateau, and Katsina lowered state RoW charges from 4,500 naira (\$11.50) to 145 naira (\$0.37) per linear meter, while Kaduna State waived its charge. ⁵ Earlier, in January, 14 state governments increased their RoW charges by up to 1,000 percent, prompting a rebuke from the federal government. ⁶

In 2017, Etisalat changed its name to 9Mobile, following the exit of the company's largest shareholder, Mubadala Development Company. Analysts believe that Mubadala's exit was due to 9Mobile's mishandling of \$1.2 billion in loans. ⁷ Although 9Mobile's proposed sale to Teleology Holdings has been mired in controversy, it continues to provide services to subscribers. ⁸ The NCC asserts that Teleology has not paid a nonrefundable, \$50 million registration fee, despite their claims to the contrary. The Central Bank of Nigeria, some vendors owed by 9Mobile, and the chairperson of a legislative committee on telecommunications have all raised objections to the sale. ⁹ The sale was approved by the NCC in November 2018, but in April 2019, the Abuja High Court ordered that no action be taken on the sale pending a lawsuit by investors demanding the return of their funds. ¹⁰

The NITDA's 2019 Framework and Guidelines for Public Internet Access is designed to regulate the provision and use of public internet access in Nigeria. Public internet access is defined as connectivity in "computer terminals, computers, mobile phones, and/or other devices without charge to the user." According to the framework, PIAPs are required to register with the NITDA and obtain approval from the body to carry out their operations.

Cybercafés are required to obtain licenses, but the large number of unlicensed cybercafés in operation suggests that the regulator has not enforced the requirement. ¹¹

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

2 / 4

Although regulatory bodies that oversee service providers have historically had a reputation for independence, some recent actions by the NCC have called the body's autonomy into question. The 2003 Nigeria Communications Act vests regulatory responsibility over the ICT sector with the NCC. The government nominates the NCC's nine-member board of commissioners. The NCC's current CEO and executive vice chairman, Umar Garba Danbatta, was appointed in 2016 through a process that was viewed as fair. Danbatta, a leading academic, is also considered an industry expert. ¹

Some of the NCC's recent actions, including blocking orders it has conveyed to service providers on behalf of the national security adviser, have cast a shadow over the body's perceived independence (see B1).

The NITDA, which was established in 2007, is tasked with planning, developing, and promoting the use of information technology in Nigeria. One of its objectives is to "accelerate internet and intranet penetration in Nigeria and promote sound internet governance." The agency also supervises the management of the country code top-level domain (.ng).

² Although the NITDA is believed to operate independently, its director

general, who is responsible for the day-to-day administration of the agency and the implementation of policy, is a political appointee. ³

B. Limits on Content

The majority of the pro-Biafra websites blocked in 2017 are now accessible. Misleading and false information about the COVID-19 pandemic proliferated online, and online misinformation increasingly spread to offline media. Google complied with an elected official's request to delist content containing sensitive videos of that official from search results in Nigeria. Social media is regularly used to engage on social and political issues.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	4 / 6
---	--------------

Score Change: The score improved from 3 to 4 because a majority of the 21 websites blocked in November 2017, many of which promoted the independence of Biafra, have become accessible.

There were no new reports of content blocking or filtering ordered by the Nigerian government during the coverage period. In November 2017, it was revealed that service providers blocked 21 websites, including the popular Naij.com online news outlet, at the request of the NCC. ¹

Though the blocking order lacked transparency, many of the blocked sites promote the independence of Biafra, the region that attempted to secede from Nigeria in 1967 and fought against the federal government in the 1967–70 Biafran War. Although access to Naij.com was eventually restored, at least a dozen pro-Biafra websites were still inaccessible as of March 2019. ² As of February 2020, at least nine websites remained inaccessible, but the others were accessible ³. The NCC's actions raised concerns that the websites of opposition parties and critical nongovernmental organizations (NGOs) could be blocked during the 2019 election campaign period. However, there were no reports of blocking around the time of the elections.

YouTube, Facebook, Twitter, WhatsApp, and other communications platforms are freely available and widely used. ⁴ The complex nature of Nigeria's internet infrastructure makes it difficult to carry out systematic filtering or censorship.

