Mapping the supply of surveillance technologies to Africa

Nigeria country report

Patrick Allam and Lawrence Oboh
Spaces for Change

SPACES FOR CHANGE | S4C
RESEARCH | POLICY | CITIZEN ACTION

1. Introduction

In recent years, multinational technology companies around the globe have made monumental strides in building surveillance technologies with promises of detecting and preventing terrorism threats and attacks. However, beyond security concerns, evidence exists that Nigeria has been using these technologies to stifle dissent and clamp down on those perceived as critical of the ruling government, aided by a regime of repressive legislative standards (Ibezim-Ohaeri *et al.* 2021).

There appears to be no express legal limitation on who has access to these technologies. The Nigerian Customs Service (NCS), responsible for enforcing import and export restrictions and prohibitions, has completely omitted surveillance technology equipment and software of any grade from their prohibition list (NCS 2015). The arms trade restriction, regulated by the Office of the National Security Adviser (ONSA), is equally cloudy on surveillance technology. There is a mandatory requirement to obtain an End-User Certificate from ONSA prior to importation of military wares, including for surveillance and counter-surveillance equipment (ONSA n.d.). Nonetheless, this has not trickled down to limit the participation of national and subnational entities in the trade. For instance, in 2015, the Bayelsa State governor forged an End-User Certificate to procure hacking tools worth N100m (US$217,071) from the Italian firm, Hacking Team (Emmanuel 2015).

Spaces for Change, a prominent civic rights group in Nigeria, has already considered the drivers and implications of surveillance technologies in the country in its study *Security Playbook of Digital Authoritarianism in Nigeria* (Ibezim-Ohaeri *et al*. 2021). Our research contribution in this report will be a deep dive into the supply chain and how these technologies are being used to shrink the civic space in Nigeria. We will also offer an analysis of the impact of surveillance technology.

2. Background

Political history

Since independence from Britain in 1960, Nigerian politics has been riddled with issues of ethnic domination and control of governance instruments. It is therefore not surprising that the elites of tribal groups believe their interests lie in the makeup of the country leadership (Suberu 1996). Fears of ethnic dominations and scrambles for political power in part lie behind military interventions in the political governance of the country, as well as in calls for secession. Nigeria has experienced five military coups (1966–98) over a staggered period of 29 of the 62 years of the country's political independence, though since 1998, the country has had more than 20 years of uninterrupted democracy. In addition to military interventions, there have been protracted agitations for both the Biafran and Oduduwa separatist agendas in the southeast and southwest of the country respectively (Ibeanu, Orji and Iwuamadi 2016; Ajala 2009), while the Boko Haram insurgency armed conflict has raged in northern Nigeria since 2011 (Global Conflict Tracker n.d.).

The country has had a series of constitutions. The first, in 1963, was modelled on the British parliamentary system. It established Nigeria as a republican state with an indigenous president (Ejemheare 2019). The second, enacted in 1979, abandoned the British parliamentary system of government in favour of a US-style presidential system with direct universal suffrage elections (Aluko and Ediagbonya 2020). The military regime enacted the third constitution in 1993 with the aim of returning to democratic rule. However, its implementation was short-lived and ended by a counter-coup. Military rule then continued until the fourth republic constitution in 1999, which has remained in force to date (Nwodim and Adah 2021). This marks the longest democratic rule in the history of the country.

Colonial patterns of surveillance

The historical perspectives that underpin the thinking behind general surveillance of citizens in Nigeria dates back to the colonial era. The different indigenous governance systems in the country's three major regions resulted in the adoption of different colonial governance methods. For instance, in the northern and western regions, people were ruled via an indirect rule system, where the colonial masters ruled through traditional rulers. The eastern region had a decentralised system of governance, hence preference for direct rule through warrant chiefs appointed by the colonial masters (Perham 1962). Regardless of the system adopted, those charged with responsibility

were also required to conduct surveillance on the people they governed on behalf of the colonial government (Afeadie 1994).

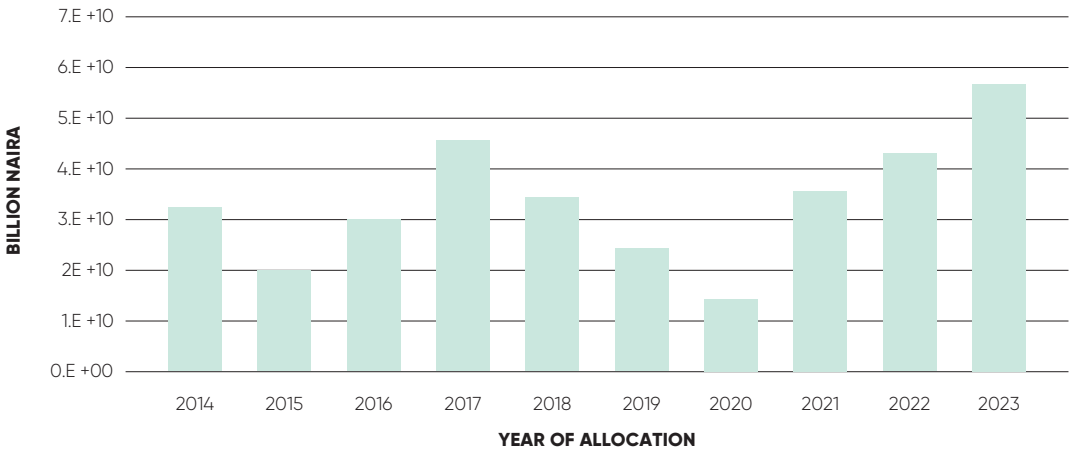
Surveillance under military rule

Nigeria has witnessed 11 coups, counter-coups, and abortive coups in its post-independence history. In the pre-digital era, private letters were intercepted and read before being sent to the rightful recipient (Amuwo 2001). In some cases, all senior functionaries and journalists were subject to massive regime surveillance programmes (Abiodun 2016). For instance, in 1985, Major General Babangida, while addressing the country after a successful coup, alleged that his predecessor spied on all members of the supreme Military Council and that his telephone was bugged (Macleo 2012). These were rampant pre-digital surveillance practices in Nigeria. Unfortunately, they persisted during the democratic era with the use of new technologies. As a result, despite a legal right to privacy, information capture to monitor Nigerian citizens' activities has increased in recent years (Oloyede 2021).

