institute of
development
studies

Mapping the supply of surveillance technologies to Africa: case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia

Editor: Tony Roberts

Authors: Tony Roberts, Judy Gitahi, Patrick Allam, Lawrence Oboh, Oyewole Adekunle Oladapo, Gifty Appiah-Adjei, Amira Galal, Jimmy Kainja, Sam Phiri, Kiss Abraham, Sebastian Klovig Skelton and Anand Sheombar

The Institute of Development Studies (IDS) delivers world-class research, learning and teaching that transforms the knowledge, action and leadership needed for more equitable and sustainable development globally.

For more information visit: www.ids.ac.uk

Research Report

Mapping the supply of surveillance technologies to Africa: case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia

Editor: Tony Roberts

First published by the Institute of Development Studies in September 2023

Suggested citation:

Roberts, T. *et al.* (2023) *Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia*, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2023.027**

ISBN: 978-1-80470-122-5
DOI: **10.19088/IDS.2023.027**

A catalogue record for this publication is available from the British Library.

Funding acknowledgements

Research carried out for this report was supported by Civic Futures. Civic Futures is a philanthropic initiative conceptualised and launched by the Funders Initiative for Civil Society (FICS), which acts as its secretariat, and the Fund for Global Human Rights (FGHR), which is a founding member. Through Civic Futures, we listen to and lift the voices of the movements on the frontlines experiencing closing civic space due to security overreach; and we ensure these insights influence the philanthropic community to fund work to push back against security overreach at scale. FICS is hosted at Global Dialogue, a registered charity (1122052) partnering with philanthropy to advance rights, equity and diversity.

Other acknowledgements

The authors would like to gratefully acknowledge reviewer feedback from Admire Mare and Becky Faith as well as expert input from Edin Omanovic and Jane Duncan. Any errors or omissions are the authors' responsibility.

Copy editor: Dee Scholey
Designer: Blossom Carrasco
Proofreader: Catherine Brown

Institute of Development Studies, Library Road, Brighton, BN1 9RE, United Kingdom
+44 (0)1273 606261
ids.ac.uk

IDS is a charitable company limited by guarantee and registered in England
Charity Registration Number 306371
Charitable Company Number 877338

Contents

About the authors

Tony Roberts is a Research Fellow in the Digital and Technology cluster at the Institute of Development Studies, UK.

Judy Gitahi is an independent Kenyan researcher.

Patrick Allam is a Legal Officer at Spaces for Change in Nigeria.

Lawrence Oboh is Program Officer for Civic Space Security at Spaces for Change in Nigeria.

Oyewole Adekunle Oladapo works in the Department of Communication and Language Arts at the University of Ibadan, Nigeria.

Gifty Appiah-Adjei works in the Department of Journalism and Media Studies, School of Communication and Media Studies at the University of Education, Winneba, Ghana.

Amira Galal is a former journalist and independent consultant specialiing in Internet Freedom. She is committed to advocating for global digital rights and fostering a more inclusive online environment for all.

Jimmy Kainja is a Senior Lecturer in the Media and Communication Studies Department, University of Malawi.

Sam Phiri is a member of faculty in the Department of Media and Communication Studies at the University of Zambia.

Kiss Abraham is an activist, researcher, media practitioner, artist and director of NewZambian Innovations.

Sebastian Klovig Skelton is a senior reporter on *Computer Weekly*.

Anand Sheombar is a researcher at HU University of Applied Sciences Utrecht, The Netherlands.

Executive summary

African governments are collectively spending as much as a US$1bn per year on surveillance technologies. There is copious evidence that states in Africa are using surveillance technologies in ways that are unlawful and/or violate the fundamental human rights of citizens.

Nigeria is Africa's largest customer, spending at least US$2.7bn on surveillance technologies in the last decade. The technology has been used to spy on peaceful activists, opposition politicians, and journalists. Nigeria spends hundreds of millions of dollars annually; the total of known contracts 2013–22 exceeded US$2.7bn.

Nigeria, Ghana, and Zambia have each spent over US$350m on 'safe cities' mass surveillance programmes from China. Malawi is alone of the five countries studied in having not implemented the 'safe city' surveillance model.

This is the most comprehensive documentation of suppliers of surveillance technology to Africa. The five country reports represent the most complete record to date of which companies from which countries are supplying which surveillance technologies to the governments.

Surveillance technologies are supplied by companies predominantly from the USA, China, Europe, and Israel. This commercial trade facilitates the violation of citizens' rights to privacy and anonymity, and freedom of expression and association. Supplier companies regularly claim that they only supply governments, or that any illegal surveillance constitutes a breach of their terms of service. European companies are supposed to conduct human rights assessments prior to supply. However, none of these voluntary self-policing measures have prevented the rapid expansion of surveillance that violates fundamental human rights.

Different countries dominate different surveillance technology market segments. The USA and Europe are losing their historical domination of the market to provide technologies of phone and internet surveillance to Chinese companies Huawei and ZTE. In Africa, China dominates the provision of public space surveillance in the form of 'safe city' street surveillance with facial recognition and car number plate recognition based on artificial intelligence (AI). The USA/UK dominate in the provision of social media surveillance and 'political marketing' consultancy to manipulate voter beliefs and behaviour. Germany, Italy, and Israel are the major exporters of mobile phone hacking malware.[1] Britain exports fake cell towers (IMSI catchers)[2] to spy on mobile calls and messaging. Russia is a minor supplier with negligible influence.

African governments differ in their surveillance profiles. Nigeria permits far more government agencies to conduct surveillance than anywhere else and is a leading customer for the five categories of surveillance technology covered in this report. Ghana appears to have focused on mobile spyware and 'safe city' surveillance. Morocco has been an avid consumer of internet and mobile phone intercept technologies and has the unique distinction of having conducted mobile surveillance of its own king. Zambia's huge investment in a Chinese 'safe city' surveillance system is a massive upgrade of its surveillance capabilities. Malawi's investment in surveillance systems is modest compared to other countries studied.

The human rights toll from the trade in digital surveillance technologies to Africa is high. Overall, the use of these technologies exerts a 'chilling effect' on citizens, stifling debate and democracy. Individuals often suffer long-term physical and psychological harm as a result of being targeted. Each country report provides examples of real-life 'surveillance stories' which illustrate the human cost of the supply of digital surveillance technologies to Africa.

Urgent action is needed to cut off the supply and demand for mass surveillance technologies.

Supply-side action: Abolish surveillance exports

- The suppliers, customers, and users of surveillance technology must be monitored and documented.
- Those supplying surveillance technology to human rights abusers should be sanctioned.
- Any export of surveillance technology should require a government export licence.
- All surveillance technology export licences should require an independent human rights assessment.
- Accountability should be enabled through real-time transparency reporting by the export authority.

[1] Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network, or server; for instance, computer viruses, worms, Trojan horses, ransomware, and spyware. These malicious programs steal, encrypt, and delete sensitive data, alter or hijack core computing functions, and monitor end users' computer activity.

[2] An international mobile subscriber identity catcher (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.

- Staff of companies breaching regulations should be suspended from working anywhere in the sector.

Demand-side action: Defund mass surveillance

- Public awareness should be raised about the constitutional right to privacy of communication.
- Public awareness should be raised about state violation of the rights of law-abiding citizens.
- Greater civil society capacity is needed to influence the reform of surveillance law and practice.
- Campaigns are needed to defund surveillance and redirect resources to education and health.
- Strategic legislation is needed to petition constitutional courts to defend/expand citizen rights.

Table 1.1 A visual summary of surveillance technology acquisitions in each country studied

This table is derived from the more comprehensive country reports included in this publication, which contain sections addressing acquisitions of each category of surveillance technology.

	Zambia	Malawi	Morocco	Ghana	Nigeria
Internet interception	◉	○	⦿	○	◉
Mobile interception	○	◉	⦿	⦿	◉
Social media monitoring	○	○	⦿	○	◉
Safe city/smart city	●	○	⦿	●	●
Biometric ID	◉	⦿	○	○	●

KEY
○ No evidence of surveillance acquisition
⦿ Less than US$10m
◉ Medium, US$10–100m
● Large, over US$100m

Source: Authors' own. See country reports for data sources.

1. Introduction

This report documents which companies, from which countries, are supplying which types of surveillance technology to African governments. We have focused on this subject in the belief that without this missing detail, it is impossible for African citizens to adequately design measures to mitigate and overcome illegal surveillance and violations of human rights.

The report documents the digitalisation and algorithmic automation of state surveillance across Africa. Since the turn of the century, we have witnessed a digitalisation of surveillance that has enabled the algorithmic automation of surveillance at a scale not previously imaginable. Surveillance of citizens was once a labour and time-intensive process. This meant a practical limit to the scope and depth of state surveillance. The digitalisation of telephony has made it possible to automate the search for keywords in communications. For the first time, state surveillance agencies can do two things: (a) conduct mass surveillance of all citizens' communications, and (b) micro-target individuals for in-depth surveillance that draws together in real-time data from mobile calls, short message service (SMS), internet messaging, global positioning system (GPS) location, and financial transactions.

This report was produced by qualitative analysis of open-source data in the public domain. The information presented is drawn from a diverse range of sources, including open government data sets, export licence portals, procurement notices, civil society databases of surveillance contracts, press releases from surveillance companies, academic articles, reports, and media coverage.

The research is organised using a typology of five categories of surveillance technology. We did not set out to detail every technology available, every company, or every supply contract. Instead, we document the main companies and countries selling digital surveillance technologies to African governments. Rather than focus on the technical functionality distinguishing each product offering, we highlight five of the most important types of surveillance technology: internet interception, mobile interception, social media surveillance, 'safe city' technologies for the surveillance of public spaces, and biometric identification technologies.

This report is the third in a series of four publications that evidence expanding digital surveillance in Africa. The first report, produced by the African Digital Rights Network (ADRN), mapped the broader landscape of ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries*** and identified digital surveillance as a key technology being used to close democratic space in Africa (Roberts and Mohamed Ali 2021). The second ADRN report, ***Surveillance Law in Africa: A Review of Six Countries***, analysed the privacy protection in surveillance law across Africa and evidenced widespread state surveillance practices in violation of constitutional guarantees and in excess of lawful interception powers (Roberts *et al.* 2021). This third report maps the supply lines of surveillance technology to Africa. The fourth publication in this series will be a collected edition book that examines additional African countries and conducts a deeper analysis of power interests shaping this pernicious trade.

The remaining sections of this report are set out as follows. In the next section, we provide the background and some key reference documents. We then briefly outline the research methodology before detailing the five categories of technology used to organise the data brought together in the country reports. We then present a two-page summary of each of the longer country reports that follow. In the final section, we make some tentative conclusions and recommendations.

2. Background

Privacy is essential to democracy, commerce, and to private family life. The right to privacy is explicitly recognised in international human rights law, including the Universal Declaration of Human Rights (UN 1948), the International Covenant on Civil and Political Rights (UN 1966), and the Declaration of Principles of Freedom of Expression and Access to Information in Africa (African Commission 2019). Without access to privacy, it can be unsafe to dissent from dominant narratives or protest injustice, impossible to compete commercially, to develop policy alternatives, or relax in one's home.

All unwarranted surveillance is a violation of citizens' constitutional rights. The right to privacy is guaranteed in most African constitutions and in international human rights conventions, and is protected in domestic laws. Privacy is a valuable right in itself, but it is also instrumental in enabling other rights, such as freedom of expression, assembly, and association (Bernal 2016; EFF 2013). Democracy requires that citizens can meet, correspond, and deliberate freely, including about instances in which their opinion differs from that of the current government, president, or other powerholders. Whereas surveillance could be warranted for the sake of national security, this provision is often not well established or enforced in African constitutions.

This report is concerned with state surveillance that is unlawful or which violates protected human rights. State surveillance here refers to any listening, observing, monitoring, or recording by agents of the state of citizens' conversations, correspondence, or communications. Citizens have good reason to value their privacy from unwarranted intrusion in their homes and businesses, in public spaces, and in private communication and correspondence.

Globally, the expansion of surveillance is occurring in the context of declining political freedoms and shrinking civic space. The world has experienced 15 consecutive years of declining political freedoms (Freedom House 2021) and shrinking civic space (CIVICUS 2022). The provision of the technological capacity for mass surveillance and targeted surveillance of government critics can only amplify this democratic backsliding (Waldner and Lust 2018; Duncan 2018; Feldstein 2019; Amnesty International 2021). The increasing availability of the technical means to conduct mass surveillance of citizens' mobile and internet communications – alongside the closing of democratic space across the globe – has raised concerns about a descent into what Freedom House (2018) has called 'digital authoritarianism'.

Illegal state surveillance has been extensively documented in the USA, China, and Europe. Three highly publicised episodes brought the illegal use of surveillance technologies to the public consciousness:

1. The Snowden revelations of mass surveillance of internet and mobile communication of citizens in the US and UK (Greenwald 2014).
2. The Cambridge Analytica case exposed how US corporations such as Facebook provide data to (UK) 'political marketing' companies to surveil social media communication globally, to micro-target citizens, and manipulate their beliefs and behaviour (Ekdale and Tully 2019).
3. The Pegasus (Israeli) spyware investigations showed how the mobile phones of tens of thousands of activists, opposition leaders, judges, and journalists were infected with spyware by incumbent governments to repress opposition and retain power (Amnesty International 2021).

Since the Snowden revelations in 2013, there has been a great deal of research about mass surveillance in the global North (Choudry 2019; Ball and Snider 2013; Feldstein 2019).

However, there has been relatively little documentation of the supply lines of surveillance technologies across Africa. Although there has been a great deal of research about digital mass surveillance in the global North, there has not been the same level of research across all African regions. A body of research on surveillance in Africa is emerging (Duncan 2018; Hunter and Mare 2020; Munoriyarwa and Chiumbu 2022). To date, this literature has tended to focus on single technologies, single countries, or on specific regions (Duncan 2022; Munoriyarwa and Mare 2023).

Yet African governments are routinely violating citizens' constitutional right to privacy with mass surveillance. Despite a multilayered articulation of rights at state, continent, and global levels, African governments routinely violate citizens' privacy and they do so with impunity. Digital surveillance is arguably the greatest threat to countries with fragile democracies, constrained civil society, weak legal protections, and existing restrictions on political freedoms and civic space.