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

3 / 4

Score Change: The score declined from 4 to 3 because an elected official successfully sought to delist URLs that displayed sensitive videos of their activities from Google search results in Nigeria and because many media houses are owned by government officials.

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

There were a total of two content removal requests made by the Nigerian government to Google in 2018, after several years of not making any such requests. ¹ According to Google's updated transparency report, there was one government request for content removal during the company's January–June 2019 reporting period. The request originated from an elected official regarding eight URLs, because “content at those URLs contained sensitive videos of the official that were allegedly uploaded without the official's consent.” ² Google complied with the request, delisting the URLs from search results in Nigeria. According to Facebook's transparency report, there were no content restrictions between July and December 2018. ³ However, Facebook complied with one government request for user data in 2019. ⁴

In August 2020, after the coverage period, the National Broadcasting Commission (NBC) published amendments to the Nigerian Broadcasting Code, which include regulations for online broadcasters for the first time.

⁵ The amendments impose liability on online broadcasters for content posted on their platforms. Sanctions for breaches of the code's provisions,

including registration requirements (see B6), include orders for content deletion and website blocking. The amended code does not define “web/online broadcasting services,” nor does it describe how sanctions will be enforced. Industry and civil society groups criticized the amended code for restricting innovation and online speech. ⁶

Many media houses in Nigeria are owned or controlled by politicians and government officials, ⁷ potentially influencing reporting from those outlets.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

2 / 4

Restrictions on internet content sometimes lack transparency. The blocking of 21 pro-Biafra websites in 2017 was not carried out through a transparent process. The block was ordered by the NCC based on Section 146 of the 2003 Nigeria Communications Act, which obligates ISPs to cooperate with the NCC to preserve national security and prevent crime. ¹

In recent years, 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, ² sparking fears of impending online censorship. ³ A number of worrying legislative proposals have added weight to those fears. The Frivolous Petitions Prohibition Bill, introduced in 2015, sought to restrict expression on social media, though it was withdrawn in 2016. Meanwhile, the Cybercrime Act, which was signed into law in 2015, has been used to arrest bloggers for posting critical content during the coverage period (see C2 and C3). During the coverage period, two other bills with the potential to restrict the internet and digital content were under consideration, the Protection from Internet Falsehood and Manipulation Bill and National Commission for the Prohibition of Hate Speeches Bill 2019 (see C2). In March 2020, the Senate held a public hearing for the Protection from Internet Falsehood and Manipulation Bill.

The hearing was attended by 110 civil society organizations; the majority of these groups asked the Senate to remove the bill from consideration.

4

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?

3 / 4

The persistent arrests of users for their online activities under the 2015 Cybercrime Act has resulted in growing self-censorship, particularly among professional journalists who publish content online (see C3). This self-censorship worsened after recent reports that revealed the extent of the Nigerian security services' surveillance and interception powers. Security forces had access to journalists' private communications, and sometimes used that information to facilitate arrests (see C6 and C6). ¹ Despite the trend of growing self-censorship, some journalists persist in testing boundaries, despite potential repercussions (see B8, C3, and C7).

Nigeria's LGBT+ community is marginalized, and online self-censorship is common among LGBT+ individuals. ² Many LGBT+ internet users report feeling unsafe using their real names online, preferring to engage anonymously. ³ While members of the community may comment on or share content discussing or promoting LGBT+ issues, most are not open about their identity online, likely due to societal prejudice and the Same-Sex Marriage (Prohibition) Act 2014, which criminalizes public displays of same-sex relationships. ⁴

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

2 / 4

Nigeria's online information landscape is marred by misinformation, particularly around the COVID-19 pandemic, and online misinformation increasingly spreads to print, radio, and broadcast media. Political parties

manipulated online content in the run-up to the February 2019 national elections, which took place before the current coverage period.