Surveillance in the democratic era

Under the pretext of curbing insecurity and extreme violence, the Nigerian government has deployed a massive wave of surveillance on citizens. Huge budgetary allocations have been approved by the federal and state parliaments for acquisition of intrusive spywares. For instance, between 2014 and 2023, the federal government approved a total budget expenditure for the National Security Adviser (NSA), the Directorate of State Security Services (DSSS), and the National Intelligence Agency (NIA) of over N336bn (US$733m) (Paradigm Initiative 2017; Budget Office of the Federation n.d.). These agencies are only a fraction of the agencies entitled to security allocations for the procurement of surveillance equipment in Nigeria. The armed forces and agencies such as the Nigerian Police Force, the Economic and Financial Crimes Commission, the Nigerian Immigration Services, and a host of others have not been considered here. The NSA, DSSS, and NIA stand out because of the specific budgetary proposal to procure surveillance equipment and technologies.

Figure 2.1 Chart of budgetary allocations to NSA, DSSS, and NIA over a ten-year period



Source: Authors' own. Created using data from Paradigm Initiative (2017) and Budget Office of the Federation (n.d.).

According to figures from the Budget Office of the Federation (n.d.), allocations to the three agencies fell by 4 per cent in 2015. This may be connected to the advent of a new administration, which spoke passionately of commitments to respecting human rights and curbing corruption among government security agencies. However, from 2016 to 2017, allocations increased by 8 per cent. The government increasingly came under criticism over the handling of the affairs of government. It was within the same period that the government not only scaled up surveillance programmes but also sought to pass laws that increased state actors' policing powers. Government spending on surveillance dropped from 2018 to 2020 by 6 per cent, perhaps partly influenced by the Covid-19 pandemic which saw a general cut on most government spending other than health. There has been consistent growth since the Covid-19 pandemic at a rate of 13 per cent.

In addition, government policies such as mandatory enrolment for the national identification number (NIN) and bank verification number (BVN), as well as linking SIM cards to NIN, are known data-harvesting schemes (Ibezim-Ohaeri *et al*. 2021: 13). The Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations requires mobile phone users to consent to the collection of their fingerprints and facial images as a precondition to their SIM card registration (FRN 2011). Data privacy concerns accompany these measures, which have large implications for enabling state surveillance on private citizens, although the official justification for them has always been the need for proactive measures to curb crime (Adebayo 2020).

3. Supply of surveillance technology

The surveillance supply chain in Nigeria includes a variety of companies and organisations that produce, distribute, and install surveillance equipment, as well as provide related services such as training and maintenance. They include manufacturers of surveillance cameras, recorders, and other equipment, as well as distributors, system integrators, and service providers. The major players are foreign companies, in some cases working in partnership with local companies. In most instances, these local companies are companies incorporated by politicians as special purpose vehicles (SPVs) or through legal partnerships with the supplying companies which hold SPVs as their local partners (Ibezim-Ohaeri *et al.* 2021: 49). These companies sell their products to a variety of customers, including government agencies, private businesses, and individuals.

It is important to note that there is remarkable difficulty identifying players in the surveillance supply chain in Nigeria. This is because of the Official Secrets Act, which criminalises the transmission, acquisition, or reproduction of documents designated as classified (Official Secrets Act 2004, s1) (PLAC). Equally, there is no official publication on this subject. The Freedom of Information Act (FoI Act) has done little to ameliorate the situation. In fact, the FoI Act waters down all critical freedoms of information by subjecting requests to public institutions to the discretions of officials (FoI Act 2011, s28[1]). This report, while relying on open-source documents, will limit its focus to five major surveillance categories.

Internet interception

Internet interception allows for the tracking of physical and digital activities of a target internet user. Interception can be either lawful or unlawful. The Lawful Interception of Communications Regulation 2019 (LICR) (FRN 2019), a subsidiary legislation of the Nigerian Communications Act 2003 (FRN 2003), expressly allows interception of communications in Nigeria. The law empowers state actors, unilaterally or in concert with telecommunication companies, to intercept and store any communication within and outside the country (LICR 2019, s6). Where intercepted communications are encrypted, the law empowers state actors to request the disclosure of the protected or encrypted communication from third parties such as platform administrators and communication device manufacturers. State actors may seek foreign assistance where the key or code to decrypt such communication is in possession of any person outside

1 Laws of the Federation of Nigeria, **Freedom of Information Act 2011**.

Nigeria (LICR 2019, s9). This law, notwithstanding any other law in force, equally requires telecommunication companies to take necessary steps to acquire and install interception capabilities and devices to enable monitoring and interception of communications (LICR 2019, ss10 and 11).

The LICR was only a sanction on entrenched government practices and mechanisms to intercept and monitor communications in Nigeria. For instance, in 2013, six years before the LICR, the Nigerian government under the administration of President Goodluck Ebele Jonathan awarded a US$40m contract to an Israeli arms manufacturing company, Elbit Systems, to secure a sophisticated cyber-defence tool, Wise Intelligence Technology (WiT). This system is believed to be capable of monitoring internet communications (Johnson 2013). The following year, 2014, in preparation for the 2015 general election, the Nigerian government engaged Romix Technologies, a Cyprus-registered company, and Packets Technologies, an Israeli company, on a US$2m contract to supply and install cyber-intelligence system software. The spyware was expected to conduct distributed denial of service (DDoS) on websites critical to the then president's political ambitions (Emmanuel 2016).