The narrow use of surveillance can be compatible with the protection of human rights. As we showed in our previous report (Roberts *et al.* 2021), there are templates of exemplary surveillance law with built-in human rights protections. Civil society must create the political will for such exemplary practice.

Strategic litigation has succeeded in holding governments accountable and improving surveillance law. Our previous report showed, however, that, to date, this has only worked in African countries with relatively strong civil society and relatively independent media and judiciary.

A mapping of the supply lines of these technologies to Africa is essential to ending illegal surveillance. Previous ADRN reports have documented illegal surveillance of citizens, journalists, judges, and opposition politicians in a dozen African countries. Yet, to date, there has never been a detailed mapping of the surveillance supply lines to countries across Africa.

Information about which companies, from which countries, are supplying which surveillance technologies is a precondition to being able to design effective programmes to cut off the supply and demand of rights-violating technologies. Civil society in Africa currently lacks data about which surveillance technologies are being supplied and used in their countries. Without this information, it is impossible to define and design effective programmes of awareness raising, policy development, and strategic legislation to cut off the supply of technologies being used to violate human rights.

This is the first publication to map the supply lines of surveillance technologies across Africa. The five country reports are the most detailed documentation to date for each country of the supply of surveillance technologies from the USA, Europe, Israel, and China. Although the data is partial and inevitably incomplete due both to the secretive nature of the trade and to our own finite research capacity, it provides a first assessment of the scale of the African market for surveillance technologies upon which other researchers can build and improve.

3. Methodology

This report was produced by a team of 12 researchers in eight countries. Five country reports were produced by eight African researchers, most of whom are citizens of those countries and based in-country. Additionally, two researchers in Europe detailed the supplier companies and countries. Another two researchers worked on this introductory synthesis.

Researchers were selected for their expertise in the focal countries and their prior research in related subjects. Ten African counties were initially selected for possible inclusion to represent Africa's main geographical regions as well as different levels of political freedoms, using CIVICUS and Freedom House indexes.

Table 3.1 Country rankings

Rankings	Political freedoms (Freedom House 2022b)	Civic space (CIVICUS 2022)	Internet freedoms (Freedom House 2022a)	GDP wealth US$bn (World Bank 2021)	Internet access (DataReportal 2022)
Ghana	80	Obstructed	64	78	53%
Malawi	66	Obstructed	57	13	20%
Tunisia	56	Repressed	61	47	67%
Zambia	54	Obstructed	58	22	29%
Côte d'Ivoire	49	Obstructed	n/a	70	36%
Nigeria	43	Repressed	57	440	51%
Morocco	37	Obstructed	51	142	84%
Zimbabwe	28	Repressed	49	28	31%
Ethiopia	21	Repressed	27	111	25%
Egypt	18	Closed	27	404	72%

Note: There are five civic space rankings: open, narrowed, obstructed, repressed, and closed.

Source: Authors' own, created using data from Freedom House (2022a, 2022b), CIVICUS (2022), World Bank (2021), DataReportal (2022).

The supply-side countries were selected based on research from our two previous studies as the countries that appeared to be supplying the most surveillance technologies to African governments. Our aim was to map the supply lines of the international trade in surveillance technologies to help inform future action to cut off the supply and demand for digital technologies used to violate human rights.

The study was carried out by a team of researchers between September 2022 and March 2023. Nine of the 12 researchers were African scholars, eight of whom are based in the countries that they are writing about. Due to security concerns, this phase of the research was restricted to pulling together the diversity of data already in the public domain from databases, export licences, procurement records, academic articles, and media reports.

We are indebted to Dr Admire Mare and Dr Becky Faith who kindly reviewed the study prior to publication.

Ethics: Researching state surveillance raises several ethical dilemmas and requires risk management. For this report, we initially intended to map the supply of surveillance technologies to ten African countries. However, risk management protocols reduced this to six countries. We originally imagined conducting primary research but, again due to risk management protocols, we took the decision to limit this phase of research to desk-based research that only involved collating and analysing data from disparate open-source information that was in the public domain. Despite restricting researchers to secondary analysis of data already in the public domain, the research was not risk-free. In many countries, a researcher who is a citizen of that country and living in that country cannot safely publish information about state surveillance in their own name. To do so is to risk a visit from state security personnel, perhaps a period of detention, and possibly worse. State security agents can claim, whether they believe it to be true or not, that your research amounts to espionage – obtaining secret information and sharing it with foreign governments. Often the objective of arresting researchers and journalists is to create a 'chilling effect' (to encourage journalists to self-censor) rather than because of any genuine threat to national security. In this project, as we worked through our ethics review process and developed our project risk management protocol, planned research in Egypt, Tunisia, Ethiopia, and Zimbabwe was set aside due to risk assessments. One other researcher was forced to withdraw for health reasons. This left us with five Africa country reports.

4. Categories

Our research objective was to identify which companies, from which countries, are providing which digital surveillance technologies to African governments. There are perhaps hundreds of different kinds of digital surveillance technology in known use, and with innovations constantly surfacing it would be impractical to maintain a complete inventory. This research did not set out to provide an exhaustive list of them; nor did we set out to provide technical explanations of their distinctive functionalities. For our purposes, creating a typology of the main categories of surveillance technologies being used by states was the most useful way of organising the data for the reader. Based on analysis from our two previous studies, five categories of surveillance technology were of evident importance. We validated these categories before we began the research with two global experts on surveillance technology, and then again empirically as we collated data on the surveillance technologies in the countries studied.

We focused our research on these five recognisable categories of digital surveillance technology foregrounded by our previous studies and review of the literature. They are: (i) internet interception technologies, (ii) mobile phone interception technologies, (iii) social media surveillance technologies, (iv) safe city technologies for surveillance of public space, and (v) biometric ID surveillance technologies. Each category of technology is briefly explained in the sections that follow.

Internet interception

Internet interception technologies enable covert spying on citizens' emails, instant messaging, browsing and search histories, etc. Because digital information is transmitted across the internet in 'packets' of data, internet intercept technology is often referred to as 'deep packet inspection' or 'packet sniffing' technology.[3] This is a form of signals intelligence (SIGINT) and may be carried out by government agencies, corporations, or individual hackers. The Snowden revelations brought to public attention the fact that the US and UK states were conducting mass surveillance of all citizens' internet communications using this technology. 'Lawful interception' usually

[3] Deep Packet Inspection (DPI) is a type of network packet filtering where network packets are evaluated as they pass a given checkpoint. A real-time decision is then made, depending on what a packet contains and based on rules assigned by an enterprise, an internet service provider, or a network manager. DPI could be used to remove spam, viruses, intrusions, and any other defined criteria to block the packet from passing through the inspection point. DPI could also be used to decide if a particular packet is redirected to another destination.

requires a warrant to be provided by a judge who must first check to establish that the interception is 'lawful, necessary and proportionate' to protect citizens' rights to privacy (Roberts *et al.* 2021). Many governments require internet service providers to save all citizens' internet communications and metadata so that government agents can access it upon production of a judicial warrant. Any surveillance that is conducted outside of this legal framework is unlawful surveillance.

Mobile interception

Mobile phone interception technologies enable covert spying on citizens' phone calls, text messages, instant messaging, or internet communications using a mobile phone. In most African countries, more than 90 per cent of all internet access is mobile internet access. Mobile interception surveillance can be via court warrant from telecommunications corporations in the same way as via an internet company above. However, illegal surveillance is often effected using mobile malware or IMSI catchers. The Pegasus spyware scandal was a global news story about how an Israeli company provided mobile malware to governments who used it to hack the cellphones of at least 50,000 citizens and to spy on activists, journalists, judges, and opposition politicians including heads of state. IMSI catchers are technology that pretends to be a cellphone tower to enable interception spying on private calls.

Social media monitoring

Cambridge Analytica's interference in the Brexit referendum and Trump 2016 election brought to global attention the fact that Facebook data was being used to surveil social media users so that they could be micro-targeted with political messages from powerful actors designed to manipulate citizens' beliefs and behaviour. As Shoshana Zuboff (2019) and others have demonstrated, 'surveillance advertising' is the business model of Facebook, Google, and other Silicon Valley corporations. UK and US 'political marketing' companies provide social media surveillance and election consultancy to many African governments. Cambridge Analytica worked in Nigeria and Kenya, while another UK company, Bell Pottinger, operated in South Africa.

Safe city/smart city

China offers huge loans to governments to buy packages of surveillance technologies from Chinese companies including Huawei and ZTE. Packages often include the installation of thousands of closed-circuit (CCTV) cameras that have facial recognition and car licence plate recognition capabilities.[4] The Chinese package often includes a command and control room in a 'data centre' from which police and security forces can surveil citizens moving around public space in real time. The US company Honeywell offers its own 'safe city' package which has been adopted in Egypt.

Biometric ID

Biometrics are the recognition of human features such as fingerprints, retina, or facial features as a form of identification. Many African governments are implementing compulsory digital ID systems using biometric fingerprints, iris scans, or facial recognition technologies. These digital ID systems are often linked to citizens' mobile phones and to their banking or mobile money accounts. In some countries, the presentation of a biometric ID is becoming a requirement to obtain a passport, driving licence, health care services, social protection payments, and other government services or entitlements. As most people in Africa use their mobile phone for email, text, voice calls, and social media, and leave their GPS switched on, this provides the potential for governments or corporations to conduct panoptic real-time surveillance of a citizen's geolocation, communications, financial transactions, browsing, posts, and 'likes', and makes available their entire network of contacts and historical digital traces.

It is not possible to sustain a claim that this level of surveillance is compatible with human rights as it clearly extends beyond anything that a court could reasonably consider to be 'lawful, necessary and proportionate' (EFF 2014).

The following section presents two-page summaries of the full-length country reports. It is followed by a section on our main findings and conclusions. The longer, more detailed country reports are found after the conclusion of this introductory synthesis report.

[4] CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. This involves placing cameras in strategic places and transmitting signals to a limited number of monitors and video recorders.

5. Country report summaries

This section contains brief summaries of the five country reports and one supply-side report.

Nigeria summary

Nigeria is Africa's largest user of surveillance technologies on its citizens. Section 37 of the Nigerian constitution5 guarantees that the government will protect citizens' rights to privacy of communication. However, there is copious evidence that multiple state agencies use a growing range of digital surveillance technologies to spy on citizens, in breach of these constitutional guarantees. According to the evidence available to our researchers, Nigeria has procured more surveillance technologies than any other country on the continent. The government is a customer of nearly every major surveillance technology company that we examined. We were able to find evidence that Nigeria has spent more than US$1bn on surveillance technologies. This is only a fraction of the true total as we were unable to assign a monetary value to many known contracts and other contracts are not public.

Colonial practices of surveillance continued under postcolonial military governments and have been expanded by recent governments using digital technologies. Nigerian citizens must submit to mandatory biometric registration to obtain mobile phone SIM cards, bank accounts, and national ID, providing the state with the potential power to track citizens' location, transactions, and communication in real time. The Lawful Interception of Communications Act (2019)[6] allows multiple state agencies in each of Nigeria's federal states to use surveillance technologies and compels internet service providers and mobile phone companies to facilitate state interception of citizens' communications. Surveillance has been used against political opposition, journalists, and civil society in ways that create a chilling effect on journalists and result in a shrinking of civic space for democratic deliberation and debate. Nigeria's laws bring confusion rather than clarity regarding the narrow circumstance under which surveillance is legitimate and consistent with human rights law. Thus far, civil society has been unable to use the media to sufficiently raise public awareness or use the courts to hold the government accountable.

[5] See **Section 37 of the Constitution of the Federal Republic of Nigeria**.

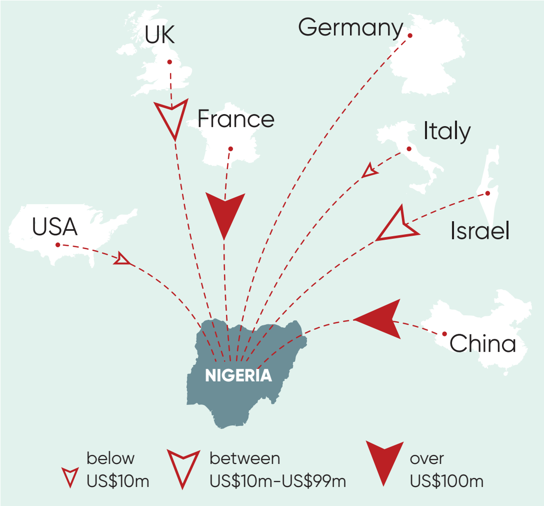
[6] See **Lawful Interception of Communications Regulations, 2019**.

- **Internet interception:** Nigeria sources a wide range of technologies to spy on citizens' internet communications from companies including Elbit (Israel), Romix (Cyprus), Packets Technology (Bulgaria), and Hacking Team (Italy).
- **Mobile interception:** The government has procured mobile phone-spying technologies, including FinFisher (UK/Germany), Mi Marathon (Australia), Cellebrite (Israel), Circles (Bulgaria/Israel), MPD Systems (USA), and Nice Security (UK).
- **Social media monitoring:** UK company Cambridge Analytica breached Facebook policies to use social media data to target voters in 2015. At least two other unnamed companies have provided social media surveillance technologies to the government.
- **Safe city/smart city:** Huge loans from China enabled Huawei and ZTE to provide extensive CCTV camera surveillance with facial and car number plate recognition in Lagos and Abuja. Companies from United Arab Emirates (UAE) and South Korea work with local companies to maintain the systems.
- **Biometric ID:** Biometric finger and facial recognition technologies are provided in huge contracts by defence companies Thales (France/Singapore) and Dermalog Identification (Germany), BIO-key (USA), and Chongqing Huifan (China).

Recommendations

Citizens' constitutional rights would be best served by a single surveillance law that details judicial protections and independent oversight and gives the power to import and use surveillance technologies to a single state agency. Civil society must build awareness and advocate for this. An agency with exclusive oversight over the deployment and acquisition of surveillance technology is necessary to reduce the misuse of surveillance technology in Nigeria.

Figure 5.1 Nigeria's surveillance supply lines



Source: Authors' own. See country reports for data sources.

Nigeria is Africa's largest market for surveillance technologies and lacks effective protections for citizens' constitutional rights to privacy, freedom of speech, and association. Multiple state agencies collectively spend billions of dollars on every kind of surveillance technology from all of the supplier countries. This translates into violations of citizens' constitutional rights and those that use surveillance unlawfully do so with impunity.