False information about coronavirus proliferated on Nigerian social media during the COVID-19 pandemic. Rumors about the government's pandemic response and the health of political figures spread widely, sometimes by supporters of the opposition People's Democratic Party (PDP) or the ruling All Progressives Congress (APC). ¹ In March 2020, three people were hospitalized after overdosing on chloroquine, a malaria medication. False information that the drug could be used to treat COVID-19 has proliferated online, in part due to US president Donald Trump's public endorsement of the medicine. ²

An April 2020 study by the Centre for Democracy and Development (CDD) West Africa found an unprecedented level of online misinformation and disinformation, especially content that inflames ethnic and political tension. The CDD West Africa study also found that false information originating online increasingly spread to Nigerian print, radio, and broadcast media. ³

The presence of misleading and false information online played a notable role in public debate in the run-up to the February 2019 national elections. Coordinated social media campaigns that spread disinformation on behalf of political candidates were common ⁴ at both the national ⁵ and local ⁶ levels. Campaigns hired individuals to create fake Twitter accounts that spread propaganda, bolstered the candidate's agenda, undermined opponents, and shaped the online conversation ahead of the elections. ⁷ According to a Quartz report published in February 2019, one campaign paid a team of 12 people to manage more than 600 Twitter accounts. A 2019 CDD West Africa study found that there was a high level of bot activity ahead of the elections. The study collected 34.5 million tweets from major politicians, political parties, media houses, and other accounts that published posts with election-related hashtags. From this data, the CDD concluded that 19.5 percent of the accounts showed signs of automation. ⁸

In addition to these efforts to manipulate the online information environment, in May 2019, Facebook announced that it was deleting 265 accounts that were used to influence the online environment through disinformation campaigns in several countries, including Nigeria. ⁹ The fake accounts were run by the Archimedes Group, an Israeli company, and sought to influence the 2019 Nigerian elections. ¹⁰

Generally speaking, many media houses in Nigeria are owned or controlled by politicians and government officials, ¹¹ potentially influencing reporting from those outlets.

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?

3 / 3

There are no significant economic or regulatory constraints that negatively affect users' ability to publish content online. The owners of online media outlets do not need informal connections with government officials to be economically viable. The state does not limit the ability of online outlets to sell advertisements or attract investment, and advertisers are generally free to do business with any online media outlet. ISPs in Nigeria are not known to manipulate network traffic or bandwidth availability, and generally respect the principles of net neutrality. There are no barriers to establishing online news outlets, blogs, or social media channels.

In August 2020, after the coverage period, the NBC published amendments to the Nigerian Broadcasting Code, which include regulations for online broadcasters for the first time (see B2). ¹ The amended code requires “persons who wish to operate web/online broadcasting services” to register with the NBC. Registered online platforms are subject to the code's provisions, including those relating to hate speech (see C2).

B7 0-4 pts

Does the online information landscape lack diversity?

3 / 4

Nigeria is home to a diverse blogosphere, which has become a source of reliable news for many users, and provides space for vibrant 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.

There were robust and lively social media conversations during the 2019 election period, with both progovernment and opposition voices active across social media platforms like Twitter and Facebook. Nigerians are known to be among the most prolific political tweeters in Africa. ¹

Nigerians are typically able to access a range of local and international news sources that are independent and balanced, and broadcast in the main languages spoken in the country. These sources include the national news broadcaster, the Nigerian Television Authority (NTA), ² which is one of the largest television networks in Africa and broadcasts in local languages. Broadcasters owned by state governments also air content in local languages, while privately owned broadcasters serve communities in both English and local languages. ³ Many of these local news sources are also available online. International news sources like the British Broadcasting Corporation (BBC) are also popular in Nigeria and offer online content in local languages, ⁴ including pidgin English. ⁵

However, some communities struggle to find online content in their local language. The majority of content is in English, while local languages are vastly underrepresented (see A2).

Online media outlets, social media pages, blogs, and websites feature a diversity of voices, providing content produced by ethnic minorities, religious groups, women, and LGBT+ people.