State-level governments in Nigeria's government system have also acquired and used some of these technologies against political opponents (*Premium Times* 2016). In 2013, the governor of Bayelsa State, Henry Seriake Dickson, illegally purchased a high-calibre Remote Control System (RCS) from Hacking Team at a cost of N98m (Emmanuel 2015). This is an invasive and ruthless technology with the ability to compromise most operating systems, scoop metadata from targets and scoop the content of targets' private communications. In the lead-up to the 2015 elections in Bayelsa State, Dickson used this spying tool to spy on his prime challenger, Timipre Sylva, and on Sylva's wife, aides, and loyalists (Ibezim-Ohaeri *et al*. 2021). Although the application of the LICR does not include subnational governments and agencies, evidence shows patronage from these secondary arms of government.

Mobile interception

There is an acknowledged difficulty in tracking, monitoring, and investigating mobile interception surveillance, often attributed to the discreet nature of such operations and the scarce traces they leave behind (Marzak *et al*. 2020: 2). Nigeria is believed to have procured a wide range of mobile surveillance equipment. Existing circumstantial evidence suggests that the Nigerian government procured FinFisher, an advanced commercial spyware programme created and marketed by UK/German company Gamma International. The spyware is believed to have extensive user-surveillance capabilities through the delivery of malware that remotely

activates features on target devices, such as microphones and cameras, to record and transmit data to their users (Glazova 2021). According to the approved 2017 budget of Nigeria, the DSSS, through budget code DOSSS86693049, proposed procurement of 'FinFisher equipment' for N70.4m (Paradigm Initiative 2018: 7). The Surveillance Industry Index (SII) had long suggested the existence of FinFisher command and control servers in Abuja (Marczak *et al*. 2020: 9), and FinFisher customers, identified through the analysis of support requests, offer circumstantial evidence of Nigeria's patronage of the sophisticated spyware. The actual contract and supply of this technology to Nigeria, like many security contracts, is shrouded in secrecy.

There are suggestions that Nigeria has also acquired the Israeli GI2 IMSI Catcher[2] developed by Verint Systems (Emmanuel 2016). According to an official at Verint Systems, this spyware is capable of accurately locating target mobile devices and extracting information from GPS coordinates to allow monitoring of calls and text messages without disabling the target's ability to communicate (Turniansky 2010). Mi Marathon Resources, an Australian company, via M.I. Smart Solutions, a Nigeria-registered company, is believed to have supplied the surveillance spyware to ONSA in April 2014 (Ibezim-Ohaeri *et al*. 2021: 46). The contract documents cited by *Premium Times* disclose that the NSA ordered two units of the Engage GI2 Tactical Solution at a cost of US$841,000 per device. However, only one GI2 IMSI Catcher was supplied at a cost of US$329,800 (Emmanuel 2016).

In 2014, Mi Marathon Resources was further reported to have supplied another mobile interception spyware, Fiber Optic Landing Solution, worth N712.2m to ONSA to enable the office backend access to all fibre-optic cables landing in Nigeria (Emmanuel 2016; Ibezim-Ohaeri *et al*. 2021). Though the contract for the supply of this technology was said to be executed by the secretary to the NSA, there is no evidence to show the actual supply or use of this technology in Nigeria. However, inferring from Article 10 of LICR 2019 (FRN 2019), such spyware may have been installed in compliance with the extant regulation for telecommunication installations in Nigeria. The Economic and Financial Crimes Commission (EFCC) has equally procured a universal forensics extraction device (UFED) from Israeli company Cellebrite to access, collect, and preserve data from mobile phones, computers, and storage devices. Quoting a source within the EFCC, the Cellebrite website disclosed patronage from the law enforcement agency and subsequent use of the UFED for investigation in Nigeria. The Committee to Protect Journalists has

2 An 'IMSI catcher' is an eavesdropping device that locates and then tracks all mobile phones within an area by pretending to be a mobile phone tower. It tricks nearby mobile phones to connect to it, which then allows it to intercept the data from connected phones to the cell tower without the phone user's knowledge (Privacy International 2021).

since confirmed the use of Cellebrite technology against journalists in Nigeria (Oloyede 2021).

Circles, affiliated to Israeli NSO Group, stands out as the biggest supplier of surveillance technology to Nigeria, with clients spanning federal government agencies, subnational governments, and independent security outfits (Ibezim-Ohaeri *et al*. 2021). The Bulgarian-produced spyware exploits the vulnerabilities of Signalling System 7 (SS7) in the global mobile phone system to snoop on calls, texts, and locations of phones around the globe (Marczak *et al*. 2020). In October 2010, the Nigerian Police Force acquired the Circles system with an annual subscription fee of N63m. The contract for the project was awarded by the Ministry of Police Affairs to an Israeli-owned but Abuja-based security firm, V&V Nigeria. The contract was tagged 'procurement of strategic GSM Tracking System for the Nigeria Police Force and expansion/upgrade of the existing system with the DSSS' (Mojeed 2015). Less than two months later, another N2.61bn contract was awarded by the same Ministry of Police Affairs to a British security firm, Gamma TSE, 'for the procurement of Strategic GSM Tracking and Interception Systems for the Department of State Security Services' (*ibid*.).

Subnational governments have equally participated in the procurement of spyware with, in some cases, private businesses acting as intermediaries to facilitate their importation. For instance, Chibuike Rotimi Amaechi, then governor of Rivers State, acquired Circles spyware through V&V Nigeria at a cost of N2.3bn in 2010 (Ogundipe 2017), one of many incidents showing the participation of private businesses in the importation of sophisticated surveillance technology into Nigeria, contrary to merchant claims of selling only to governments. Two years earlier in 2008, Amaechi[3] had picked up a similar gadget, the C4i (Command, Control, Communications, Computers and Intelligence) technology, from the company MPD Systems – a security firm based in the US (Emmanuel 2016).