1. Internet interception: Nigeria spent US$40m acquiring surveillance tools from Israeli arms company Elbit Systems. US$2m was spent on software to conduct attacks on websites using distributed denial of service (DDoS) and at least one governor bought surveillance services from the Italian company Hacking Team.

2. Mobile interception: Nigerian national and state governments have acquired multiple spyware technologies such as FinFisher (UK/Germany), Circles (Israel), and Fiber Optic Landing Solution to snoop on calls, texts, and phone locations, totalling over US$18m.

3. Social media monitoring: The state has spent at least US$20m on social media surveillance software and services. Budgetary allocations show approvals of US$6.6m in 2018 and US$10m in 2021 to acquire social media mining technologies. UK company Cambridge Analytica was paid US$2.8m in 2015 to use citizens' Facebook data to influence Nigerian elections.

4. Safe city/smart city: Nigeria paid Chinese company ZTE US$470m in 2008 to install CCTV cameras across Lagos and Abuja. US$113m was paid to Chinese company Huawei for an electronic borders project.

5. Biometric ID: US$430m was paid to the Singapore office of French arms company Thales for a biometric national ID system in 2012. Additional biometric scanning technologies were procured from German company Dermalog (US$50m) and US company BIO-key (US$45m).

Ghana summary

The colonial Special Branch function for political surveillance was retained after Ghana's independence and has since been deployed against opposition politicians. Ghana only introduced a security and intelligence agencies act in 1996,[7] prior to which the operations of the intelligence agencies were extra-legal.

Recently, Ghana's democratic profile has been declining as the government increases its possession of surveillance technologies. Ghana has been recognised as one of the continent's most politically open and free countries. Article 18 of Ghana's constitution[8] prohibits state interference with citizens' privacy, family, home, or correspondence, and the government generally respects these prohibitions in practice. However, the recent Pegasus mobile spyware cases have shown that Ghana is not completely free of state surveillance and the recent and rapid expansion of public space surveillance and biometric registration have given cause for concern to civil society organisations.

- **Internet interception:** State security forces have reportedly purchased internet surveillance technology; however, no cases of security forces monitoring private communications have been reported (Freedom House 2022b). The Cybersecurity Act (Republic of Ghana 2020) provided additional powers of surveillance to the government. The law creates a legal obligation for internet service providers to install interception technology and to retain the content of citizens' communications and metadata for several years to facilitate access by state agencies (*ibid.*). The technology required to conduct this surveillance must therefore now be in place in Ghana's internet and mobile companies. There has been a lack of transparency about supplier contracts or regularity of use.
- **Mobile interception:** Ghana has purchased mobile interception technologies from six overseas companies: NSO Group (Israel), Cellebrite (Israel), Quadream (Israel), Decision Group (Taiwan), Tactical Devices (Switzerland), and Intellexa (Greece).
- **Social media monitoring:** Cambridge Analytica (UK) has operated for the government in Ghana, but there is no evidence that it used social media surveillance as it did in Nigeria, the UK, and the USA.
- **Smart city/safe city:** Ghana is implementing a safe city project with a CCTV component powered by Chinese company Huawei's facial recognition AI. Phase I of the project cost US$176m, while Phase II cost

[7] See **Security and Intelligence Agencies Act, 1996 (ACT 526)**.

[8] See **Constitution of the Republic of Ghana 1992**.

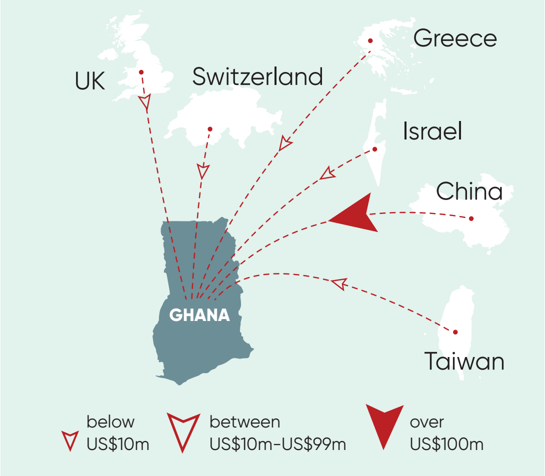
US$235m. Ghana is also implementing a US$300m comprehensive smart city project, via ArisCel (Ghana/China).

- **Biometric ID:** Ghana has multiple biometric identification systems that require citizens to provide facial recognition or fingerprint biometrics. The biometric Ghana Card is being made compulsory and is a pre-requisite for obtaining mobile SIM cards and banking services.

Recommendations

There is a need to increase public awareness of expanding surveillance and the digital rights implications of safe cities and biometric identification. Greater transparency is needed regarding the procurement of surveillance technologies and their use through the publication of annual reports by an independent oversight body. A truly independent judiciary and media are necessary for civil society to be able to hold the government accountable.

Figure 5.2 Ghana's surveillance supply lines



Source: Authors' own. See country reports for data sources.

Ghana's democratic ranking is one of the highest in Africa, however, it has used digital technologies to conduct mass surveillance of citizens. Recent cases of surveillance and arrests of journalists, civil society actors, and protesters coincide with the government's increased possession of surveillance technologies.

1. Internet interception: No evidence was found of contracts to procure internet interception surveillance technologies. However, in Ghana citizens mainly access the internet from mobile phones so mobile internet intercept is relevant here.

2. Mobile interception: Ghana spent more than US$5m in 2016 on Pegasus spyware from Israeli company NSO Group. Ghana has also acquired spyware from Israeli companies Quadream and Mer Group, and telecommunication interception technology from a Swiss company. Security forces have also had access to digital forensics by Cellbrite (Israel), which decrypts encrypted devices.

3. Social media monitoring: Ghana has engaged the services of UK company Cambridge Analytica and politicians have employed the services of other actors to shape opinions on social media.

4. Safe city/smart city: Ghana has spent US$300m on a comprehensive smart city project to provide countrywide WiFi connectivity and US$410m on a safe city project powered by Huawei's facial recognition AI.

5. Biometric ID: Ghana has a national biometric passport system and is currently implementing a biometric identification system (Ghana Card). This will link to SIM cards and become the exclusive means of identification when accessing mobile and banking services.

Morocco summary

Article 24 of the 2011 Moroccan constitution[9] guarantees citizens the right to privacy of communication and freedom of speech. However, Privacy International and Amnesty International have separately documented multiple cases of journalists and activists who have been directly targeted by government surveillance agencies and been subject to unwarranted detention. Journalists and bloggers who are critical of the state are routinely subject to arrest without warrant and to long periods of pre-trial detention. The lack of an independent judiciary removes any realistic possibility of redress or accountability. In recent years, Morocco's human rights record has deteriorated further. The Moroccan state has been investing in digital technologies to increase its surveillance capacity and has awarded itself new surveillance powers. This has led to a chilling effect, causing journalists to self-censor criticism of government policy and practice. The lack of a clear legal framework to protect citizens' rights in cases of state surveillance compounds the increasing concern of local civil society organisations.

- **Internet interception:** The Moroccan government has procured Eagle internet interception technology from French company Amesys Bull, which also supplied to Egypt and Libya. The government also secured internet-spying technology from Italian company Hacking Team. It was used against the award-winning citizen media organisation Mamfakinch, eventually causing the organisation to shut down operations.
- **Mobile interception:** The government has expanded its ability to listen in to citizens' mobile calls, texts, and instant messages by procuring mobile interception technologies from EXFO (Canada/Finland), Circles (Israel), and an unnamed Swiss company.
- **Social media monitoring:** No evidence of specific social media surveillance contracts has been identified, but 2022 saw a marked rise in the number of activists and influencers sentenced for comments they made on social media. Activists and journalists often fear being subjected to surveillance, and multiple activists and influencers have been charged and sentenced for their social media content.
- **Safe city/smart city:** There are no known acquisitions of smart city surveillance technologies, but the interior ministry has made a US$94m tender to equip drones and CCTV cameras to enforce Covid-19 distancing in Casablanca. In 2022, Morocco also began tendering for facial recognition systems in Rabat's Salé Airport.

[9] See **Morocco's Constitution of 2011**.

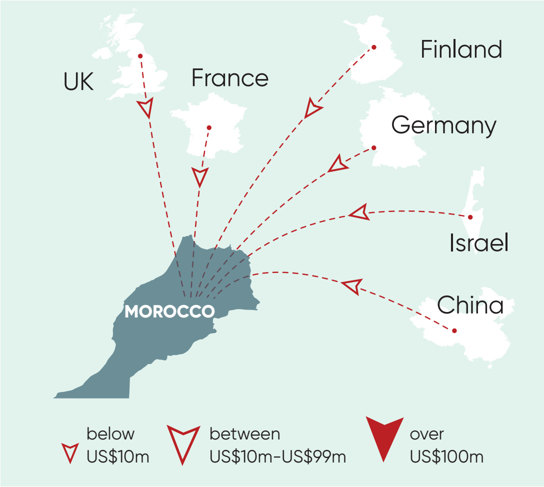
- **Biometric ID:** Biometric identification technologies in Morocco are supplied by French company IDEMIA. Biometric scanners are used to verify the identity of passengers entering and leaving Morocco. In 2022, Morocco also launched the first digital ID system which Moroccans will use as proof of citizenship.

Recommendations

As with other countries in the study, Morocco cites 'national security' as the reason that it awards itself new surveillance powers and invests in digital surveillance technologies. However, what counts as national security is not defined in law, and surveillance powers secured to narrowly target terrorists are in practice used against peaceful critics and journalists.

To secure public support for government surveillance it would be advantageous to make the process transparent and subject to independent oversight. Clear regulations and guidance for government officers to follow would be beneficial, as would clear mechanisms for remedy and redress when mistakes are made. The government should engage in an open dialogue with citizens to build trust and confidence in the use of digital surveillance for the common good. The right to anonymity and access to encryption and other anonymity-preserving software are essential to human rights defenders and journalists in any country. Companies should be prosecuted if they supply surveillance technology to countries that abuse human rights.

Figure 5.3 Morocco's surveillance supply lines



Source: Authors' own. See country reports for data sources.

Morocco has a history of citizen surveillance and has used Pegasus surveillance technology to monitor its own head of state. Whereas the kingdom has data protection laws to protect freedom of expression and the right to privacy, the laws are vague and permit surveillance with judicial approval.

1. Internet interception: US$2m was spent on the Eagle internet-spying technology from French company Amesys Bull.

2. Mobile interception: Moroccan intelligence agencies have acquired a range of mobile interception technologies likely to have cost more than US$10m, including FinFisher malware (UK/Germany) and a contract for Pegasus spyware (Israel) and Nokia (Finland).

3. Social media monitoring: There are no known contracts on Morocco's acquisition of social media monitoring technology. However, the government has had crackdowns on social media users, with many activists and influencers being charged and sentenced for social media content.

4. Safe city/smart city: The interior ministry has reportedly distributed a non-public call for US$94m to equip drones and CCTV surveillance cameras in Casablanca. However, there is no evidence of contracts to procure technology.

5. Biometric ID: Biometric identification technologies in Morocco are supplied by French company IDEMIA.

Malawi summary

According to data available to our researchers, Malawi has invested the least of our five countries in surveillance technologies and has the least well-developed legislative framework for data protection and privacy rights protection from unwarranted surveillance. Until relatively recently, civil society had not been that digitally active and there is relatively little information in the public domain about government surveillance technology contracts. The formation of a new digital rights network provides an opportunity to put human rights-sensitive legislation in place before surveillance creep begins.

Section 21 of Malawi's constitution[10] guarantees citizens' right to privacy of communication. However, mobile phone registration is compulsory and the 2010 National Registration Act[11] requires citizens to provide fingerprint and facial recognition biometrics. This biometric ID is linked to people's mobile phones. Most Malawians access social media via their phones and have mobile money accounts and electronic banking services on their phones. Most mobile phone users have GPS-enabled phones allowing real-time geolocation. This provides the government with a potentially pervasive means to monitor citizens' location, transactions, calls, text messages, social media, and personal contact networks. In the hands of bad actors, and in the absence of appropriate legal protections and oversight, this could lead to wholesale violation of fundamental human rights.

Although the government justified mandatory registration saying that it would reduce phone crime, the country's telecommunication regulator has since confirmed that mobile money fraud has actually increased since implementing SIM card registration.

- **Internet interception:** There is no available evidence of contracts to supply internet interception technology to the Government of Malawi. However, government surveillance is strongly suspected in light of the regulatory authority's January 2018 implementation of the Consolidated ICT Regulatory Management System (CIRMS), which is known locally as the 'spy machine' (Freedom House 2022b). The CIRMS system has the capability to intercept mobile internet which is how more than 90 per cent of Malawians access the internet.
- **Mobile interception:** The CIRMS system can intercept mobile and mobile internet communications and was bought from Agilis (USA) for a total of US$26m. The use of the CIRMS system was later halted by court order. Malawi has also had mandatory SIM card registration since 2018

[10] See **Malawi's Constitution of 1994**.

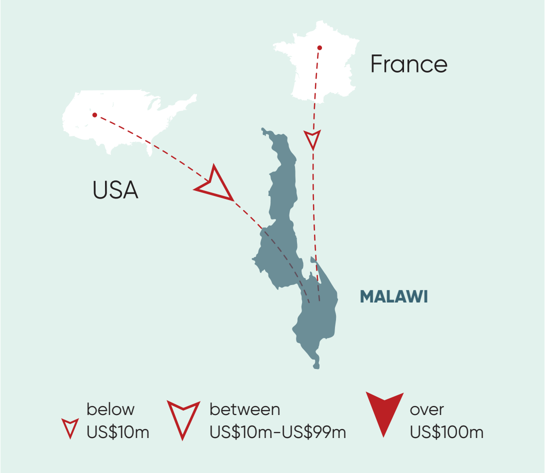
[11] See **National Registration Act**.

- **Social media monitoring:** No evidence of social media surveillance contracts has been identified, but several citizens have been arrested for their online content. In 2022, the prominent investigative journalist Gregory Gondwe was interrogated by police after publishing a story exposing corruption within the government (*ibid.*). Several people have also been arrested for allegedly insulting the state president on WhatsApp conversations, despite WhatsApp having end-to-end encryption..
- **Safe city/smart city:** There are no safe city projects in Malawi. Chinese company Huawei has established a national data centre in the country, but few details are available about its costs or function. The government has also identified a smart city location in Dowa, 50km from Lilongwe, the capital, but no details exist of its establishment.
- **Biometric ID:** Biometric fingerprint and facial recognition technology was provided by SELP Group (France) for US$1.27m with an unspecified amount of funding coming from the former UK Department for International Development (DFID), the European Union (EU), Irish Aid, and USAID.