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	6 / 6
---	---------------------

Online mobilization tools are freely available to users. 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. A number of digital campaigns have been successful, including digital activism that contributed to 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 (see B3). ¹

Since the Protection from Internet Falsehood and Manipulation Bill's reintroduction in the Senate in November 2019, and ahead of a public hearing in March 2020, Nigerians mobilized online, using the hashtag #saynotosocialmediabill, and offline to oppose the bill, which threatens to constrict the space for freedom of expression in the country. ² Nearly 100,000 people have signed an online petition in opposition to what has also been called the "social media bill." ³ A similar hashtag, #SayNoToHateSpeechBill, has also been widely used. ⁴

The #RevolutionNow hashtag is popularly used in online discussion of poor governance and corruption. This sometimes spills offline; in August 2019, protesters held #RevolutionNow demonstrations over election irregularities. ⁵

Online activists played a significant role during the 2019 election period, mobilizing voters and spurring citizen action to hold elected officials accountable. Supporters of the leading candidates in the presidential election, President Buhari and Atiku Abubakar, used the Twitter hashtags #Buhariiswinning ⁶ and #Atikuiswinning ⁷ to build support for their candidates.

In an example of effective digital activism that preceded the current coverage period, in February 2018, when over 100 girls were abducted from their school in northern Nigeria, citizens started a social media campaign similar to #BringBackOurGirls in 2014, demanding information and action from the government. In response, the government provided more details on the situation, and continued to give status updates until all but one of the girls were returned by March 2018. ⁸

C. Violations of User Rights

New disclosures revealed that the government has used sophisticated forensic search technology on electronic devices belonging to journalists and obtained call records from service providers to arrest at least three journalists since 2017. Numerous bloggers and internet users were arrested for online activities. Several cyberattacks targeting journalists and news sites were also reported.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	3 / 6
--	---------------------

Nigeria's 1999 constitution guarantees freedoms of expression and the press, but these rights are not always respected in practice, including for online activities.

Paradigm Initiative, a digital rights organization, has led efforts to codify protections for internet freedom through the introduction of the draft Digital Rights and Freedom Bill in 2015. Sponsored by lawmaker Chukwuemeka Ujam, the bill was passed by the House of Representatives in December 2017 and the Senate in March 2018. However, President Buhari declined to sign the bill in March 2019, claiming that it “covers too many technical subjects and fails to address any of them extensively.” ¹ Following Buhari's rejection of the legislation, the bill was revised to address the president's concerns and was reintroduced in the House of Representatives in July 2019. ² The bill's objectives include protecting freedoms of expression, assembly, and association online, guaranteeing the application of human rights within the digital environment, providing sufficient safeguards against online abuse and providing opportunity for redress, and equipping the judiciary with the necessary legal framework to protect human rights online. As of May 2020, the president has not signed the bill. ³

Nigeria's judiciary has achieved a degree of independence, but political interference, corruption, and a lack of funding, equipment, and training remain important problems. The suspension of Nigeria's chief justice by President Buhari in January 2019, ⁴ which occurred without the involvement of the National Judicial Council (NJC) or the National Assembly, as required by law, ⁵ brought the judiciary's independence further into question.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?

1 / 4

A number of laws assign criminal penalties or civil liability for legitimate online activities in Nigeria.

Before leaving office in 2015, former president Goodluck Jonathan signed the Cybercrime Act 2015 into law, which provides a framework for addressing the country's cybercrime epidemic but contains broadly worded provisions that can be used to punish legitimate expression. ¹ 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 10 million naira (\$27,000), or both. ² Recent reporting has also revealed that Section 27, which criminalizes any person who "aids, abets, conspires, counsels, or procures another person(s) to commit any offence under [the Cybercrime] Act," ³ is being used to prosecute journalists. ⁴

A coalition of civil society organizations led by Paradigm Initiative filed a suit to challenge the constitutionality of sections 24 and 38 of the law in 2016. ⁵ However, a judge dismissed the case in a 2017 ruling. Following the defeat of another appeal in June 2018, the same group filed an appeal with the Supreme Court in August 2018. ⁶ Another civil society

organization, the Incorporated Trustees of Laws and Rights Awareness Initiative, also filed a suit to challenge the law. ⁷

Internet freedom advocates have raised concerns that a broadly worded draft hate speech bill, which passed its first reading in the Senate in November 2019, ⁸ could be used by the government to silence the online activities of opposition critics and civil society. Proposed in March 2018, the bill prescribes the death penalty for speech that leads to a person's death. The bill, sponsored by Senator Aliyu Sabi Abdullahi, a member of ruling APC, ostensibly seeks to eliminate "hate speech and discourage harassment on the grounds of ethnicity, religion or race among others" and, among its provisions, states that "any person who uses, publishes, presents, produces, plays, provides, distributes and/or directs the performance of any material, written and/or visual, which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words, commits an offense." ⁹ While the bill has been met with strong opposition, it is one of many recent proposals to clamp down on free speech in a moment when citizens are increasingly using online tools to defend democracy.