In some cases, technologies have been purchased with huge annual subscription fees, passed on to succeeding administrations. Under the pretext of combating insecurity, subsequent administrations in the various states have perpetuated the use of spywares on perceived political opponents (Ibezim-Ohaeri *et al*. 2021). For instance, Emmanuel Uduaghan, then governor of Delta State, purchased the 3G surveillance equipment from Circles for N1.5bn in February 2012 and paid a yearly service fee of N31.9m (Ogundipe 2017). Ifeanyi Okowa, successor to Uduaghan, on assuming office immediately signed a memorandum to continue subscribing to the equipment for two years (*Premium Times* 2016). Seriake Dickson, as governor

3 Mr Chibuike Rotimi Amaechi was the governor of Rivers State from 2007 to 2015. He is currently the federal Minister of Transportation.

of Bayelsa State, in the same year also purchased the Circles surveillance equipment for N1.7bn with an annual maintenance fee of N31.9m from Nice Security, a UK-based company (Emmanuel 2016; Ibezim-Ohaeri *et al*. 2021).

Social media monitoring

Some of the most widely used social media apps in Nigeria are Twitter, Facebook, Instagram, WhatsApp, and TikTok. There is evidence to show that the Nigerian government possesses spyware used for social media surveillance. In 2017, speaking on national TV, a military spokesperson disclosed that the military has 'strategic media centres that monitor the social media to enable it [the military] to sieve out and react to all posts that are anti-government, anti-military and anti-security'. He further explained that the military has scientific measures to be able to sieve this information (Paradigm Initiative 2018: 7). This statement is a clear admission that the government, through some of its agencies, is monitoring social media activities in the country.

According to a report from the Budget Office of the Federation, the Nigerian government allocated N2.2bn (US$6.6m) in its 2018 budget to procure 'Social Media Mining Suite'[4] (Shahbaz and Funk 2019). Further substantiating this report, President Muhammadu Buhari, while delivering his 2018 budget speech, stated, '… we have also increased our focus on cyber-crimes and the abuse of technology through hate speech and other divisive material that is being propagated on social media' (Buhari 2017: 17). While the supplying companies of these technologies are generally unknown, budgetary allocations for the procurement of social media surveillance equipment continue to be made each year. For instance, under the 2021 supplementary budget alone, the National Assembly approved N4.9bn for the NIA to procure equipment to monitor WhatsApp messages, phone calls, and text messages, among others (Iroanusi 2021). Similarly, the National Assembly approved over N7.46bn for the DSSS to launch an 'independent lawful interception platform for voice and advanced data monitoring' (Uduu 2021).

Private individuals have also been involved in the importation of social media surveillance into Nigeria. A UK newspaper reported that, in 2015, a Nigerian billionaire interested in the re-election of the then president, Goodluck Jonathan, engaged UK company SCL Elections, the parent company of Cambridge Analytica, for an estimated US$2.8m fee to improperly swipe data from Facebook to sway voters against an opposition candidate (Cadwalladr 2018). According to his testimony to the newspaper, whistle-blower Christopher Wylie, who worked with a University of Cambridge

4 Also known as the Social Media Mining Toolkit, this is spyware used to harvest and process large amounts of personal data from social media platforms for the surveillance and profiling needs of a user.

academic to obtain the data, said: 'We exploited Facebook to harvest millions of people's profiles and built models to exploit what we knew about them and target their inner demons' (*Premium Times* 2018).

Smart city/safe city projects

'Smart cities have become controversial for commodifying digital spaces, exploiting citizens' data without consent, reinforcing spatial inequalities and undermining their right to protect their data' (Duncan 2022: 117). In 2008, the late President Umaru Musa Yar'Adua's administration awarded a US$470m contract to a Chinese company, ZTE, to procure and install CCTV cameras in Lagos and the Federal Capital Territory (FCT), Abuja (*Punch* 2021). The Chinese Export-Import (Exim) Bank of China provided the Nigerian government with a loan of US$399.5m to fund the project, while the federal government paid the remaining US$70.5m as counterpart funding (*ibid.*). However, most of the CCTV systems soon failed due to poor maintenance. In 2020, the federal government entered into a concession agreement with MPS Technologies, a Nigerian SPV, to replace all broken and vandalised CCTV cameras already installed under the previous project.

At the subnational level, many state-level governments, to bolster their security and economies, have embarked on varieties of smart/safe city projects. The Kaduna State government in 2016 budgeted N2.55bn to procure CCTV cameras and drones to provide security cover within the state (*Premium Times* 2016). The Lagos State government seems to be leading the campaign for a smart and safe city (Oolasunkanmi 2021), and in June 2016, with Dubai Holding, it signed a memorandum of understanding (MoU) to develop 'sustainable smart, globally connected knowledge-based communities that support knowledge economy in Ibeju-Lekki', a suburb of Lagos (*The Guardian* 2016). In addition, the Lagos State government in the same year approved a total of N9.6bn for the development of ICT infrastructure, including smart city initiatives to enhance state security. These gadgets have already been mounted at major points in Lagos (*The Nation* 2017). The vendors contracted for these projects are unknown. However, surveillance cameras have since been installed in most parts of the state.