Recommendations

An opportunity exists in this early stage to put into place data protection and legal intercept legislation that protects digital rights to ensure that all surveillance is legal, necessary, and proportionate (Roberts *et al.* 2021).

Figure 5.4 Malawi's surveillance supply lines



Source: Authors' own. See country reports for data sources.

Malawi has the least developed state surveillance system of the five countries studied. There is very little public information about the few contracts that do exist. In collaboration with Huawei, Malawi commissioned a data centre in Blantyre in 2022. Malawi lacks data protection laws and has previously overlooked safeguards to protect citizens' rights in the national ID and SIM card registration processes.

1. Internet interception: No confirmed contracts; however, the CIRMS system has the capability to intercept mobile internet which is how more than 90 per cent of Malawians access the internet.

2. Mobile interception: In 2010, the Malawi government bought a CIRMS from US firm Agilis and has now spent US$26m in contracts for the system which some now wish to upgrade.

3. Social media monitoring: There are no known acquisitions of social media monitoring technology in Malawi.

4. Safe city/smart city: Malawi does not have a smart city, facial recognition, or CCTV for surveillance, but a smart city location has been identified in Dowa, 50km from Lilongwe, the capital.

5. Biometric ID: In 2017, Malawi began a digital ID programme in collaboration with French company SELP for US$1.27m.

Zambia summary

Privacy of citizens' communications are expressly guaranteed in Zambia's 2019 Bill of Rights (Section 32e).[12] However, the government has made the registration of mobile SIM cards compulsory and introduced a mandatory digital ID card requiring fingerprint and facial biometrics. Little is known about the procurement and use of surveillance technologies in Zambia due to the secrecy practised by the previous administration. The state has invested hundreds of millions of dollars on safe-city public space surveillance, automated car licence plate recognition, and a centralised command and control centre to monitor surveillance data. This has raised concerns on the part of civil society about what the surveillance data will be used for, especially in a country where the detention of journalists and critics of the government has been commonplace.

The new government says that this expenditure was wasteful given Zambia's economic situation, but since taking power it has given no indication that it will reduce levels of surveillance or shut down the command and control centre. There is an opportunity for civil society to use this critique of surveillance expenditure as a hook to engage the government in scaling back surveillance and making the system transparent and compliant with Zambia's new Bill of Rights.

- **Internet interception:** The government's Financial Intelligence Centre procured internet interception technology from Cyberbit (Israel) in 2017 and has reportedly used it to monitor Skype calls and instant messaging communication.
- **Mobile interception:** The software of surveillance company Circles (Israel) has been detected on mobile phones in Zambia operated by an unknown agency. The company claims it only sells its products to governments.
- **Social media monitoring:** The Zambian government has warned citizens that it has installed equipment that enables it to monitor social media and identify users as part of lawful interception measures. A UK company run by notorious political marketing strategist Lynton Crosby reportedly ran an online political influencing campaign on behalf of foreign mining interests to get the current president elected.
- **Safe city/smart city:** Zambia is implementing a safe city project with Chinese loans and the companies Huawei and ZTE. Huawei has built a national data centre in Lusaka to monitor input from surveillance cameras, including automated car licence plate recognition.

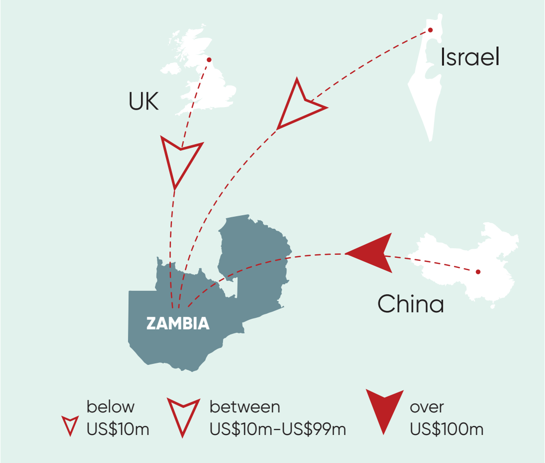
[12] See **Zambia's Bill of Rights**.

- **Biometric ID:** Biometric identification systems are being applied to register citizens' national ID, passports, and voter registration with the UK company Smartmatic.

Recommendations

The change in government provides an opportunity to improve Zambia's human rights profile by clarifying the legal basis for surveillance in Zambia, making the process transparent and improving independent oversight mechanisms. Civil society may wish to discuss with the government making public the full list of surveillance procurement of previous administrations and setting a time frame for the closure of the Chinese surveillance systems.

Figure 5.5 Zambia's surveillance supply sines



Source: Authors' own. See country reports for data sources.

Zambia has paid US$210m to China to construct a national surveillance command and control centre for Lusaka. However, Zambia has no legislative framework to control the use of CCTV despite the introduction of a bill in 2019, raising concerns about the use of digital technologies to surveil public spaces.

1. Internet interception: The Zambian government contracted Israeli company Cyberbit in 2017 for a US$10m cyber-surveillance system. Internet service provider companies are also required to save data for use by police and state intelligence agencies.

2. Mobile interception: Circles and Pegasus, both NSO-affiliated technologies that exploit system weaknesses to snoop on calls, texts and phone locations, have been used in Zambia.

3. Social media monitoring: In 2020, Zambia installed technology that allows the ICT regulator to intercept messages and communication.

4. Safe city/smart city: In 2022, China began the construction of a national surveillance command centre, 36 communication towers across the country, e-government, radio communication, and video surveillance systems at a total cost of US$210 million.

5. Biometric ID: In 2022, Zambia signed a US$54.8 million contract for a system in which all citizens will receive biometric-enabled National Registration Cards, birth and death certificates, passports, and citizenship registrations. The electoral commission has also implemented a US$16m biometric voter registration system supplied by the UK.

Supply-side summary

The supply of surveillance technologies to Africa comes primarily from the US, China, Europe, and Israel. The US and China are the principal suppliers of AI-based internet and mobile interception technologies (Feldstein 2019). China dominates the 'safe city' market of public space surveillance (although the USA supplies Egypt). The EU is the principal funder of border surveillance technology across North and West Africa. Israel is most active in the supply of mobile hacking malware. The UK provides a range of surveillance technologies about which there is little publicly available data.

China: China is eating into the US/European dominance of surveillance technology supply to Africa. China is providing billions of dollars in loans to African governments to buy its 'safe city' package of CCTV cameras with facial recognition and car licence plate recognition. Out of the five countries in this report, four already have Chinese 'safe city' programmes: Nigeria, Ghana, Malawi, and Zambia. Huawei and ZTE are the two Chinese companies delivering surveillance technologies, training, and support.

EU agencies: The European Union funds multibillion dollar border surveillance and biometric identification projects in African countries. This includes projects in Morocco and Ghana. Exports of surveillance technologies from the EU should conduct human rights risk assessments before export but EU agencies themselves have failed to do so on several documented occasions.

USA: The USA is home to 122 surveillance companies and competes with China to dominate the market to supply AI-based internet and mobile phone interception systems, including through Verint Systems. The USA leads in social media surveillance and the tracking of protests through companies such as Dataminr. US company Honeywell provides AI surveillance technology and safe city technology to Egypt. Palantir is active in biometric capture technologies.

Israel: There are many Israeli companies providing mobile hacking software to Africa. The most well known is NSO Group, whose Pegasus and Circles technologies were used in Nigeria, Ghana, Morocco, and Zambia. Briefcam surveillance cameras are used extensively in South Africa. Team Jorge hacked into the phones of opposition politicians in Nigeria's 2015 elections.

France: French companies including Altrnati and Nexa are active in the provision of internet and mobile surveillance technologies, especially in francophone Africa. French defence contractor Thales provides biometric capture technologies in Nigeria.

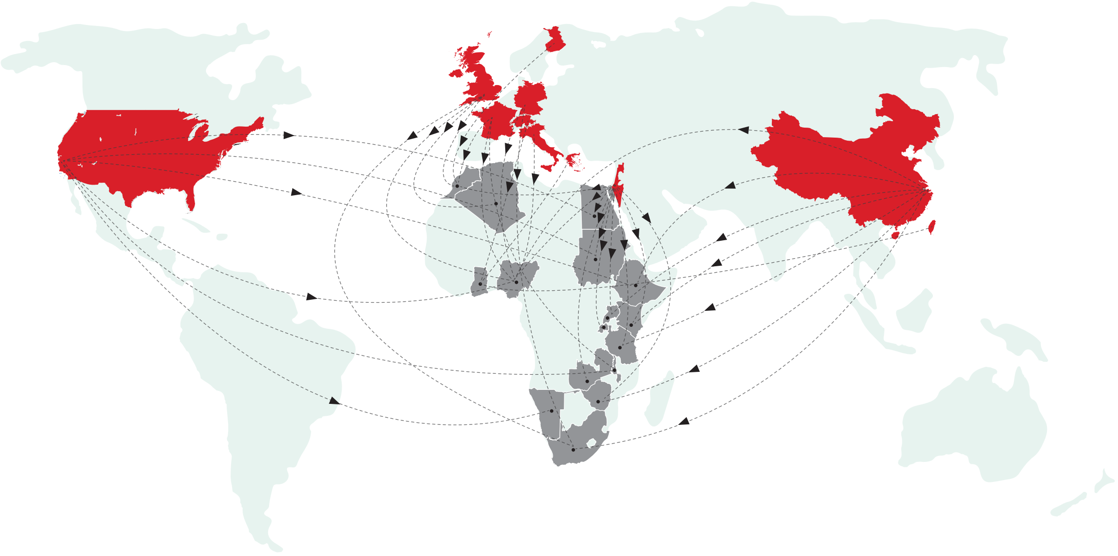
Germany: The UK/German company Gamma supplied its FinFisher mobile phone spyware across Africa including Nigeria and Morocco.

Italy: The best-known Italian surveillance company Hacking Team (now Memento Labs) supplied internet interception technologies to at least five African countries, including Morocco and Nigeria.

UK: The UK exports 'dual-use' internet and mobile interception technologies to all of the African countries in this report. Nigeria is the largest customer, followed by Morocco, Ghana, Zambia, and Malawi.[13] UK defence company BAE Systems provided intercept technologies to Morocco; Airbus' Nigeria and Ghana offices provided border surveillance technologies. The UK has exported IMSI catcher mobile intercept technology to multiple countries with poor human rights records including to Egypt.

Russia: there was no evidence of Russian supply of surveillance technologies to Africa.

Figure 5.6 surveillance supply lines



🟥 SOURCE COUNTRIES ● DESTINATION COUNTRIES

Source: Authors' own.

[13] Dual-use technologies are technologies that have applications in both the commercial and defence sectors.

6. Findings

This section presents what we learn about the supply lines of surveillance technologies to African governments by reading across the country reports and a supply-side study.

Surveillance was introduced by colonisers, retained by liberators, and automated by today's African leaders. The country reports note that European colonial governments introduced state surveillance into Africa. Colonial surveillance institutions and practices were often retained and expanded by post-independence governments. Digitalisation has enabled current leaders to effect a major upgrade in both the scale and scope of state spying, making the mass surveillance of all citizens technically possible for the first time, as well as the extension of surveillance into many new facets of citizens' social, economic, and political lives.

The trade in mass surveillance technologies to governments in Africa is growing. The country reports in this study document growth in contracts for public space surveillance (safe city) and biometric ID systems which cost hundreds of millions of dollars each (see, for example, the country reports from Nigeria, Ghana, and Zambia).

African governments spend as much as a billion dollars a year on digital surveillance technologies. Although definitive figures are impossible in this often-secretive trade, our calculations suggest that Nigeria alone has spent more than US$1bn on surveillance technologies in recent years. We are confident that this figure is a major underestimation for three main reasons: we have only studied a few countries to date, our research budget and time is limited, and many (perhaps most) surveillance technologies are not made public. Despite these considerable limitations, this report provides the first mapping of the supply of digital surveillance technologies to Africa. It provides the most detailed documentation to date of which companies, from which countries, are supplying surveillance technologies to African governments.

African governments are awarding themselves increased surveillance powers and buying ever more powerful technologies. In every country we studied, the state used threats to national security to justify the expansion of its surveillance powers. National security was often a Trojan horse to establish surveillance powers which were then deployed for other purposes. Each of the six country reports begins by reflecting on the reasons given by African governments for awarding themselves new powers of surveillance.

Increased spending on digital surveillance has made panoptic real-time mass surveillance possible. The adoption of the five surveillance technologies in this report together produces the potential for panoptic real-time monitoring of citizens' location, communications, transactions, 'likes', and network of associates. Mandatory mobile phone SIM card registration is increasingly common in African countries, as is the compulsory use of biometric digital ID linked to a citizen's mobile phone and mobile banking or mobile money account.

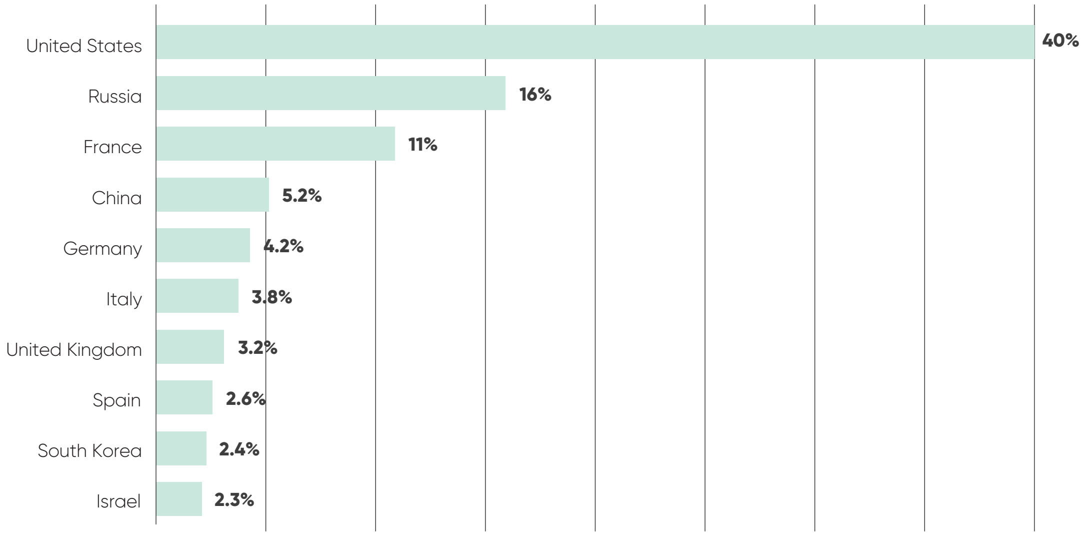
This raises civil society concerns about surveillance creep and a possible descent into digital authoritarianism. Social media monitoring combined with safe city facial recognition of public space introduces the potential (not yet fully operationalised) for state data centres to monitor in real time citizens' location, transactions, calls, 'likes', and political preferences, as well as their social network of friends, followers, and associates. Our reports provide evidence of authoritarian creep; surveillance power justified as necessary for 'national security' to protect citizens against terrorists is already being used to monitor opposition politicians, journalists, judges, peaceful activists, and human rights defenders.