In November 2019, the Protection from Internet Falsehood and Manipulations Bill 2019 passed its first reading, second reading, and Senate vote. The bill would allow the government to disrupt internet access, block social media platforms, and would also institute fines of up to 300,000 naira (\$820) or imprisonment of up to three years for statements that are "prejudicial to national security" or "diminish public confidence" in the government. ¹⁰ A public hearing on the bill was then held in March 2020; civil society organizations and government agencies like the NCC and the Broadcasting Organization of Nigeria voiced their opposition to the bill. ¹¹ The bill's progress has been met with uproar in Nigeria due to clauses that restrict freedom of expression online. After the public hearing, the bill was referred to the Senate Committee on Judiciary, Human Rights, and Legal Matters.

In August 2020, after the coverage period, the NBC published amendments to the Nigerian Broadcasting Code (see B2). The changes included an upward review of fines from 500,000 naira (\$1,280) to 5

million naira (\$12,840) for hate speech. ¹² These regulations could negatively impact freedom of expression in the country.

The implementation of Sharia (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.

C3 0-6 pts

Are individuals penalized for online activities?

2 / 6

Numerous bloggers, online journalists, and private citizens were arrested for their online activities during the coverage period, including for COVID-19 misinformation and criticism of government officials.

In April 2020, Katsina state police arrested Lawal Abdullahi Izala, Bahajaje Abu, and Hamza Abubakar for insulting President Buhari and Governor Aminu Bello Masari in a viral social media video. ¹ Izala, who is over 70 years old, was sentenced to 18 months' imprisonment in May.

² As of June 2020, details about Abu and Abubakar were not publicly available.

Also in April 2020, Akinloye Saheed was held in custody by a court in Osogbo Osun State for a Facebook post in which he claimed that the state government imported COVID-19 patients from outside the state in order to claim funds from the federal government ³. The charges against him were later dropped by the state government ⁴.

Emperor Gabriel Ogbonna, a barrister, was arrested by the Department of State Security (DSS) in late March 2020 after he alleged impropriety relating to the governor of Abia State in a Facebook post. ⁵ Ogbonna reportedly received a petition alleging he had published falsehoods against the governor ⁶. Ogbonna was released on bail in late April, but

was rearrested hours later by the DSS. He remained in custody as of June 2020. ⁷

Agba Jalingo, publisher of online news outlet CrossRiverWatch, was arrested in August 2019 and detained without charge. His arrest came after CrossRiverWatch's critical reporting on corruption in Cross Rivers State, which included allegations against the state's governor ⁸. Later that month, he was charged with disturbance of public peace, treason, cybercrimes, and terrorism for his reporting and social media posts about the governor. ⁹ Jalingo was released on bail in February 2020. ¹⁰

Similarly, Omoyele Sowore, a Nigerian journalist and activist who also ran for president in 2015, ¹¹ was arrested and charged with treason, cyberstalking, and money laundering. ¹² Sowore is an online journalist for news website Sahara Reporters, which he founded, ¹³ and has campaigned against corruption and poor governance, including through his popular online hashtag and protest movement, #RevolutionNow. Sowore was originally arrested in August 2019 and was detained until early December, despite court orders to release him on bail; Sowore was released that month but was rearrested the next day, and was eventually released on bail on Christmas Eve ¹⁴. The conditions of Sowore's bail restricted him from leaving the capital city of Abuja or speaking to the press. His case garnered major international attention, including an appeal by six members of the US Congress to the Nigerian attorney general on Sowore's behalf. ¹⁵

In April 2019, activist IG Wala was sentenced to 12 years in prison for criminal defamation ¹⁶ and other charges arising from a 2017 Facebook post alleging corruption in Nigeria's National Hajj Commission. ¹⁷ For the three charges on which he was convicted—unlawful assembly, public incitement, and criminal defamation, he was sentenced to seven, three, and two years in prison, respectively. ¹⁸ Wala appealed the sentence later that month. The Court of Appeal in Abuja reduced his seven-year term to two years in March 2020. In April 2020, Wala was released when President Buhari pardoned a total of 2,600 prisoners throughout Nigeria. ¹⁹