Similarly, the Niger State government in 2021 commissioned and received a feasibility report from South Korean company DOHWA Engineering on the development of Suleja Smart City (*Arewa Reporters* 2021). In Kano State, the government contracted a Nigerian company, Vestigio Technology Solutions, 'to install CCTV cameras across Kano metropolis and other parts of the state to provide 24/7 video surveillance of streets, roads, markets, junctions and many areas of interest' (*Nigerian Tracker* 2020). The programme is expected to be able to 'identify colour, number plates, brand of vehicles, the driver and passengers… [and] send signals to patrol cars and the control room

[as well as] identify faces [to] determine whether [a person is] happy or sad' (Adegbamigbe 2021). Kogi State government has recently joined the league of state-level governments with intrusive surveillance technology. The Kogi State government signed an MoU with a Chinese company, Hytera Communications, for the supply of a 'state-wide digital surveillance for improved security' (*The Cable* 2022). According to a Kogi State official, the project is about:

> *putting the whole state on the map real-time, virtual, audio and visual. The idea is that the moment you come into the state, we'll see you; if you're driving, walking or talking, we'll be able to pick it. If you do something wrong, we'll be able to intercept you using our field personnel on the ground.*
> (*Ibid.*)

Recently, governor Bello Matawalle of Zamfara State signed an MoU with a Dubai-based company, Worldwide Jet Aviation, to supply MBB BO105 Bell 206 surveillance helicopters to carry out aerial surveillance in the state. A Zamfara State official explained that the expected 'American model choppers have been remodelled for advanced security surveillance with attached cameras capacities as well as… tracker systems' (Umar 2020).

Deployment of e-border facilities has equally received a boost in Nigeria. The Nigerian government is investing huge sums of money in border surveillance. For instance, in 2019, the federal government of Nigeria approved N52bn for an e-border project expected to be implemented by Huawei, a Chinese technology vendor. The project includes the installation of surveillance cameras across the country's borders for real-time monitoring (Akintaro 2022).

Biometric ID

In Nigeria, biometric enrolment is required at almost every civic and social activity. There has been a surge in biometrics deployment by public and private actors, ranging from identity verification to travel documentation to financial inclusion (Ibezim-Ohaeri *et al*. 2021: 13). These deployments raise concerns that are not adequately addressed by the current human rights and data protection frameworks (European Commission Joint Research Centre 2005). The biometric technology supply chain shows that fingerprints and facial capture are the most widely harvested specimens in Nigeria. In 2012, Thales Solutions, a French company working in cooperation with a Nigerian company, Auspoint, was selected to supply Nigeria's multi-purpose electronic identity card gadgets for fingerprint and facial capture (Thales Group n.d.). This move was one of the key policy objectives of the Nigerian

government to stimulate the implementation of a digital identity programme. The World Bank, Agence Française de Développement (AFD), and the European Union (EU) funded implementation of the programme to the tune of US$433m (Adepetun 2020). As at October 2022, the number of NINs issued to Nigerians by the National Identity Management Commission (NIMC) reached 90.6 million (Adepetun and Oderemi 2022).

Another company facilitating biometric capture in Nigeria is Dermalog Identification System, based in Germany. In 2014, the company signed a contract with the Central Bank of Nigeria (CBN) to supply Dermalog LF10 and its operating software for US$50m for the implementation of BVNs in Nigeria. The project was described as 'the most comprehensive biometric project in Nigerian history' (PR Newswire 2014). According to the Nigerian Inter-Bank Settlement System (NIBSS), BVN enrolment as of 1 January 2023 stood at 56.5 million bank customers in Nigeria (NIBSS n.d.).

Following the decentralisation of enrolment for the NIN by the NIMC in 2020, and licensing of public agencies and corporate businesses to undertake the enrolment (Emego 2020), Sterling Bank Nigeria struck a deal with BIO-key International, a US company, to supply Pocket10 mobile FAP50 fingerprint scanners for US$45m in early 2020 (Burt 2022). The enrolment initiative was said to be co-funded by the World Bank and supported by the United Nations and Nigerian federal government as part of the country's digital identity inclusion drive (*ibid*.). Also, Airtel Nigeria, a telecommunications operator, signed a contract with Chongqing Huifan Technology, registered in China, for the supply of customised Huifan android handheld fingerprint terminal FP05 to facilitate SIM card registration (HF Security n.d.).

The questions that arise when biometric technology is integrated into crucial parts of Nigerian life, such as immigration, national identification, and bank accounts, are: what happens when the biometrics identification is turned off against a person on any of these platforms?; and, are there actions that must be completed before such deactivation can begin?

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Naira (N)	US$
Internet interception			
Elbit System (Israel)	Wise Intelligence Technology (WiT) – can monitor computer and internet communications (2013, NSA)	6.4bn	40m
Romix Technologies (Cyprus), with Packets Technology (Israel)	Cyber-intelligence software – can conduct DDoS on websites (2014, NSA)	398m	2m
Hacking Team (Italy)	To hack computers and phones (2013, governor of Bayelsa State)	98m	215,800
Mobile interception			
Gamma International (UK/Germany)	FinFisher spyware – can remotely activate mobile phone features to record and transmit target's data (2017, DSSS)	70.4m	153,000
Mi Marathon Resources (Australia) via M.I. Smart Solutions (Nigeria)	GI2 IMSI Catcher – can locate and extract information on a target's mobile phone (2014, NSA)	151.8m	329,800
Mi Marathon Resources (Australia)	Fibre-optic landing solution can create backdoor access to fibre-optic cables (2014, NSA)	712.2m	1,533,274
Cellebrite (Israel)	Cellebrite UFED and Cellebrite Pathfinder – can collect data from mobile phones, computers, and storage devices (unknown, Economic and Financial Crimes Commission)	Unknown	Unknown
Circles (Israel)	Spyware (2010, Nigerian Police Force)	Annual subscription fee of 63m	136,780
Gamma TSE (UK)	Strategic GSM tracking and interception system (2010, Nigerian Police Force)	2.61bn	5.66m
V&V Nigeria	Circles spyware – can spy on private communication (2010, governor of Rivers State)	2.3bn	4.9m
MPD Systems (USA)	C4i Technology – can monitor calls and track location of users (2008, governor of Rivers State)	Unknown	Unknown
Circles (Israel)	Spyware (2012, governor of Delta State)	1.5bn	3.25m
Nice Security (UK)	3G communication interception spyware (2012, governor of Bayelsa State)	1.7bn	3.69m
Social media monitoring			
Unknown	Social Media Mining Suite (2018, DSSS)	2.2bn	6.6m
Unknown	Social Media Mining Suite (2021, DSSS)	4.8bn	12.32m