The countries providing the most surveillance technology to Africa are the USA, China, Israel, and Europe. Over recent years, a series of whistle-blower revelations and investigative journalism has detailed a dramatic expansion in mass surveillance using internet interception technologies as well as targeted surveillance of activists using mobile phones.

The companies providing the most surveillance technology to Africa include: Huawei and ZTE from China, BIO-key and Agilis from the USA, Hacking Team from Italy, Thales from France, BAE Systems from the UK, Gamma (FinFisher) from the UK/Germany, Dermalog from Germany, and NSO Group (Pegasus and Circles), Cyberbit, and Elbit from Israel.

Arms-exporting countries are the main surveillance-exporting countries. As the demand for armaments and munitions has dwindled in recent decades, arms-exporting countries such as the USA and China, and arms companies such as BAE Systems (UK), Elbit (Israel), and Thales (France), have pivoted to the supply of surveillance technologies and systems. A multibillion dollar African market for digital surveillance technologies has been built by companies predominantly from the arms-exporting countries of the USA, China, Europe, and Israel. There is a correlation between the world's largest arms exporters as illustrated in Figure 6.1 and the surveillance-exporting countries discussed in this report.

Figure 6.1 Market share of the leading exporters of major weapons between 2018 and 2022, by country



Source: Authors' own. Created using data from Statista (2023).

The digitalisation of surveillance has been accompanied by the privatisation of surveillance. The provision of surveillance technologies and expertise used to be primarily a state-to-state relationship. In the past, African governments accessed surveillance data, surveillance technologies, and surveillance training primarily from the military, police, or secret services of states with whom they had strong 'diplomatic' relations (Rid 2020; Duncan 2018; Ball and Snider 2013). In that era, geopolitics was the main determinant of who got access to the latest surveillance technology. Now, in addition to that traditional source of surveillance technologies, there exists a burgeoning private sector in digital surveillance technologies that is less partisan.

Legacy private arms companies such as BAE Systems and Thale have added the provision of surveillance technologies to their weapons portfolio. But now they must compete with dozens of surveillance start-ups being spun off from the Israeli military and secret services such as NSO Group featured in this report. These Israeli surveillance start-ups exemplify how the digitalisation of surveillance has been accompanied by its partial privatisation, commodification, and marketisation. Fierce competition for market share and profit-seeking behaviour is evidently a key driver in the proliferation of rights-abusing surveillance in Africa.

State surveillance used to take place on government-owned telecommunications but now takes place on private sector platforms. A second sense in which surveillance has been privatised is that internet platforms, mobile phone companies, social media platforms, safe city technologies, and biometric scanners are almost exclusively privately owned. Signals intelligence (SIGINT) used to be carried out by government employees on government-owned monopoly telecommunications companies. Legislation and effective regulation of platforms and algorithms owned by foreign companies is challenging.

Vendors and governments violate citizens' fundamental rights with impunity. Examples of investigative journalism to expose the abuse of digital surveillance technologies by civil society advocacy campaigns have resulted in rights-abusing companies being closed down. This includes Cambridge Analytica, for illegal social media surveillance, and FinFisher, for its internet interception surveillance. However, the people who run the companies are free to begin work the next day in another surveillance technology company. There appears to be impunity on the supply side for companies providing technology to violate citizens' human rights as well as impunity on the demand side for government agencies found to be conducting rights-violating surveillance.

Digital surveillance technologies are used to violate citizens' rights. Unwarranted surveillance unjustly deprives citizens of their constitutional rights and freedoms. It can result in suffering and long-term physical and psychological harm. Each country report in this publication provides examples of real-life 'surveillance stories' which illustrate the human cost of the trade in digital surveillance technologies to Africa.

7. Conclusion

This report makes a valuable contribution to understanding the scope and scale of for-profit surveillance by providing the first mapping of the supply lines of surveillance technologies to African governments from companies in China, the USA, Europe, and Israel. Further research is necessary to understand how this trade operates in francophone and lusophone African countries.

The country reports show how the trade in surveillance technologies reflects postcolonial geopolitical trade ties with the arms-exporting countries of China, USA, Europe, and Israel now developing a multibillion dollar trade in surveillance technologies.

The consequences of surveillance on citizens' rights are the same irrespective of which country the technologies come from. Surveillance technologies are used to violate fundamental human rights – with impunity for the companies supplying the technology as well as the government agencies deploying it despite legal protections.

Governments argue that surveillance is necessary to defend national security interests. However, our country reports make it clear that, in practice, surveillance technologies are used to defend vested power interests, shrinking democratic space for peaceful debate and dissent.

On the supply side, this report shows that each supplier country has its own profile and specialisms that serve different market niches and geographies. On the demand side, this report shows that each African country has a unique surveillance landscape, using different surveillance technologies, having distinct legal frameworks, and with different civil society strength and degrees of media and judiciary independence. These empirical differences show that action to mitigate and overcome abuse must be bespoke in each country.

It is notable that when held accountable, vendor companies claim to be acting within the law, in line with human rights commitments and voluntary codes. This makes it perfectly clear that existing voluntary measures are inadequate. They simply do not work – except to provide cover for impunity. Even when caught in the act and companies are shut down, the perpetrators are free to begin work the next day in another surveillance provider.

Urgent action is needed to cut off both the supply and the demand for mass surveillance technologies. The next phase of our research will include work to define and refine what needs to be done. In supplier countries, 'surveillance watch' movements are needed to monitor export licences, company records, and arms fairs. Legislation is necessary to require human rights assessments prior to licensing, real-time transparency of licence portals, and sanctions for directors and personnel of surveillance companies.

In African countries, there is a need to raise awareness about both privacy rights and surveillance abuses. Research capacity needs to be built in each country to effectively monitor abuse of surveillance powers, its effects on citizens' rights, and viable pathways to overcome injustice. Legal capacity is needed to petition constitutional courts. Policy capacity is needed to draft improved surveillance legislation in line with the UN Draft Legal Instrument on Government-led Surveillance and Privacy (UN 2018).

Abolition of surveillance technologies used to violate human rights should be the ultimate goal. Defunding surveillance would allow billions of dollars of government resources to be redirected to socially useful projects and technologies.

References

African Commission (2019) ***Declaration of Principles of Freedom of Expression and Access to Information in Africa***, Banjul: African Commission on Human and Peoples' Rights (accessed 17 June 2023)

Amnesty International (2021) ***Forensic Methodology Report: How to Catch NSO Group's Pegasus***, London: Amnesty International (accessed 31 May 2023)

Ball, K. and Snider, L. (eds) (2013) *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, London: Routledge

Bernal, P. (2016) '**Data Gathering, Surveillance and Human Rights: Recasting the Debate**', *Journal of Cyber Policy* 1.2: 243–64 (accessed 31 May 2023)

Choudry, A. (2019) *Activists and the Surveillance State: Learning From Repression*, London: Pluto Press

CIVICUS (2022) ***CIVICUS Monitor: Tracking Civic Space*** (accessed 15 June 2023)

DataReportal (2022) ***Digital 2022: Global Overview Report*** (accessed 15 June 2023)

Duncan, J. (2022) *National Security Surveillance in Southern Africa*, London: Zed Books

Duncan, J. (2018) *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*, Johannesburg: Wits University Press

EFF (2014) ***Necessary and Proportionate: On the Application of Human Rights Law to Communications Surveillance***, Electronic Frontier Foundation (accessed 16 June 2023)

EFF (2013) ***International Principles on the Application of Human Rights to Communications Surveillance***, Electronic Frontier Foundation (accessed 31 May 2023)

Ekdale, B. and Tully, M. (2019) '**African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers**', *African Journalism Studies* 40.4: 27–43 (accessed 15 June 2023)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Washington DC: Carnegie Endowment for International Peace (accessed 26 June 2023)

Freedom House (2022a) ***Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet***, Washington DC: Freedom House (accessed 15 June 2023)

Freedom House (2022b) ***Freedom in the World 2022: The Global Expansion of Authoritarian Rule***, Washington DC: Freedom House (accessed 16 June 2023)

Freedom House (2021) ***Freedom in the World 2021: Democracy Under Siege***, Washington DC: Freedom House (accessed 15 June 2023)

Freedom House (2018) ***Freedom on the Net 2018: The Rise of Digital Authoritarianism***, Washington DC: Freedom House (accessed 15 June 2023)

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*, London: Hamish Hamilton

Hunter, M. and Mare, A. (2020) ***A Patchwork for Privacy: Mapping Communications Surveillance Laws in Southern Africa***, Johannesburg: Media Policy and Democracy Project (accessed 31 May 2023)

Munoriyarwa, A. and Chiumbu, S.H. (2022) 'Powers, Interests and Actors: The Influence of China in Africa's Digital Surveillance Practices', in F.A. Kperogi (ed.), *Digital Dissidence and Social Media Censorship in Africa*, London: Routledge

Munoriyarwa, A. and Mare, A. (2023) *Digital Surveillance in Southern Africa: Policies, Politics and Practices*, Cham: Springer International Publishing AG

Republic of Ghana (2020) ***Cybersecurity Act 2020***, Accra: Government of Ghana (accessed 17 June 2023)

Rid, T. (2020) *Active Measures: The Secret History of Disinformation and Political Warfare*, London: Profile Books

Roberts, T. and Mohamed Ali, A. (2021) '**Opening and Closing Online Civic Space in Africa: An Introduction to the Ten Digital Rights Landscape Reports**', in T. Roberts (ed.), *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.005** (accessed 31 May 2023)

Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) ***Surveillance Law in Africa: A Review of Six Countries***, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.059** (accessed 31 May 2023)

Statista (2023) ***Market Share of the Leading Exporters of Major Weapons Between 2018 and 2022, by Country*** (accessed 15 August 2023)

UN (2018) ***Draft Legal Instrument on Government-led Surveillance and Privacy***, Geneva: United Nations Office of the High Commissioner on Human Rights (accessed 31 May 2023)

UN (1966) ***International Covenant on Civil and Political Rights***, New York NY: United Nations (accessed 31 May 2023)

UN (1948) ***Universal Declaration of Human Rights***, New York NY: United Nations (accessed 17 June 2023)

Waldner, D. and Lust, E. (2018) '**Unwelcome Change: Coming to Terms with Democratic Backsliding**', *Annual Review of Political Science* 21.1: 93–113 (accessed 31 May 2023)

World Bank (2021) ***Gross Domestic Product 2021***, World Development Indicators database (accessed 15 June 2023)

Zuboff, S. (2019) *Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Profile Books

Mapping the supply of surveillance technologies to Africa

Nigeria country report

Patrick Allam and Lawrence Oboh
Spaces for Change

SPACES FOR CHANGE I 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).

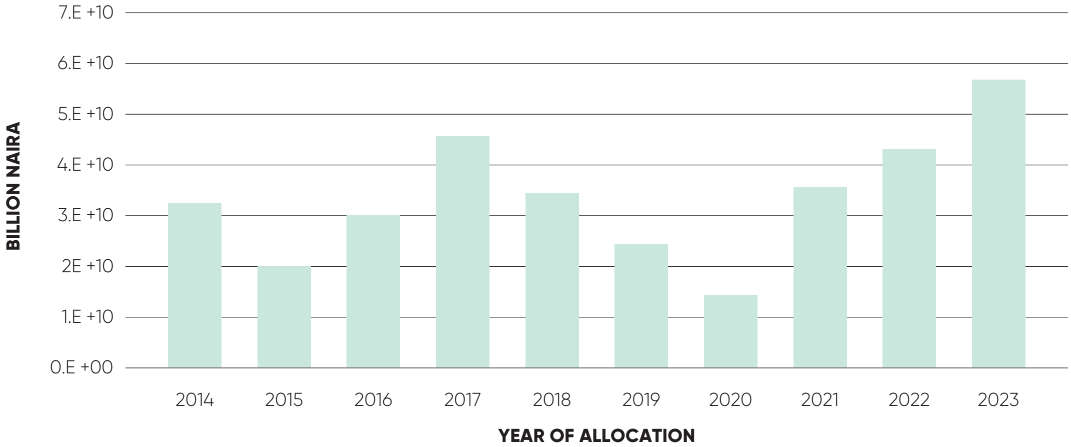
Surveillance under military rule

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)

Mapping the supply of surveillance technologies to Africa

Ghana country report

Oyewole Adekunle Oladapo and Gifty Appiah-Adjei

1. Introduction

This report focuses on Ghana and addresses the types of surveillance technologies Ghana has acquired, the suppliers of those technologies, and their impacts on society. Ghana is central to the discourse on freedom in Africa. In 1957, it became the first British West African colony to attain political independence and, although the democratic governance instituted then was short-lived due to military interventions, Ghana's sustained peaceful transition of power since the restoration of democracy in 1993 has been a key democratic advancement on the continent. However, given Ghana's fast-changing intelligence-gathering technological capability, it is imperative to map Ghana's surveillance technologies to have a view of what the future of human rights in the country holds.

The report is structured in six sections: this introduction provides a general justification for the report; section 2 presents the background, which situates surveillance practices in Ghana in a historical and political context; section 3 documents Ghana's technological policies and practices which create a favourable atmosphere for surveillance; section 4 presents existing evidence on the impact of illegal surveillance in Ghana; section 5 recommends measures to make surveillance compatible with human rights; and section 6 presents cases of individuals whose life stories illustrate the dangers of rights-violating surveillance.