In March 2019, Obinna Don Norman, the owner and editor in chief of online news outlet Realm News, was arrested and charged under sections 24 and 27 of the Cybercrime Act 2015. Norman was specifically charged with cyberstalking, sending defamatory messages using a computer, using a computer to send messages “for the purpose of causing public hatred,” and using a computer to “bully, threaten and harass.” He was also charged under Abia State’s 2009 antiterrorism and kidnapping law, for allegedly threatening the Abia state governor’s life with “messages through [the] internet and phone calls.” ²⁰

In February 2019, Chijioke Nnamani, a student at Madonna University in the southern town of Okija, was arrested after criticizing the university in a Facebook post. Family and friends protested the arrest vigorously on social media, using the hashtag #FreeNnamani, without success. ²¹ Nnamani was arraigned in Anambra State in March 2019 on cybercrime charges, and reports suggested that he was still in detention at the end of the reporting period. ²² In October 2019, a court hearing to hear the case in Akwa Ibom State was stalled because of the absence of the judge. ²³

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	3 / 4
--	--------------

While users can generally communicate anonymously online and can freely use encryption tools, there are some legal provisions that threaten anonymity.

The NITDA’s 2019 Framework and Guidelines for Public Internet Access mandates that PIAPs “ensure every user goes through a registration process to acquire an access code for the purpose of public internet access after verification through the user’s mobile number which is the unique login ID.” This measure eliminates anonymity for those who utilize free internet connections and increases the collection and processing of user data. However, the framework also mandates that PIAPs use the most recent encryption standards to protect users’ data and communications on the internet. ¹

The NBC's August 2020 amendments to the Nigerian Broadcasting Code requires broadcasters, including online broadcasters, to comply with decryption orders from the NBC "at times of national emergency." ²

Draft regulations on the interception of communications (see C5 and C6) introduced by the NCC in 2013 would direct 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. ³ The regulations have not yet been approved.

SIM card registration requirements instituted in 2009 threaten users' rights to anonymous communication and privacy, ⁴ particularly in the absence of a data protection law. ⁵

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?

3 / 6

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. ¹

In October 2019, a Nigerian law enforcement agency disclosed that Nigerian security forces use software from Cellebrite and AccessDataGroup, two companies that provide technology to extract and forensically search data from electronic devices, including devices protected by strong encryption. Forensic search technology was reportedly used to search over 20 computers and phones seized from the *Daily Trust* when the paper's editors were arrested in January 2019 for their reporting on military operations in the northeast. ²

In June 2019, President Buhari signed the Mutual Assistance in Criminal Matters Bill 2016 into law. Drafted to target international corruption, the law establishes procedures for cooperation with other countries in criminal cases through a mutual legal assistance treaty framework. ³ The act

includes provisions to comply with requests from third states for telecommunications interception, stored telecommunications, or other forms of stored electronic data, subject to oversight in some circumstances from the attorney general or the courts. ⁴

Recent revelations show that the government has been using these capabilities against journalists. In February 2020, the Committee to Protect Journalists (CPJ) reported on the use of cell phone data by Nigerian security forces to arrest investigative journalists (see C6). Police used phone records to identify journalists' contacts, detained those contacts, and then used those contacts to access and arrest the journalists. ⁵

In March 2019, President Buhari declined to sign the draft Digital Rights and Freedom Bill (see C1), which would have provided a comprehensive data privacy and protection framework, into law. The bill aimed to guarantee the fundamental privacy rights of citizens and define the legal framework regarding surveillance. It also contained provisions outlining procedures for the lawful and authorized interception of communications within the digital environment without sacrificing the constitutional rights of citizens. Despite this setback, stakeholders in Nigeria's ICT policy space have commenced advocacy and negotiation towards getting the bill back on the president's desk for his signature.