Contract	Description (contract date, buyer/user)	Nzaira (N)	US$
Cambridge Analytica (UK)	Technology which can harvest Facebook profiles for targeted messaging (2015, private businessman)	1bn	2.8m
Safe cities			
ZTE (China)	CCTV cameras to monitor movement and traffic (2008, federal government)	216. 4bn	470m
MPS Technology (Nigerian SPV)	Contract to repair and replace CCTVs in major cities (2020, federal government)	Unknown	Unknown
Huawei (China)	e-border project (2019, federal government)	52bn	112.9m
Unknown	Cameras and drones for surveillance (2016, Kaduna State government)	2.55bn	5.4m
Dubai Holding (United Arab Emirates)	CCTV cameras for security and traffic management (2016, Lagos State government)	Unknown	Unknown
DOHWA Engineering (South Korea)	CCTV cameras for security and traffic management (2021, Niger State government)	Unknown	Unknown
Biometric ID			
Thales Solutions (Singapore subsidiary of a French company)	Facial and fingerprint biometric capture (2012, NIMC)	199.4bn	433m
Dermalog Identification Systems (Germany)	Facial and fingerprint biometric capture (2014, Central Bank of Nigeria)	23bn	50m
BIO-key International (USA)	Pocket 10 mobile FAP50 fingerprint scanner for biometric capturing (2020, Sterling Bank Nigeria)	20.7bn	45m
Chongqing Huifan Technology (China)	Android handheld fingerprint terminal FP05 for SIM registration (unknown, Airtel, Nigeria)	Unknown	Unknown
	Total	1.2tn	1.2bn

Source: Authors' own. Created using data and figures as referenced in the research paper.

4. Impacts

As there are no specific laws against the supply or importation of surveillance technology in Nigeria (Oloyede 2021), limitations on the trade are inferred from other laws protecting privacy. For instance, the Constitution of the Federal Republic of Nigeria[5] (as amended) 1999 recognises the right to privacy as a fundamental right of its citizens, free from interference from the government, its agencies, or anyone else. Section 37 provides that 'the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected'. This is the foundation upon which other privacy laws/regulations rest.

However, Section 45 of the same constitution allows the derogation from these rights on grounds such as defence, public safety, public order, public morality, or public health. Article 7(3) of the Lawful Interception of Communications Regulation 2019 has equally provided grounds for justifying interception, with national security at the top of the list.

More telling, acquisition of surveillance technologies is often limited by the requirement to obtain End-User Certificates from ONSA (ONSA n.d.). There are doubts as to whether these powers enjoy legislative backing; however, ONSA exercises these powers with the cooperation of the Nigerian Customs Service (*Premium Times* 2022). Perhaps these powers are inferred from the discretionary powers of the president to add to the responsibilities of ONSA matters relating to internal security of the country (National Security Agencies Act 1986, s3(c)[6]).

There is also the concern of dignity of the human person provided in Section 34 of the 1999 constitution regarding biometric capture. Consent extracted during enrolment for all state-mandated biometric capture is often a matter of legal compliance. People are exposed to risks that can only be imagined in the event of data collected falling into the hands of unauthorised persons with sinister intentions. In the past, there have been attempts by some civil society groups to stop government acquiring surveillance technologies (Ojo 2013). However, these conversations are only beginning to take centre stage in public discourse.

The demand side of these surveillance technologies includes a wide spectrum of actors, ranging from the federal government, federal law enforcement agencies, public and private financial institutions, subnational governments, and private businesses. This acutely contradicts assertion by

5 **Consitution of the Federal Republic of Nigeria**.
6 **National Security Agencies Act**.

surveillance technology merchants that they sell only to law enforcement agencies. Some of these technologies are procured with enormous annual maintenance and subscription fees which importing agencies pay to these companies. The lucrative nature of this trade is a testament to its persistence and patronage over the years despite evidence of human rights breaches. For instance, the known contract sums for the procurement of surveillance technologies in Nigeria between 2008 and 2021 are over N1.2tn (US$1.2bn). This sum does not take into account undisclosed contract sums curated in this report. It also excludes other budgetary allocations for procurement of surveillance equipment within the period.

These surveillance technologies have been found to be used for more than the often-projected security and financial inclusion concerns. Reported incidents of spying, hacking, and over-harvesting biometric features have been widespread in Nigeria. Contrary to constitutional guaranteed rights and freedoms, laws, policies, and regulations have been promulgated by the legislature under the pretext of national security as allowed by the constitution to justify the procurement and use of these surveillance technologies. More telling, the importation of these surveillance technologies is loosely spread among different agencies of government with considerable discretion on deployment and use.

5. Solutions

We recommend express legislative enactments to limit the importation of surveillance technology into the country to a single designated agency of the federal government. The agency should have exclusive oversight over the deployment and use of the technologies. Such legislation should ensure abolition of surveillance technologies on civilian targets. Civil society organisations must seek to understand and increase this advocacy while actively sponsoring bills that protect the civic space.

6. Surveillance stories

Aminu Adamu Muhammed's story affirms the indiscriminate deployment of social media monitoring surveillance technology on citizens. Muhammed, a student of Federal University Dutse, had, in June 2022, posted on Twitter that the wife of President Buhari had suddenly put on a lot of weight after taking part in plundering the nation's meagre resources as the masses endured hardship under her husband's brutal regime. On 8 November 2022, members of the State Security Service trailed Muhammed to his university and arrested him (Closing Civic Spaces 2022). More importantly, Solomon Akuma, a pharmacist, was arrested on 2 April 2020, in Aba, Abia State, for allegedly making a social media post critical of President Buhari and his late chief of staff, Abba Kyari. Akuma was held in detention for three months without trial. He was eventually arraigned for charges of terrorism, sedition, criminal intimidation of the president, and threat to the life of the president (*ibid*.).