2. Background

Independent Ghana inherited the baggage of a colonial intelligence system. Codenamed Special Branch, and started in 1948 by the British colonial government, it was said to have masterminded the coup that truncated Ghana's nascent democracy in 1966 (Africa 2009; Arnold 2020). The Ghana Police Special Branch was saddled with the responsibility of collecting security-relevant information and disseminating it to a select few members of the government (Arnold 2020). Arnold noted that before the independence of Ghana, the colonial government either destroyed or relocated to the UK all records relating to the country's security and intelligence matters. However, the attempt at completely erasing any memory of colonial intelligence was unsuccessful and Special Branch's structure persisted in independent Ghana. It was noted that from the 1966 coup to the late 1980s there was a sustained decrease in the staff strength of Ghana's intelligence agencies (Africa 2009). However, nothing suggests that this resulted in a weakened state capacity for intelligence-gathering. Rather, it has been revealed that none of Ghana's intelligence agencies were referred to in the laws of the country until the passage of Act 526 of 1996 (*ibid.*), suggesting that operations of the intelligence agencies in Ghana from independence to 1996 were in fact extra-legal (*ibid.*). In such an environment, where no explicit laws guided the operation of intelligence-gathering agencies, abuse could hardly be ruled out.

These historical trajectories point to the likelihood of independent Ghana using its intelligence-gathering agencies for citizen surveillance. Yet Ghana's democratic profile has remained stellar compared to most African democracies. For example, Freedom House has consistently ranked Ghana free (Freedom House 2022) and only Mauritius ranked ahead of Ghana in the Economist Intelligence Unit's (EIU) typology of African democracies. Although Ghana and five other African countries were considered 'flawed democracies' in an EIU ranking, they performed better than the scores of other African countries ranked as either 'hybrid' or 'authoritarian regimes' (Economist Intelligence 2021). In addition, with a score of 43 out of 100 and a rank of 73 out of 180 countries in 2021, Ghana's corruption perception index is low compared to most African countries (Transparency International 2022). Regarding adherence to the principles of the rule of law, the World Justice Project ranked Ghana 58 out of 139 countries globally, and seven out of 33 countries regionally, in its Rule of Law Index 2021.

Despite the relatively positive outlook, Ghana has recently witnessed a slight regression in its rankings. Its Rule of Law Index decreased by 2.2 per cent in 2021 and its Freedom House Ranking dropped by two points in 2022. Its Internet Freedom Ranking has been consistently ranked ‘partly free’ for the past five years (Freedom House 2022). On a closer look, it can be seen that what is going wrong with rights and freedom in Ghana did not start in just those five years. Freedom of expression and the right to privacy have been compromised for some time. Odartey-Wellington (2014) chronicled eight cases of leaked tapes of personal, confidential conversations involving highly placed politicians of ruling and opposition parties, all the leaks taking place between 1999 and 2013 in a democratic Ghana. Although the means through which the tapes were recorded remains largely unknown, and interested parties to the leaked conversations questioned their authenticity in some cases, illegal surveillance cannot be ruled out.

As its positive democratic ratings are decreasing, so Ghana’s cases of human rights abuse are increasing. There are documented cases of arbitrary arrests and excessive use of unnecessary force against journalists, civil society actors, and protesters (Freedom House 2022). In February 2021, Ibrahim Mohammed, an activist in the Ashanti Region, was attacked by assailants and died two days later (*ibid*.). In February 2022, Oliver Barker-Vormawor, founder of the #FixTheCountry protest movement, was arrested, imprisoned for two months, and had his passport confiscated (Akinwotu 2022). In June 2022, 29 Arise Ghana protesters were arrested by the police, while a combined force of the police and the military shot dead two protesters and wounded four others at Ejura Sekyedumase in the Ashanti Region (Freedom House 2022).

These growing cases of intolerance for dissent coincide with the government’s increased possession of surveillance technologies and citizens’ private data. Amidst growing concern about human rights violations, Ghanaian and foreign media houses have published stories alleging that Ghana has taken possession of and used surveillance technologies to spy on its citizens in recent years (Dogbevi 2022). Ghana is among countries implementing the safe city project powered by Chinese Huawei artificial intelligence (AI), and Ghana’s Cybersecurity Act, passed in 2020, makes it legal for the government to conduct surveillance on citizens and retrieve data from the country’s mobile network service providers in the interest of national security.

Reactions to the news of Ghana’s purchase of NSO Group’s Pegasus spyware reinforced this need, generating as it did considerable concern about citizens’ rights to privacy and general human rights in Ghana (Dadoo 2022a). While Ghanaian activists and civil society organisation actors believed they were targets of illegal surveillance (*ibid*.), Pegasus software was found to have been used to target journalists and opposition politicians in other countries that purchased it, confirming their fears (Dogbevi 2022). Although key actors in the spyware purchase and use were tried, only former government officials involved were jailed while NSO's local representative in Ghana was discharged and acquitted (*ibid*.). The situation became even more worrisome when a Ghanaian high court found the Government of Ghana guilty of breaching the country's Data Protection Act by collecting mobile phone subscribers' personal information (Dadoo 2022a).

With this record of violation of the country's privacy law to access citizens' sensitive data, and its confirmed digital technological capability for surveillance, it is incontrovertible that there is a need for a strong system of oversight from different sections of society. This is to keep the Ghanaian state's use of surveillance technologies both legal and sensitive to human rights and freedom.

3. Supply of surveillance technology

Having established that the Ghanaian state possesses the digital technological capability for surveillance and has a record of illegal access to citizens' personal information, it is important to know the sources and types of surveillance technologies Ghana has acquired. This is necessary as suppliers of surveillance technologies vary in their compliance with good international practices. It is also useful to map the type of surveillance technologies as their capabilities vary just as their potential for illegal use.

The documentation will serve two purposes: it will, first, guide local and international efforts to keep the country's use of the technologies under check; second, it will guide efforts to know exactly what signs to look out for to determine if the technologies are being used for illegal surveillance. Of interest are surveillance technologies that can intercept the internet and mobile telecommunication services, monitor social media, record citizens' public lives, and capture citizens' biometric information. These are examined in the next five sections.

Internet interception

Before the Ghanaian general elections of 2016 and 2020, there was widespread fear that the government would shut down the internet. Election-related 'fake news' was becoming a threat to the peaceful conduct of a free and fair election. Just before the 2016 election, the then country's Inspector General of Police, John Kudalor, revealed that the security agency considered shutting down access to social networking sites to curb the spread of disinformation. The development coincided with the launch of the #KeepItOn campaign,[1] with its primary objective of fighting internet shutdowns worldwide. Civil society groups in Ghana and other countries pressured the government to abort the planned shutdown, and a few months before both the 2016 and 2020 elections, the government assured Ghanaians there would be no shutdown, living up to its word (Akwei 2016; Olukotun 2016; Christian 2020; Muya 2021). Ghana thus remains one of the African countries without a history of internet shutdown or denial of access to social media platforms.

[1] Founded in 2016, the **#KeepItOn** coalition comprises over 280 organisations from 105 countries mobilising against internet shutdowns around the world.

Mobile interception

Ghana's Anti-Terrorism Act 2008, Electronic Communications Act 2008, and Cybersecurity Act 2020 provide legal grounds for the interception of mobile communications, and the power of mobile interception may be used in the interest of 'national security'. Worryingly, the term 'national security' is not defined explicitly in law, its interpretation being left open to whatever those authorised to exercise the power consider national security to mean. In the Cybersecurity Act 2020, this power is reserved for top government officials such as the president or security personnel from the rank of Assistant Commissioner of Police and above.

Despite the procedures established by the relevant laws for mobile communication interception, Ghana was found to have acquired Pegasus from NSO Group, an Israeli company, for US$5.5m in 2016 (Dadoo 2022a; Dogbevi 2022). Pegasus is a powerful spyware that can remotely access a mobile phone's contents and location information and use its functions such as the microphone and camera to generate live feeds. An advanced version of the Pegasus spyware can secretly install itself on the target's phone without the target needing to click a link; all that is needed is access to the phone through a vulnerable application (Gurijala 2021).

Although NSO Group claimed that Pegasus was never operational in Ghana, evidence points to the contrary as some of its employees confessed to having trained Ghanaian officials on how to use the spyware (Benjakob 2022). Some Ghanaian activists alleged that they, alongside journalists and political opposition, were the targets of the spyware (*ibid.*). To allay public fears, the Government of Ghana tried former government officials for their roles in procuring the spyware and those found guilty were jailed (Dogbevi 2022). Nevertheless, investigators were reported to have hit a brick wall in their attempts to talk to Ghanaian journalists, government officials, and security personnel about the spyware, creating grounds to suspect that it is still in use in the country (Dadoo 2022a, 2022b).

In addition to its array of surveillance technologies, Freedom House (2021) cites a report of the then director of Ghana's Criminal Investigation Department (CID), Maame Yaa Tiwaa Addo-Danquah, confirming that the country's security forces had access to Israeli company Cellebrite's digital forensics, a tool she stated was used for decrypting encrypted devices. The Government of Ghana claimed that the hacking tool was a gift from the US, UK, and Interpol (Rozen 2020).

Ghana acquired spyware technology from two other Israeli companies, Quadream and Mer Group. Ghana also acquired telecommunication interception technology from an unnamed Swiss company. The details of these technologies and their costs are shrouded in secrecy.

Social media monitoring

Social media monitoring is another popular means through which governments illegally access citizens' personal information and Ghana was found to have engaged the services of Cambridge Analytica, a British ('political consulting') company known for the illegitimate use of Facebook data to covertly target voters. Cambridge Analytica rose to infamy with the revelation that it had meddled in the 2016 US presidential election and influenced the UK's Brexit referendum of the same year with information from the Facebook accounts of millions of voters that they had illegally accessed (*Ghana Web* 2020). However, available information shows that the operation of Cambridge Analytica in Ghana was not based on social media data, but on a dataset generated from a 30,000-respondent survey commissioned in 2014 by the country's Ministry of Health for the purpose of health policy planning (*ibid.*). Proof of Cambridge Analytica's hacking of Ghanaians' social media accounts has been hard to find as the company's operation in the country became public.

Nevertheless, the social media space in Ghana is not free from political influence. As Freedom House (2021) reported, Ghanaian politicians employed the services of paid social media commentators to shape opinions on social media platforms. Whether they employed technology to achieve the same goal is not yet public knowledge.

Meanwhile, Reporters Without Borders cited two cases in which journalists were either arrested or imprisoned over their social media posts. Kwabena Bobie Ansah, a presenter at Accra FM, was jailed for falsely alleging in a social media video that Ghanaian President Nana Akufo-Addo's two wives acquired state land through fraudulent means, and Oheneba Boamah Bennie, a journalist and owner of Power FM, was handed a two-week jail term and a fine over a Facebook video alleging that President Nana Akufo-Addo bought over judges to secure victory over his rival in the courts. These cases, both involving the president, offer up an understanding about the Government of Ghana's low tolerance level for social media freedom.

Smart city/safe city projects

Ghana is implementing a comprehensive smart city project that cuts across different aspects of societal life. A memorandum of understanding for a US$300m component of the project, ArisCel, was signed in 2019 by Celltel Networks, Roberta Annan Consulting, and China National Electronics Import & Export Corporation. Celltel secured approval to start implementing the project in December 2021 (Techfocus24 2021). The project seeks to provide countrywide WiFi connectivity and access to digital devices such as mobile phones, tablets, laptops, and smart TV sets – a good initiative considering the number of opportunities that come with it. Nevertheless, such connectivity increases the government's potential to conduct technology-enabled surveillance, even in the remotest locations.

More importantly, Ghana is implementing a safe city project, the Integrated National Security Communications Enhancement Network (ALPHA) project. Of particular interest is its facial recognition CCTV camera component. These CCTV cameras are being installed around Accra, Ghana's capital city, its regional capitals, entry ports, and other state infrastructure, and are powered by Chinese company Huawei's facial recognition AI. The Government of Ghana signed a contract with Beijing Everyway Traffic & Lighting Technology and Huawei Technologies in 2012 for Phase 1 to install 800 CCTV cameras. The contract was worth US$176m. The contract for Phase 2 of the project, to install 8,400 CCTV cameras, was signed in 2018 (*Whatsup News* 2021). Phase 2 was financed with US$200m from the Export-Import Bank of China and US$35.5m from Barclays Bank of Ghana. Other components of the project, detailed in a project agreement document retrieved from the Parliament of Ghana Library, include the installation of 50 automatic number plate recognition (ANPR) devices at checkpoint sites, expansion of an existing data centre and establishment of a backup data centre, a video transmission network, and an intelligent video analysis system.

Although Huawei maintains that its surveillance system is for public safety and improved security, the abuse of the technology in other countries raises concerns. In Uganda, for example, the same Huawei AI-powered facial recognition technology was used to target for arrest hundreds of supporters of opposition politician Bobi Wine (Nkwanyana 2021). Since living under a siege of surveillance technologies leads to datafication of even private aspects of citizens' lives, there is the fear that governments, makers of the technologies, and hackers could use remote access to data for illegal or harmful purposes.

As surveillance technologies fast become a ubiquitous feature of major cities around the world, people are becoming tolerant of surveillance in public places. However, when the same technologies are used to target and access personally identifying information about individuals or groups, such use compromises their right to privacy and violates the legal protection that the constitutions of many countries assure their citizens.

Biometric ID

Ghana has multiple biometric identification systems. In addition to its national passport, which is strictly for citizens, the country is implementing a biometric identification system known as the Ghana Card for all Ghanaians at home and abroad and all legal permanent residents in Ghana. Holders of the card are expected to link it to their SIM cards and proceed to the service centres set up by telecommunications companies to have their biometrics captured.

It is noteworthy that the Ghana Card is the exclusive means of identification that is acceptable for SIM card registration in the country. As of November 2022, about 30 million SIM cards had been partly linked to Ghana Cards while almost 21 million SIM cards had been fully linked, having completed the biometric capturing. In all, the two constituted about 70 per cent of SIM cards operational in Ghana at that time (Macdonald 2022). The Government of Ghana had issued deadline after deadline for the completion of the registration and threatened to disconnect all SIM cards not fully registered (Adu-Gyamfi 2022). The 31 October 2022 final deadline was eventually upheld with data access restriction placed on partly registered SIM cards and 5.7 million unregistered SIM cards – resulting in the disconnection of about a quarter of the subscribers to one mobile company, MTN, alone (Macdonald 2022).