Data security issues were prevalent surrounding the February 2019 presidential election. According to reports, a number of Nigerians received phone calls from individuals reportedly conducting political mobilization ⁶ on behalf of the ruling party. The phone numbers and locations of the call recipients were reportedly obtained from the Independent National Electoral Commission (INEC), which collects citizens' data while conducting elections.

Although Nigeria has no data protection legislation, in January 2019, the NITDA issued the Nigeria Data Protection Regulation to protect data privacy within the country. ⁷ Consultations on how the regulation would be implemented continued through the coverage period, ⁸ and the significance and effectiveness of the regulation remains unclear.

In recent years, the government has acquired equipment for mass surveillance. In 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 2013.⁹ The active period of the contract, from 2012 to 2013, coincides with the governor's crackdown on so-called "rumormongering" online.¹⁰ Citizen Lab research from 2014 also found a FinFisher command-and-control server located in a private ISP in Nigeria.¹¹ The extent to which that surveillance system is operational is unclear.¹²

The government's intent to enhance its surveillance capabilities is reflected in the federal budget, which in 2018 allocated 4.6 billion naira (\$12.8 million) to Stranvisky Project 2.¹³ Observers believe the project, which falls under the purview of the Office of the National Security Adviser (ONSA), is for new surveillance technology. Several other budget allocations for the ONSA and DSS were intended to increase their surveillance capabilities, including a "Social Media Mining Suite," "Wolverme Next Generation SDRIMSI," "Surveillance Drone," and "Mobile Surveillance Facilities."¹⁴ Government officials frequently assert that new technology to fight the Boko Haram terrorist group is necessary.

The 2019 Executive Budget Proposal¹⁵ revealed that some of these projects were still ongoing. Stranvisky Project 2 received an allocation of 4 billion naira (\$11.1 million) in the proposal. The DSS budget allocated 990.6 million naira (\$2.7 million) for a social media mining suite and 199.8 million naira (\$555,000) for a "surveillance drone with precism camera \$ISMI payload capabilities." The drone's "\$ISMI payload capabilities" may refer to International Mobile Subscriber Identity-Catchers (IMSI), a telephone eavesdropping device used to intercept mobile phone traffic and track the location data of mobile phone users. The 2020 Executive Budget Proposal¹⁶ included allocations for many of the items reported in 2019, including Stravinsky Project 2 and a DSS surveillance drone. The proposal also allocated 3.1 billion naira (\$8.7 million) for a "Counterterrorism Center (All Eye Project)."

Many online journalists have long suspected that they are being surveilled by the state. In 2017, the federal government denied monitoring calls and

social media posts. ¹⁷ However, the NCC stated during a March 2018 event that “the Office of the National Security Adviser has a direct link to the NCC’s SIM registration database in order to monitor and apprehend criminals in the country.” ¹⁸

The Draft Lawful Interception of Communications Regulation introduced by the NCC in 2013 did not take effect during the current reporting period.

¹⁹ If implemented, the regulation would enable interception both with and without a warrant under different circumstances. Critics have complained that the regulation has bypassed the legislative process and threatens privacy rights, since it lacks judicial safeguards against abuse or opportunities for redress. ²⁰

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	3 / 6
---	--------------

Score Change: The score declined from 4 to 3 due to the revelation that the government has used call records from service providers to arrest at least three journalists since 2017.

There are numerous legal mechanisms that compel service providers to assist the government in its efforts to monitor users’ communications. The Nigerian government has used those mechanisms to investigate and arrest journalists.

The Nigeria Governors’ Forum announced in April 2020 that it would partner with MTN to provide contact tracing and other services to contain the pandemic. ¹ This development could involve subscribers’ information, and raised privacy concerns amongst the citizenry, though no further details were reported.

In February 2020, the CPJ reported at least three cases since 2017 where the government used call detail records to arrest journalists. In each case, security forces used records from service providers to identify trusted

contacts of the journalist, detained the contact, and had them call the journalist to report to a police station. ²

The 2015 Cybercrime Act requires service providers to retain user data and intercept electronic communications upon the request of law enforcement. ³ 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. ⁴ The law implies a degree of judicial oversight for these requests, but the procedure involved is unclear. ⁵

The Guidelines for the Provision of Internet Service, published by the NCC 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. ⁶ The guidelines do not include oversight mechanisms, creating the potential 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. ⁷

Data localization is mandated under the Guidelines for Nigerian Content Development in Information and Communications Technology, issued by the NITDA in 2013. The guidelines require ICT companies to “host all subscriber and consumer data locally within the country.” ⁸ The stated aim of the guidelines 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. ⁹ The extent to which the guidelines have been enforced remained unclear as of 2020, as there have been no reports that international ICT companies have been compelled to comply.