Another case is Emeka Richmond Ngornadi who the DSSS trailed for two years and eventually arrested and detained in April 2021. Allegations against him included that he used social media to drum up support for the Indigenous People of Biafra and to condemn security agents for extrajudicial killings in the eastern region of the country. Emeka was arrested while travelling from Lagos to Anambra State to deliver baby items and goods to his pregnant wife. His wife eventually gave birth in June 2021 but she lost the baby, allegedly due to psychological trauma from the arrest of her husband (*ibid*.).

One case illustrating the real anxieties behind biometric identification is that of Omoyele Sowore. The Nigerian government deactivated the biometric identification of Sowore, a human rights activist and former presidential candidate, in January 2022 (*ibid*.). The activist's national identification card, permanent voter card, foreign passport, and driver's licence were among the documents to be deactivated. Because the cards cannot be read biometrically, Sowore was then unable to use any of the above-mentioned IDs because they could not be read as a result of his biometrics being deactivated (*ibid*.).

References

Abiodun, A. (2016) 'Media, Military and Democratic Struggles in Nigeria: Tensions and Contentions', *New Media and Mass Communication* 47: 16–21

Adebayo, O. (2020) '**Nigeria: Considering the Legal Tenability of the Implementation of New Sim Registration Rules**', *Mondaq*, 31 December (accessed 13 January 2023)

Adegbamigbe, A. (2021) '**Surveillance Security: The Kano Example**', *PM News*, 5 June (accessed 3 January 2023)

Adepetun, A. (2020) '**Why Identity Matters for Nation's Development**', *The Guardian*, 27 May (accessed 6 January 2023)

Adepetun, A. and Oderemi, C. (2022) '**NIMC Registers 90.6 Million NIN as Teething Problems Persist**', *The Guardian*, 3 November (accessed 6 January 2023)

Afeadie, P.A. (1994) 'Adamu Jakada's Intelligence Reports 1899–1901', *Sudanic Africa* 5: 185–223

Ajala, A.S. (2009) ***Yoruba Nationalist Movements, Ethnic Politics and Violence: A Creation from Historical Consciousness and Socio-Political Space in South-Western Nigeria***, Working Paper 105, Mainz: Institute for Ethnology and African Studies, Johannes Gutenberg University (accessed 7 February 2023)

Akintaro, S. (2022) '**FG to Deploy Surveillance Cameras for Security at Nigerian Borders**', *Nairametrics*, 25 May (accessed 2 January 2023)

Aluko, Y.E. and Ediagbonya, M. (2020) '**The Fall of the Second Republic of Nigeria, 1979–1983: A Lesson for the Future**', *International Journal of Scientific Research and Engineering Development* 3.2: 806–27 (accessed 7 February 2023)

Amuwo, K. (2001) '**Introduction: Transition as Democratic Regression**', in D.C. Bach and Y. Lebeau (eds), *Nigeria during the Abacha Years (1993–1998): The Domestic and International Politics of Democratization*, Ibadan: IFRA-Nigeria, DOI: 10.4000/books.ifra.632 , M. (accessed 10 August 2023)

Arewa Reporters (2021) '**Korean Firm Submits Suleja Smart City Report to Niger State**', 8 July (accessed 2 January 2023)

Budget Office of the Federation (n.d.) ***Budget Documents 2018–2023*** (accessed 7 February 2023)

Buhari, M. (2017) '**Speech: President Buhari's 2018 Budget Address**', Federal Government of Nigeria, 8 November (accessed 24 May 2023)

Burt, C. (2022) '**BIO-key to Supply Tens of Thousands of Mobile Biometric Scanners for NIN Enrollment Through Bank**', *BiometricUpdate.com*, 1 March (accessed 6 January 2023)

Cadwalladr, C. (2018) '**Revealed: Graphic Video Used by Cambridge Analytica to Influence Nigerian Election**', *The Guardian*, 4 April (accessed 17 January 2023)

Closing Civic Spaces (2022) '**SSS Arrests Twitter User for Saying Aisha Buhari's Size Exploded after Eating Nigerians' Money**', 8 November (accessed 8 February 2023)

Duncan, J. (2022) National Security Surveillance in Southern Africa: An Anti-Capitalist Perspective, London: Bloomsbury Publishing

Ejemheare, I.J. (2019) '**The Nigerian First Military Coup and its Implications on Inter-Group Relations**', *RIMA International Journal of Historical Studies (RIJHIS)* 4.1: 293–310 (accessed 7 February 2023)

Emego, J. (2020) '**With Decentralisation, NIMC Targets 200m NIN Registration**', *This Day* (accessed 3 January 2023)

Emmanuel, O. (2016) '**How Jonathan Government Paid Companies Linked to Doyin Okupe to Hack "Unfriendly" Websites**', *Sahara Reporters*, 19 January (accessed 13 January 2023)

Emmanuel, O. (2015) '**INVESTIGATION: Bayelsa Governor Forges End User Certificate to Procure N100M Hacking Tools**', *Premium Times*, 15 July (accessed 13 January 2023)

European Commission Joint Research Centre (2005) ***Biometrics at the Frontiers: Assessing the Impact on Society***, Technical Report (accessed 13 January 2023)

FRN (2019) '**Lawful Interception of Communications Regulations, 2019**', *Federal Republic of Nigeria Official Gazette* 106.12: B105–18 (accessed 24 May 2023)

FRN (2011) '**Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011**', *Federal Republic of Nigeria Official Gazette* 98.101: B1125–34 (accessed 6 January 2023)

FRN (2003) '**Nigerian Communications Act, 2003**', *Federal Republic of Nigeria Official Gazette* 90.62: A287–349 (accessed 24 May 2023)

Glazova, J. (2021) '**FinSpy: The Ultimate Spying Tool**', *Kaspersky Daily*, 8 October (accessed 2 January 2023)