In addition, the Bank of Ghana issued a directive to all banks operating in the country to accept only the Ghana Card for financial transactions from 1 July 2022. The effective date for implementation was later set as 1 January 2023, but with this development, all financial transactions in Ghana became linked to the biometrics of those who initiated them.

When the policies become fully implemented, the Ghana Card will become the exclusive means of identification for accessing both mobile telecommunication and banking services in Ghana.

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Cedis	US$
Internet interception			
Unknown			Unknown
Mobile interception			
NSO Group (Israel)	Pegasus – mobile communication interception (2016)	21.45m	~ 5.5m
Cellebrite (Israel)	Digital forensics for decryption of encrypted devices (unknown)		A gift from the US, UK, and Interpol
Quadream (Israel)	Spyware (unknown)		Unknown
Decision Group (Taiwan)	Network monitoring (2016)		Unknown
Tactical Devices (Switzerland)	Telecommunications interception/jammer (2015)	22,000	~ 5,000
Intellexa, Greece	Unknown		5.66m
Social media monitoring			
Unknown			Unknown
Safe cities			
Phase I: Beijing Everway Traffic and Lighting Technologies (China); Huawei Technologies (China)	800 facial recognition CCTV cameras (2012)	334.4m	176m
Phase II: Chinese companies	8,400 CCTV cameras, 50 automatic number plate recognition devices, data centre, video transmission network, and intelligent video analysis system (2018)	10.81m	2.35m
Biometric ID			
Unknown			Unknown
	Total	366.7	184m

Source: Authors' own. Created using data from Edin Omanovic's Surveillance Technology suppliers' database, and Ghana's Safe City (ALPHA) project contract document retrieved from the Parliament of Ghana Library.

Note:The conversion rate for 2012 from **United States Dollar(USD) To Ghanaian Cedi(GHS) Exchange Rate on 31 Dec 2012 (31/12/2012)**. For all other years, from Statista: **Annual average exchange rate of U.S dollar in Ghanaian cedi (GHS) from 2016 to 2022.**

4. Impacts

The secrecy surrounding the procurement and use of surveillance technologies in Ghana makes it difficult to measure the impact of their use for illegal purposes. Nevertheless, knowledge of the Government of Ghana's surveillance capability has created a sense of siege among activists, journalists, and opposition politicians. This results from living under the gaze of CCTV cameras, with every item of personally identifying information stored up in government and organisational databases.

Fears have been intensified by the illegality involved in the acquisition of the Pegasus spyware and the later reports that it was used in the country, contrary to the government's initial claims. Activists and dissidents believe that the Government of Ghana used the technologies to spy on them (Dadoo 2022a).

Meanwhile, Oliver Barker-Vormawor founded Ghana's #FixTheCountry movement to demand accountability, good governance, and better living conditions for Ghanaians. The activities of the movement brought him into conflict with government and security agencies, and he shared a story of how the phone of a member of the movement he leads became hacked after meeting with National Security officials. It was observed that calls from the phone 'began being diverted to an unknown number' (Dadoo 2022a, 2022b).

Expressing his worries over illegal surveillance in Ghana, Dogbevi, a member of the International Consortium of Investigative Journalists, was quoted as saying: 'If a state agency can decode my system without access to my password, that is scary (Rozen 2020). While worrying that he too might be a target of illegal surveillance, Dogbevi was further quoted: 'Sources send me information, send me documents. I wouldn't want anyone to have access to that' (*ibid.*).

Secrecy in Ghana creates an environment in which illegal surveillance can thrive. Why? The public does not have sufficient information about surveillance technologies and their use. As a result, it is difficult to hold the Government of Ghana to account for them.

5. Solutions

With the Government of Ghana's growing capacity for surveillance and the possibility of the government and its security agencies violating the legal protection that laws of the country give citizens against illegal surveillance, Ghanaians, especially activists, journalists, and protesters, have no choice but to adapt to living and working in a state under surveillance.

First, it requires capacity building for improved data literacy and data security; individuals and groups have to adjust their actions, especially those carried out on digital devices. Investment in sophisticated anti-spyware solutions is also important. When kept up to date, anti-spyware solutions can save individuals and groups from attacks that compromise their privacy.

The laws guiding the procurement of surveillance technologies in Ghana must also be revisited to identify and block those loopholes that enable the government to execute secret procurement. For a full appraisal of Ghana's public surveillance situation to be possible, litigations may be necessary. The government has not shown a willingness to divulge information about its surveillance capacity, so it will take pressure from civil society organisations (CSOs), and the judgement of a court of competent jurisdiction, to compel it to do so. This will require CSOs to engage in coalition building to demand this accountability.

Meanwhile, for the courts to function effectively as a last resort for securing accountability in the use of public surveillance technologies, the independence of the Ghanaian judiciary must be protected and preserved. Relevant laws of Ghana make judicial approval a precondition for accessing citizens' information to ensure that government does not engage in the illegal surveillance of citizens. In cases of the violation of such laws, it takes a truly independent judiciary to convict the government of its illegality.

6. Surveillance stories

Illegal surveillance has devastating effects on people. Whether real or perceived, the threat of surveillance results in people modifying substantial aspects of their lives and work. For journalists, the extent to which they can use confidential sources is limited significantly (Waters 2017). Illegal surveillance costs investigative journalists access to important stories that could not be broken without others agreeing to provide information unobtainable through conventional journalistic approaches.

Further, the challenges are now real, not only for journalists but for everyone who uses digital devices (and the use of these has permeated every aspect of human endeavour). Victims of illegal surveillance tell of how the acts resulted in experiences that left them in excruciating pain, altered significant aspects of their lives, and curtailed their freedom of expression, rights to privacy, and personal liberty.

In the case of Ghana, such stories are hard to find – which is strange given the surveillance capacity of the Government of Ghana and the country's history of an unholy alliance between intelligence agencies and highly placed government officials. Confirmation that the Pegasus spyware was used in the country specifically to target journalists makes the situation disturbing. The absence of stories of people whose lives have been impacted by illegal surveillance does not prove there was no illegal surveillance. It is a pointer to something ominous: an environment that silences victims.

Stories of how Ghanaian security agencies brutalised citizens in recent years confirm the abusive credentials of these agencies. That they were always interested in the contents of their victims' digital devices is a pointer to their hidden surveillance agenda. Nyabor (2021) told how an editor for ModernGhana.com, Emmanuel Ajarfor Abugri, was arrested in July 2019 alongside a reporter, Emmanuel Yeboah Britwum, and tortured by the police:

> *They slapped me and used a taser on both arms… They also made me go 'head down legs up' against a wall. I did this till I could no longer continue then they hit my back and I fell. They commanded me to do some push ups. I got exhausted and couldn't do it anymore. One officer pulled me up by my trousers and another knocked my back with his elbow, and I fell again.*

Another journalist, Caleb Kudah, suffered a similar fate in the hands of Ghanaian security agents. Nyabor (2021) also related Kudah's account of his ordeals:

> *They pushed me in a chair and slapped me from the back… They took me under a mango tree. One officer came and asked me to kneel down. He kicked me in the groin and gave instructions for me to be beaten… The officers remarked that I'm a dead man since they've been instructed to 'deal' with me. I was commanded to do 30 push ups… I was so tired and fell on the ground. They hit me in the back… When they said I needed to write a statement, one officer said he will dictate some things for me to write.*

In the account provided by Nyabor, the officers accessed Kudah's mobile phone and communicated to a colleague of Kudah's who was later arrested for reasons not explained. Recounting his ordeals to *The Guardian*, the #FixTheCountry movement activist Oliver Barker-Vormawor stated that after having been severely tortured, he was blindfolded and taken in a convoy of police and military vehicles to a cell on the outskirts of the city, where he was stripped and forced to give officers access to his phone. Meanwhile, Emmanuel Ajarfor Abugri and his journalist colleague were arrested together and had their phones and laptops confiscated and accessed by police officers. Upon their release from custody, only their phones were returned; the police held on to their laptops (Committee to Protect Journalists 2019). These experiences confirm Ghanaian security agencies' interest in citizens' personal communication, the same interest behind illegal surveillance.

References

Adu-Gyamfi, K. (2022) '**Ghana to Block all Unregistered SIM Cards after October**', *Africanews*, 18 October (accessed 8 January 2023)

Africa, S. (ed.) (2009) ***Changing Intelligence Dynamics in Africa***, African Security Sector Network (ASSN) and Global Facilitation Network for Security Sector Reform (GFN-SSR) (accessed 10 February 2023)

Akinwotu, E. (2022) '**Ghana "Fix the Country" Activist Says He was Assaulted and Illegally Detained**', *The Guardian*, 14 July (accessed 10 February 2023)

Akwei, I. (2016) '**Ghana Stands to Lose if Internet is Shut Down on Election Day**', *Africanews*, 12 June (accessed 10 January 2023)

Arnold, C. (2020) ' "The Cat's Paw of Dictatorship": Police Intelligence and Self-Rule in the Gold Coast, 1948–1952', *The Journal of the Middle East and Africa* 11.2: 161–77

Benjakob, O. (2022) '**NSO Ghana Op Exposed: Never-Before-Seen Pegasus Spyware Footage, Workers' Passports**', *Haaretz*, 20 January (accessed 22 November 2022)

Christian, A. (2020) '**The Ghana Internet Shutdown Conundrum is Disturbingly Entangled in Press Mis-Reportage**', *WT*, 10 February (accessed 10 January 2023)

Committee to Protect Journalists (2019) '**Two Ghanaian Journalists Arrested and Interrogated, One Allegedly Tortured in Custody**', *CPJ*, 9 July (accessed 10 January 2023)

Dadoo, S. (2022a) '**Is Ghana's Government Using Israeli Kit to Spy on Activists and Dissidents?**', *The Africa Report*, 21 July (accessed 22 November 2022)

Dadoo, S. (2022b) '**Israel's Spyware Diplomacy in Africa**', *Orient XXI*, 12 September (accessed 10 January 2023)

Dogbevi, E.K. (2022) '**Revealed: Israeli Tech Company NSO's Pegasus Was Used in Ghana – Reports**', *Ghana Business News*, 22 January (accessed 22 November 2022)

Economist Intelligence (2021) ***Democracy Index 2021: The China Challenge*** (accessed 22 November 2022)

Freedom House (2022) ***Freedom in the World 2022: Ghana*** (accessed 22 November 2022)

Freedom House (2021) ***Freedom on the Net 2021: Ghana*** (accessed 22 November 2022)

Ghana Web (2020) '**Election Leaks: Did Cambridge Analytica Play NDC and NPP Ahead of 2016 Polls?**', 28 February (accessed 22 November 2022)

Gurijala, B. (2021) '**What is Pegasus? A Cybersecurity Expert Explains how the Spyware Invades Phones and What It Does When It Gets In**', *The Conversation*, 9 August (accessed 10 February 2023)

Macdonald, A. (2022) '**Ghanaians Encouraged to Complete Biometric Capture for SIM Registration as Deadline Nears**', *Biometric Update*, 28 November (accessed 9 January 2023)

Muya, C. (2021) '**Internet Shutdowns and the Future of African Democracy: What More Can We Do?**', *Open Internet for Democracy*, 7 April (accessed 8 January 2023)

Nkwanyana, K. (2021) '**China's AI Deployment in Africa Poses Risks to Security and Sovereignty**', *The Strategist*, 5 May (accessed 9 January 2023)

Nyabor, J. (2021) '**Ghana: Arbitrary Arrests & Torture of Journalists, How Free is the Press?**', *The Africa Report*, 26 May (accessed 9 January 2023)

Odartey-Wellington, F. (2014) 'Technological Invasion of Privacy: The Need for Appropriate Responses to the New Surveillance Society in Ghana', *CDD-Ghana Briefing Paper* 13.4: 1–10

Olukotun, D. (2016) '**Victory! President of Ghana Says No to Internet Shutdowns During Coming Elections**', *Access Now*, 16 August (accessed 10 January 2023)

Rozen, J. (2020) '**US, UK, Interpol Give Ghana Phone Hacking Tools, Raising Journalist Concerns on Safety and Confidentiality**', *CPJ*, 14 July (accessed 4 January 2023)

Techfocus24 (2021) '**Celltel Set to Begin US$300 Million Ghana Smart Cities Project**', *News Ghana*, 24 December (accessed 8 January 2023)

Transparency International (2022) ***Corruption Perceptions Index: Ghana*** (accessed 10 February 2023)

Waters, S. (2017) '**The Effects of Mass Surveillance on Journalists' Relations with Confidential Sources**', *Digital Journalism* 6.10: 1294–1313, DOI: 10.1080/21670811.2017.1365616 (accessed 24 April 2023)

Whatsup News (2021) '**Gov't 10,000 Surveillance Cameras to be Completed by December**', 4 November (accessed 9 January 2023)

Mapping the supply of surveillance technologies to Africa

Morocco country report

Amira Galal

1. Introduction

In recent years, Morocco has invested heavily in technology and infrastructure for digital surveillance, including the implementation of various laws and regulations. While digital surveillance can be an effective tool for protecting national security, it can also raise significant concerns about privacy and civil liberties. In Morocco, the use of digital surveillance has been the subject of ongoing debate, with human rights organisations, civil society organisations (CSOs), and activists raising concerns about its impact on individual rights and freedoms.

One of the key issues surrounding Moroccan digital surveillance is a lack of transparency and accountability. Critics argue that the extent of the government's monitoring activities is not well understood and that there is a lack of a clear legal framework governing the use of digital surveillance tools. This can result in a lack of independent oversight and checks and balances, making it easier for the authorities to abuse their power and violate the privacy of citizens.

Another concern is the potential for government to use digital surveillance to target journalists, human rights activists, and political opposition. In some cases, individuals who have spoken out against the government or reported on sensitive issues have reported being targeted for surveillance and harassment. This can have a chilling effect on freedom of speech and expression as individuals may be afraid to express their opinions for fear of government retaliation.

