Nigeria | Freedom House

Overview

Despite some improvements in the online environment, manipulation of online content in the run-up to the February 2019 national elections and the arrests of users for online activity hampered internet freedom in Nigeria during the coverage period. The election period was also marred by an increase in violence, harassment, and prosecutions of journalists, including online journalists, impeding the otherwise vibrant online landscape. A push for the protection of digital rights, through the Digital Rights and Freedom Bill, was frustrated in 2019 when President Muhammadu Buhari declined to sign the bill into law.

The vibrant media landscape is impeded by criminal defamation laws. Nigeria has made significant improvements in the competiveness and quality of national elections in recent years, though political corruption remains endemic, particularly in the petroleum industry that dominates the economy. 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, 2018 – May 31, 2019

- Over a dozen of the pro-Biafra websites blocked in 2017 remained unavailable at the end of the coverage period (see B1). However, there were no reports of other websites being blocked by the government during the reporting period.

- A preponderance of misleading and false information online, including through coordinated campaigns and bots, played a notable role in the run-up to the February 2019 national elections (see B5).

- In May 2019, Facebook announced that it was deleting 265 accounts that were used to carry out disinformation campaigns in several countries, including Nigeria. The fake accounts were run by the Archimedes Group, an Israeli company, and sought to influence the 2019 Nigerian elections (see B5).

- In March 2019, President Buhari declined to sign the Digital Rights and Freedom Bill (see C1). The bill, originally introduced in 2015, was passed by the House of Representatives in 2017 and the Senate in March 2018.

- Several arrests were reported for online activities, and one individual received a 12-year prison sentence for a post on Facebook on charges of unlawful assembly, public incitement, and criminal defamation (see C3).

A Obstacles to Access
Internet penetration rates are high, but sporadic access to electricity continues to pose a barrier to consistent 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? | 36 |

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 2017. The government’s National Broadband Plan (2013–2018) 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. 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. The ITU documented a lower mobile phone penetration rate of 83 percent in 2016.

There have been news and reports of vandalism and destruction of communication infrastructure. In 2018, the Nigerian Communications Commission (NCC) warned against vandalism of telecommunications infrastructure and stressed that vandalism interferes with the Federal Government’s plan to improve broadband penetration.

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. However, recent data from the polling service NOI Polls shows 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.

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. 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.

The average fixed broadband download speed is 6.41 Kbps and the average mobile download speed is 7.5 Kbps. 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.”

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.”

The 2016 acquisition of Visafone by the mobile service provider MTN enabled it to obtain 800 megahertz clock (MHz) spectrum access, giving it the potential to launch 4G LTE service (see A4).

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?

Although significant digital divides around gender and language persist, affordable data services for mobile subscribers has increased internet access. The Alliance for an Affordable Internet ranked Nigeria the 18th most affordable internet environment among 61 low- and middle-income countries assessed in its 2018 Affordability Report. As of February 2018, mobile internet plans remained very popular, with 1.5 GB of data available for $3.28. In 2017, the average cost of a mobile plan was $0.02 per MB, 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 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. The bill was ultimately folded into the Telecommunications Service Tax Bill 2016, and was before the Senate as of October 2019, despite its unpopularity among various stakeholders.

Nigeria’s internet landscape is characterized by a significant digital gender divide. Research published in 2015 by the World Wide Web Foundation and the Paradigm Initiative found that poor women in Lagos were 50 percent less likely to have access to the internet than men of the same age, education, and income level. A 2018 survey by the GSMA of 23 low and middle income countries, 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.

Language barriers prevent another obstacle to internet access in Nigeria. While over 500 languages are spoken in Nigeria, 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. 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?

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).

A4 0-6 pts

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

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 decade, with the number of licensed internet service providers (ISPs) rising from 18 in 2000 to 98 as of February 2018, though the growth of ISPs has slowed in recent years with the rise in mobile access. Despite the large number of registered ISPs, there is a high degree of market concentration. 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. In 2016, MTN acquired Visafone, securing access to its 800 MHz spectrum, which is a possible precursor to the launch of 4G LTE service.

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. Although 9Mobile’s proposed sale to Teleology Holdings has been mired in controversy, it continues to provide services to subscribers. 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. Although the sale was approved by the NCC in November 2018, 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.