Global Conflict Tracker (n.d.) ***Violent Extremism in the Sahel*** (accessed 23 February 2023)

HF Security (n.d.) ***Biometric Projects We Did in Nigeria*** (accessed 13 January 2023)

Ibeanu, O.; Orji, N. and Iwuamadi, C.K. (2016) ***Biafra Separatism: Causes, Consequences and Remedies***, Enugu: Institute for Innovations in Development (accessed 7 February 2023)

Ibezim-Ohaeri, V. *et al.* (2021) ***Security Playbook of Digital Authoritarianism in Nigeria***, Lagos: Action Group on Free Civic Space (accessed 2 May 2023)

Iroanusi, Q. (2021) '**Nigerian Govt Moves to Control Media, Allocates N4.8bn to Monitor WhatsApp, Phone Calls**', *Premium Times*, 12 July (accessed 2 January 2023)

Johnson, J. (2013) '**Scandal in Nigeria Over Israeli Arms Firm's Internet Spying Contract**', *The Electronic Intifada*, 2 July (accessed 13 January 2023)

Macleo, P. (2012) ***Nigerian Military Rule in Perspective*** (accessed 23 February 2023)

Marczak, B.; Scott-Railton, J.; Rao, S.P.; Anstis, S. and Deibert, R. (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles***, Citizen Lab Research Report 133, Toronto: University of Toronto (accessed 2 January 2023)

Mojeed, M. (2015) '**EXCLUSIVE: Nigerians Beware! Jonathan Procures N11 Billion Equipment to Tap Your Phones**', *Premium Times*, 26 February (accessed 13 January 2023)

NCS (2015) ***Import Prohibition List***, Nigeria Customs Service, Federal Government of Nigeria (accessed 15 August 2023)

NIBSS (n.d.) ***BVN***, Nigeria Inter-Bank Settlement System (accessed 1 January 2023)

Nigerian Tracker (2020) '**Vestigio Technology Works with Kano Govt to Install CCTV Cameras**', 22 September (accessed 16 May 2023)

Nwodim, O. and Adah, R.U. (2021) '**Colonial Policies and Post-Independence Development in Nigeria**', *International Journal of Social Science and Human Research* 4.4: 795–802 (accessed 23 February 2023)

Ogundipe, S. (2017) '**INVESTIGATION: Two Years After, Niger Delta States Continue Controversial Spying Programmes**', *Premium Times*, 30 June (accessed 13 January 2023)

Ojo, E. (2013) '**Media Rights Agenda Tasks Nigerians on Internet Surveillance**', *African Examiner*, 24 September (accessed 16 May 2023)

Oloyede, R. (2021) '*Nigeria Country Report*', in T. Roberts (ed.) **Surveillance Law in Africa: A Review of Six Countries**, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.059** (accessed 2 January 2023)

ONSA (n.d.) ***End-User Certificate Portal***, Office of the National Security Adviser (accessed 23 February 2023)

Oolasunkanmi (2021) ***Lagos and the Smart City Project: Toyosi Ogunrinde***, Lagos State Government

Paradigm Initiative (2018) '**Status of Surveillance in Nigeria: Refocusing the Search Beams**', *Policy Brief* 9 (accessed 13 February 2023)

Paradigm Initiative (2017) ***Nigerian Military's Surveillance of Social Media Alarming – Paradigm Initiative***, 28 August (accessed 6 January 2023)

Perham, M. (1962) *Native Administration in Nigeria*, 2nd ed., London: Oxford University Press

PLAC (2004) ***The Complete 2004 Laws of Nigeria***, Abuja: Policy and Legal Advocacy Centre (accessed 13 February 2023)

PR Newswire (2014) ***DERMALOG Wins 50 Million Dollar Contract for Nigerian Bank Project***, 18 February (accessed 10 May 2023)

Premium Times (2022) '**Customs Donates 86 Seized Drones to Nigerian Navy**', 11 October (accessed 16 May 2023)

Premium Times (2018) '**Election Manipulation: Nigeria Investigates Cambridge Analytica**', press release, 1 April (accessed 17 January 2023)

Premium Times (2016) '**Kaduna to Spend N2.55 Billion on Drones, Surveillance Equipment in 2017**', *Premium Times*, 21 October (accessed 6 January 2023)

Privacy International (2021) ***How IMSI Catchers Can Be Used at a Protest***, 5 May (accessed 24 May 2023)

Punch (2021) '**On FG's New Nationwide CCTV Project**', 1 March (accessed 6 January 2023)

Shahbaz, A. and Funk, A. (2019) '**Governments Harness Big Data for Social Media Surveillance**', in *Freedom on the Net 2019: The Crisis of Social Media*, Washington DC: Freedom House (accessed 12 January 2023)

Suberu, R.T. (1996) 'Introduction', in *Ethnic Minority Conflicts and Governance in Nigeria*, Ibadan: IFRA Nigeria

Thales Group (n.d.) ***Nigerian National ID Program: An Ambitious Initiative*** (accessed 13 January 2023)

The Cable (2022) 'Kogi Partners with Chinese Firm on State-Wide Digital Surveillance for Improved Security', 30 November

The Guardian (2016) '**Lagos State Signs Smart City Deal with Dubai**', 21 June (accessed 2 January 2023)

The Nation (2017) '**13,000 More CCTV Cameras for Lagos Roads**', 17 January (accessed 2 January 2023)

Turniansky, A. (2010) ***Verint Introduction***, presentation, Israel HLS Conference 2010 (accessed 2 January 2023)

Uduu, O. (2021) '**Lawful Interception: NASS Approves N7.46bn for DIA to Intercept Voice Calls and Internet Communications of Nigerians**', *Dataphyte*, 15 July (accessed 13 January 2023)

Umar, S. (2020) '**Banditry: Matawalle Signs MoU with Dubai's Company on Surveillance Helicopters**', *Daily Trust*, 13 March (accessed 16 May 2023)