The Draft Lawful Interception of Communications Regulation (see C5) would require mobile phone companies to store voice and data communications for three years if enacted.

User registration is required in cybercafés. A 2013 directive from the NCC requires cybercafés to “maintain an up-to-date database of subscribers

and users, including their full names, physical addresses, passport photos, and telephone numbers.” ¹⁰ Under Section 7 of the 2015 Cybercrime Act, cybercafés must make their registers “available to law enforcement personnel whenever needed,” with no clear requirement for judicial oversight. ¹¹

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	2 / 5
--	--------------

Online journalists and activists have been subject to increasing extralegal harassment and intimidation in retaliation for their activities in recent years, particularly by local officials or powerful businesspeople who have taken issue with critical commentary posted about them on social media. Along with the threat of arrest as an intimidation tactic, police often raid the homes of targeted bloggers, sometimes seizing equipment. ¹

In May 2020, Mienpamo Saint, a blogger and owner of independent news site Naijalivetv.com, was abducted at night by DSS officers in Yenagoa Bayelsa State. The officers questioned him on the sourcing of his stories regarding the potential arrest of the Ebonyi state deputy governor ². He was released without charge when he apologized for his website’s reporting, and denied he had been abducted in the first place at a conference organized by the DSS.

Also in May 2020, five female Nigerian Immigration Service (NIS) officers were officially sanctioned by the NIS for participating in a viral social media video challenge called “Don’t Rush.” The videos, which showed the women appearing in their uniforms and then in civilian attire, were deemed to have violated the NIS’s internal code. Their sanction and subsequent reassignment to posts in the northeast, where the insurgency is active, was widely condemned by Nigerians. ³

In March 2020, state security officers visited the home of Musikilu Mojeed, editor of the Premium Times online newspaper, in an attempt to have him reveal the source behind a leaked government document published by the

outlet. Another Premium Times editor reported that two unmarked vans, which he suspected belonged to the security services, were parked outside of the Premium Times office. ⁴ In late February, Samuel Ogundipe, a Premium Times journalist, received anonymous phone calls telling him to stop his work, as well as a phone call from someone claiming to work in the Nigerian army. In late March, he reported that his email had been hacked (see C8), and state security offers were reportedly parked outside his home that same month. ⁵

There were significant incidents of violence and harassment against journalists covering the presidential election in February 2019, which escalated in the run-up to state elections in March 2019. ⁶ Kunle Sanni, a Premium Times reporter who covered the election in Plateau State, told the CPJ that he was held for nearly 30 minutes and was forced to delete photos of what appeared to be underage voters by three men calling themselves “farmers.” ⁷

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	1 / 3
--	--------------

Score Change: The score declined from 3 to 1 because of multiple reported cyberattacks against journalists and news sites during the coverage period.

Several cyberattacks against news sites and journalists were reported in Nigeria during the coverage period. Ogundipe, a *Premium Times* journalist, claimed that security services hacked his email in March 2020. The *Premium Times* website itself was targeted with multiple cyberattacks in February and March 2020, and two distributed denial-of-service (DDoS) attacks were reported in early March. State security officials have denied allegations of involvement. ¹ Similarly, NewsWireNG, an investigative news site came, under DDoS and malware attacks ² in March 2020, though they were repelled. ³ NewsWireNG is known for its critical and

investigative work targeted at government and other prominent figures in Nigeria.



On Nigeria

See all data, scores & information on this country or territory.

[See More >](#)

Country Facts

Global Freedom Score

47/100 Partly Free

Internet Freedom Score

60/100 Partly Free

Freedom in the World Status

Partly Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

No

Users Arrested

Yes

In Other Reports

[Freedom in the World 2020](#)

Other Years

**Be the first
to know
what's
happening.**

Join the Freedom
House monthly
newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2021 FreedomHouse