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

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. Professor Danbatta is a leading academic and considered an industry expert.

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). 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.

**B Limits on Content**

*Over a dozen of the pro-Biafra websites blocked in 2017 remained inaccessible at the end of the coverage period. The presence of misleading and false information online, including through coordinated campaigns, played a notable role in public debate during the run-up to the 2019 national elections. Social media is regularly used to engage on social and political issues.*

Does the state block or filter, or compel service providers to block or filter, internet content?

Although the Nigerian government has not historically blocked websites, 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. 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 Biafran War. Although access to Naij.com was eventually restored, as of March 2019 at least a dozen of the pro-Biafra websites remained inaccessible. 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. 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? | 44 |

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, including one during the coverage period, after several years of not making any such requests. According to Facebook’s latest transparency report, there were no content restrictions between July and December 2018.

B3 0-4 pts

| Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process? | 24 |

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.

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, sparking fears of impending online censorship. 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).

B4 0-4 pts

| Do online journalists, commentators, and ordinary users practice self-censorship? | 34 |

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).

Nigeria’s LGBT+ community is marginalized, and online self-censorship is common among LGBT+ individuals. Many LGBT+ internet users report feeling unsafe using their real names online, preferring to engage anonymously. 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
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 was common at both the national and local 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. 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 study by the Centre for Democracy and Development (CDD) West Africa published in 2019 found that there was a high level of bot activity ahead of the election. The study collected 34.5 million tweets from major politicians, political parties, media houses, and other accounts that tweeted with election-related hashtags. From this data, CDD concluded that 19.5 percent of the accounts showed signs of automation.

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. The fake accounts were run by the Archimedes Group, an Israeli company, and sought to influence the 2019 Nigerian elections.

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.

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.52

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),53 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.54 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, including pidgin English.55

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? | 66 |

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).57

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 #Buhariiswinning58 and #Atikuiswinning59 to build support for their candidates.

In another example of effective digital activism, 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 2018.60

C Violations of User Rights
The Digital Rights and Freedom Bill was passed by the House of Representatives in December 2017 and the Senate in March 2018, but in March 2019 the president declined to sign it. Several arrests were reported for online activities, and one individual received a 12-year prison sentence for a post on Facebook. Intimidation and violence against journalists and activists increased, especially around the elections.

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?

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.”

Following Buhari’s rejection of the legislation, the bill was revised to address the president’s concerns and reintroduced in the House in July 2019, after the reporting period.

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.

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, which occurred without the involvement of the National Judicial Council or the National Assembly, as required by law, 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?

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 2015 Cybercrime Act 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. 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 ($50,000), or both. Recent reporting has also revealed that Section 27 of the law is being used to prosecute journalists. Section 27 criminalizes any person who “aids, abets, conspires, counsels, or procures another person(s) to commit any offence under [the Cybercrime] Act.”

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. 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. Another NGO, the Incorporated Trustees of Laws and Rights Awareness Initiative, has also filed a suit to challenge the law.

Internet freedom advocates have raised concerns that a broadly worded draft hate speech bill proposed by the Senate in March 2018 could be used by the government to silence the online activities of opposition critics and NGOs; 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 the president’s party, 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.” 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. As of March 2019, the bill had not yet been voted on in the Senate.

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? 26

Numerous bloggers, online journalists, and private citizens were arrested for their online activities during the coverage period. Most arrests were for “cyberstalking” under Section 24 of the Cybercrime Act, though no cyberstalking cases have led to convictions. Section 27 of the act is also now employed to prosecute journalists. In March 2019, Obinna Don Norman, the owner and editor-in-chief of online news outlet the Realm News, was arrested and charged under sections 24 and 27: 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.”

In April 2019, activist IG Wala was sentenced to 12 years in prison for criminal defamation and other charges arising from a 2017 Facebook post alleging
corruption in Nigeria’s National Hajj Commission. In April, Wala appealed the sentence. 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. The sentences will run concurrently, meaning Wala will spend a total of seven years in prison.

In February 2019, Chijioke Nnamani, a student at Madonna University in 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. Nnamani was arraigned in Anambra state in March on cybercrime charges, and reports suggested that he was still in detention at the end of the reporting period.

In November 2018, activist Deji Adeyanju was arrested on charges of criminal defamation and disturbance of public peace, based on his social media posts. Adeyanju had been leading a protest against the perceived partisan posture of army officers ahead of the 2019 presidential election. He was released after several days in custody and the charges were dropped. However, Adeyanju was then arrested in December 2018 in connection with a 2005 murder charge for which he had been acquitted in 2009. In February 2019, Adeyanju was released after over two months in custody and no charges were filed.

C4 0-4 pts

| Does the government place restrictions on anonymous communication or encryption? | 34 |

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

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.

Draft regulations on the interception of communications 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. The regulations have not yet been approved.

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

C5 0-6 pts

| Does state surveillance of internet activities infringe on users’ right to privacy? | 36 |
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.\(^87\)

While there is no evidence that authorities proactively monitor internet and mobile phone communications, 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.\(^88\) However, the NCC stated during a March 2018 event that “the Office of the National Security Adviser (ONSA) has a direct link to the NCC’s SIM registration database in order to monitor and apprehend criminals in the country.”\(^89\)

In March 2019, President Buhari declined to sign the 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.

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 on behalf of the ruling party. The phone numbers and locations of the call recipients were reportedly obtained from the Independent National Electoral Commission, which collects citizens’ data in 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.\(^91\) Consultations on how the regulation would be implemented continued through the coverage period,\(^92\) and the significance and effectiveness of the regulation remains unclear.

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 the Stranvisky Project 2,\(^93\) an ONSA project that was allocated 13.9 billion naira ($45.6 million) in 2017.\(^94\) Observers believe the project is for new surveillance technology. A number of other line items in the 2018 budget for the ONSA and Department of State Security were intended to increase surveillance capabilities include the “Social Media Mining Suite,” with an allocation of NGN 2.2 billion, “Wolverme Next Generation SDRIMSI” with a provision of NGN 1 billion, “Surveillance Drone” with a budget provision of NGN 1 billion, and “Mobile Surveillance Facilities” with NGN 240 million allocated, among others.\(^95\) Government officials frequently assert that new technology to fight the Boko Haram terrorist group is necessary.

The 2019 Executive Budget Proposal reveals that some of the projects named above are still on-going. The project proposal lists the “Stranvisky Project 2” as an “ongoing” project with an allocation of NGN 4 billion (US $11.1 million) for the Office of the National Security Adviser (ONSA). Social media mining suite and an item called ‘surveillance drone with precision camera $IMSI payload capabilities” are listed for the Directorate of the State Security Service, Nigeria’s Secret Police, at NGN 990,689,907 (US$ 2.7 million) and 199,786,908 (US$555,000) respectively. The “$IMSI payload capabilities” of the precision drone may refer to International Mobile Subscriber Identity-Catchers (IMSI), a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users.
In March 2019, the president 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; outline the provisions of lawful and authorized interception of communications within the digital environment without sacrificing the freedom and 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 table for his signature.

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. The active period of the contract, from 2012 to 2013, coincides with the governor’s crackdown on so-called “rumormongering” online. Citizen Lab research from 2014 also found a FinFisher command and control server located in a private ISP in Nigeria. The extent to which that surveillance system is operational is unclear.

The Draft Lawful Interception of Communications Regulation introduced by the NCC in 2013 was still being considered at the end of the reporting period. 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.

C6 0-6 pts

| Are service providers and other technology companies required to aid the government in monitoring the communications of their users? |

There are numerous legal mechanisms that compel service providers to assist the government in its efforts to monitor users’ communications.

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

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. 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.

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.” 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.\textsuperscript{109} The extent to which the guidelines have been enforced remained unclear as of 2018, as there have been no reports that international ICT companies have been compelled to comply.

The Draft Lawful Interception of Communications Regulation (see C\textsuperscript{4} and C\textsuperscript{5}) 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.”\textsuperscript{110} 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.\textsuperscript{111}

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? | 25 |

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.\textsuperscript{112}

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.\textsuperscript{113} Kunle Sanni, a reporter for the Premium Times news site covering the March elections in Plateau State, told the Committee to Protect Journalists that he was held for nearly 30 minutes and forced by three men calling themselves “farmers” to delete photos of what appeared to be underage voters.\textsuperscript{114}

C8 0-3 pts

| Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack? | 33 |

Cyberattacks against news websites, civil society groups, and human rights activists were not reported in Nigeria during the coverage period.