Despite these concerns, the Moroccan government has argued that digital surveillance is necessary for national security and law enforcement purposes, and it claims that such surveillance is subject to strict regulations and oversight. For example, the government has stated that all digital surveillance activities must be authorised by a court order and that the data collected is only used for specific purposes, such as preventing terrorism or investigating serious crimes. This report will assess whether such claims are supported by evidence.

However, human rights organisations and civil society groups argue that these regulations are not always respected in practice. In some cases, it has been reported that digital surveillance has been used to target individuals without sufficient evidence or justification. Additionally, there have been instances where the authorities have refused to disclose information about their monitoring activities, making it difficult to hold them accountable for any abuses.

2. Background

Morocco is the most westerly North African country with an ethnically diverse population of some 37.6 million Arabs, Amazigh/Berbers, and Sahrawis (tribal communities concentrated in Morocco's deserts and contested Western Sahara region). Its population is almost entirely Sunni Muslim and is largely conservative and religious. Morocco is a constitutional monarchy and holds regular multiparty elections, although King Mohammed VI maintains full dominance through a combination of substantial formal powers and informal lines of influence in both state and society. The current political climate has improved since the reign of his father, King Hassan II, when Morocco was reported to have had one of the worst human rights records in Africa and the world. Nonetheless, repression of political dissidence, and torture of citizens by officials, is still commonplace (El Hamamouchi 2023).

The Western Sahara, annexed by Morocco in 1975, is a controversial topic for both human rights defenders and civilians. Since annexation, it has been the subject of one of the longest-standing conflicts in the world, that between Morocco and the indigenous Sahrawi population, which is led by the Polisario Front. The conflict has killed between 14,000 and 21,000 people. A ceasefire agreement was reached in 1991 but broke down in November 2020. Since then, Amnesty International has documented human rights violations by the Moroccan security forces against multiple Sahrawi activists and human rights defenders, including cases of torture and rape (MacDonald 2022).

The country's Amazigh account for at least 40 per cent of the population and most Moroccans have Amazigh roots. Nonetheless, most Amazigh communities are socially, economically, and politically marginalised, driving the widescale Hirak Rif protests[1] in the northern Amazigh Rif region which stemmed from inequities experienced by many Amazigh residents and their inability to obtain justice through the political system. The state cracked down hard on the protests, arresting hundreds of activists and protesters. The Euro-Mediterranean Human Rights Monitor reported in 2021 that many had been subjected in detention to violations that affected their health and they were denied necessary health care (Euro-Mediterranean Human Rights Monitor 2021).

Terrorist groups in the Sahel, particularly in the so-called 'triangle of death' (Mali, Niger, and Burkina Faso), pose a serious threat to Morocco and its

[1] The Hirak Rif Movement or Rif Movement (meaning 'Movement of the Rif') was a popular mass protest movement that took place in the Berber-speaking Rif region in northern Morocco between October 2016 and June 2017. The mass protest movement was met with repression, with many violent clashes between police and protesters in various cities and towns.

porous desert borders means that outlaws can enter and exit the country with ease. Similarly, Latin American drug traffickers have increasingly used Morocco for their transnational cocaine trade, leveraging Moroccan gangs' foothold in Europe, Africa, and the Middle East.

Morocco's constitution officially guarantees freedom of expression and the right to information, and it prohibits censorship. However, journalists are routinely subjected to arrest without warrant and prolonged pre-trial detention (The Tahrir Institute 2022). Corruption, the role of Islam, the status of the Western Sahara, the security services, the handling of the Covid-19 pandemic, and crackdowns on protests are among subjects effectively banned from media coverage. As such, the country's media is heavily restricted, de facto subject to strict censorship, many civil liberties are constrained, and criticism of the king and his entourage is severely penalised (*Africa News* 2022).

In this context of political repression, Morocco's widespread use of surveillance technologies and spyware is a serious concern. Journalists, activists, and bloggers that are critical of the state are routinely subject to arrest. Vague legislation regarding freedom of expression and the lack of an independent judiciary are used as an effective deterrent to public debate and collective action.

While the country's constitution protects freedom of expression and the right to privacy, as well as having a data protection law in place (Law No. 09-08 of 2009[2]), these laws are vaguely worded and allow for surveillance in certain circumstances, with judicial approval. This proves a great challenge given the judiciary's lack of independence and accountability and lack of oversight of the intelligence services.

Issues surrounding digital surveillance and the right to privacy are obfuscated in Morocco, grounded in vague legislation, weak national institutions, and ambiguous adherence to international treaties. For instance, Article 24 of the Moroccan 2011 Constitution[3] guarantees citizens the fundamental right to privacy, stating:

> Any person has the right to the protection of their private life. The home is inviolable. Searches may only be conducted in the conditions and forms provided by the law. Private communications, under whatever form that may be, are secret. Only justice can authorise, under the conditions and following the forms provided by the law, the access to their content, their total or partial divulgation or their summons [invocation] at the demand [charge] of whosoever.

[2] See **Morocco Data Protection Factsheet**.

[3] See **Moroccan Constitution 2011**.

Another instance of ambiguity relates to Morocco's adoption of the International Covenant on Civil and Political Rights (ICCPR).[4] Article 17 of the ICCPR states that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. Signatories of the ICCPR are obliged to 'adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]' (United Nations 1994). However, while Morocco's constitution affirms that international treaties have primacy over national law, it also states that this is only 'within the framework of the dispositions of the Constitution and laws of the Kingdom, in respect of its immutable national identity [Islam]'.[5] This ambiguous wording renders unclear the assertion of international treaties' supremacy over national law.

Amnesty International has documented numerous cases of the state using digital surveillance to crack down on human rights defenders. The organisation found strong evidence of Moroccan authorities using the NSO Group's Pegasus spyware. Evidence shows that as many as 10,000 individuals were targeted – including its own monarch, King Mohammed VI. This is the only confirmed case of a country monitoring its own head of state – though pundits contend that including the king's phone in the spying operation merely provided a convenient alibi, intended to exonerate him should the spyware operation be uncovered.

Prominent figures abroad have also been targeted by Morocco's surveillance. France is considering criminal charges against Moroccan officials for using Pegasus spyware to monitor French journalists and President Emmanuel Macron himself (Chrisafis 2021). Algeria also broke diplomatic ties with Morocco, citing 'massive and systemic acts of espionage' (Allen and Lime 2021) that targeted key members of its government.

In 2022, Amnesty International (2022a) uncovered the use of Pegasus spyware against activists from the disputed Western Sahara region. Moroccan authorities demanded that 'Amnesty provide evidence' for its claims in March 2022 and dismissed its report as 'arbitrary accusations' (Bounani 2021). The authorities claim that they never acquired computer software to infiltrate communications devices (*The New Arab* 2022). Yet analysis of human rights defenders' mobile phones conclusively showed that spyware had been installed on their devices.

Amnesty International says targeted attacks have been ongoing since at least 2017. While NSO Group has not outright denied the use of its software to monitor human rights defenders, it issued a statement in 2019 saying that it

[4] See **International Covenant on Civil and Political Rights**.

[5] See **Moroccan Consitution 2011**.

would investigate the allegations. The findings of the investigation have not been released.

In 2019, Carnegie Endowment for International Peace (Feldstein 2019) reported that Morocco had been using Chinese facial recognition software for surveillance. The following year, the interior ministry reportedly made a closed call for tenders worth almost US$10m (MAD100m) to equip drones and CCTV cameras, ostensibly to limit 'delinquency' and enforce Covid-19 social distancing and mask-wearing rules (Samaro 2022).

As digital and physical attacks on journalists and human rights defenders increase, observers report that Morocco is slowly reverting from being a 'soft' authoritarian government to a full dictatorship.

3. Supply of surveillance technology

Evidence shows that Morocco has a well-equipped and diverse surveillance landscape having procured millions of dollars' worth of digital forensics, network monitoring, spyware, and telecommunications interception from countries all over the world, including Israel, Finland, Cyprus, Italy, Germany, France, and China, among others. This section documents which companies from which countries are supplying which surveillance technologies to the Moroccan government. The information is organised into five categories.

Internet interception

In 2011, the Moroccan government was found to have invested US$2.2m in Eagle System, an online surveillance system that allows it to censor and monitor internet traffic using Deep Packet Inspection. Eagle was developed by French company Amesys Bull and is capable of intercepting countrywide communications, including email, Facebook, and instant Messenger conversations. Investigations by Privacy International in 2016 (Privacy International 2016b) found evidence of Eagle being used to spy on Moroccan civil society but they were unable to directly link it to the government. However, French investigative journalism website Reflet found direct evidence of Morocco's purchase of Eagle System in the form of procurement requests and invoices (Privacy International 2019). The outlet suggested that the French government may be complicit in the sale of the software, pointing to former French President Nicolas Sarkozy's contracts with Libya to provide Eagle and the continued close relations between the Moroccan and French governments.

Morocco also purchased malware from the Italian surveillance technology firm Hacking Team to use against journalists (Privacy International 2015). In 2015, a large trove of Hacking Team's internal documents was leaked, revealing that Morocco was one of the company's clients. The Hacking Team leaks showed that the two Moroccan intelligence agencies – the High Council for National Defence (CSDN) and the Directory of Territorial Surveillance (DST) – both purchased Remote Action Trojan malware that provides the attacker with full remote control over a target's system. The report showed that CSDN first acquired the malware in 2009 and the DST obtained it in 2012. Since the 2015 leak, there have been no further reports about Morocco's use of Hacking Team and it is unclear whether the country is still a client of the company.

Hacking Team first came into the public spotlight in 2012 when its malware was used against citizen media outlet Mamfakinch (Amnesty International

2016). The outlet was attacked a couple of days after the website was awarded a Google and Global Voices Breaking Borders Award in recognition of efforts to use the internet to promote public debate and democratic values. An email received via the contact form on the organisation's website, titled 'Dénonciation', contained a link to what appeared to be a Microsoft Word document labelled '*scandale* (2).doc' along with a message asking to keep the sender's identity anonymous. Some members of the organisation tried to open the file which ultimately necessitated 'drastic measures' to clean their computers before the file was sent for analysis.

Analysis showed that the file was a type of malicious software (malware) called a Trojan horse because of its outer cover disguises and its intent to take control of the target's computer, including taking screenshots, intercepting email, recording chats, and covertly capturing data using the computer's microphone and webcam, all while bypassing virus detection (Marquis-Boire 2012). The spy tool would detect which operating system the targeted computer was running, before attempting to infect it with either a Mac or Windows version of the virus. Once installed, the Trojan tried to connect to an IP address that was traced to US-based hosting company Linode, which provides 'virtual private servers' that host files but help mask their origin. Linode says using its servers for such purposes violates its terms of service and confirmed the IP address in question was no longer active. The process is clearly designed to obscure the identity of the government conducting the spying.

Unfortunately, Mamfakinch was forced to close as staff felt that 'it didn't matter whether our machines were clean or not, or whether we used encryption or not. They proved they could do it once. It means they can do it again' (Amnesty International 2016). Three months after the malware was detected, the outlet's team of 30 dwindled to just three contributors and eventually Mamfakinch closed due to safety concerns and fears that the government would pursue its contributors.

A Citizen Lab (Marczak *et al*. 2014) report showed that the Moroccan government had also used FinFisher malware produced by the Gamma Group of companies. Morocco has been found to use Israeli Pegasus spyware to monitor local journalists, activists, government members, foreign politicians and, as described, its own king (Bachir 2021).

Mobile interception

Morocco has also been found to intercept mobile communications. Data released by the Finnish government under the Freedom of Information Act (Privacy International 2016a) showed that Finland has issued several licences to the Finnish subsidiary of the Canadian company EXFO allowing sales of telecommunications surveillance technology to countries including Morocco. Switzerland also released a document that revealed a list of countries that bought surveillance technologies from Swiss companies. Among the purchasers of advanced surveillance technology was Morocco, which appeared to have tested mobile telecommunication interception or jamming equipment in 2013 or 2014 (Privacy International 2015).

Citizen Lab (Marczak *et al*. 2020) reported with 'high confidence' that Morocco's interior ministry was a 'likely' client of Circles Technologies from 2018. NSO Group-affiliated Circles is a company that exploits telecommunications infrastructures' weaknesses to monitor calls, texts, and locations of phones around the globe. The report said that Citizen Lab's scanning had 'identified what appeared to be a single Circles system in Morocco'.

Security and defence company Total Secure Defence (n.d.) showed on its website that it had sold Morocco the GSM/3G Interception System and the international mobile subscriber identity catcher (IMSI catcher).

Social media monitoring

Morocco's media landscape has traditionally been very restricted and social media has posed a challenge to government fears of an Arab Spring-style mobilisation online. Many activists and journalists express concerns that they may be subject to surveillance. A Human Rights Watch report (2020) highlighted a growing government crackdown on social media users in recent years. Students, activists, citizen journalists, and social media commentators who have criticised Moroccan authorities and King Mohammed VI have been arrested and charged.

Ostensibly to fight disinformation during the Covid-19 pandemic, Morocco's government council approved but then withdrew Draft Law 22-20 related to the use of social media and open broadcast networks. According to the justice ministry, the law would 'put an end to a legislative vacuum' regarding cybercrime, allow effective response to disinformation and acts which 'damage the reputation and honour of individuals',[6] and harmonise the country's legislation with the Budapest Convention on Cybercrime,[7] despite the convention not including any clauses related to freedom of expression on social media. The draft law stipulates that network providers should restrict access to and suppress online content that could pose a threat to security and public order within 24 hours.

[6] See Majalat **'In Morocco, Under Pressure From Civil Society, the 'Liberticide' Bill Concerning Social Networks is Backtracking'**.

[7] See **Convention on Cybercrime**.

The year 2022 saw a marked rise in the number of activists and influencers being charged and sentenced for social media content. In March, authorities arrested blogger Saida Al-Alami (Skyline 2022) over posts critical of the Moroccan government and security services. Al-Alami, a well-known activist, has been vocal in her criticism of Morocco's authorities. The Court of Appeals convicted her of 'insulting a legally regulated institution', 'insulting public officials', 'denigrating judicial decisions' and 'spreading false allegations and facts against individuals with the aim of defaming them' (*ibid.*). She was sentenced to two years' imprisonment, later extended to three. Just days after Al-Alami's arrest, blogger Rabih al-Ablaq was detained for videos he had shared on Facebook which questioned the wealth of the king and prime minister (El Hamamouchi 2022). He was imprisoned for four years for 'publicly violating the duty of reverence and respect for the King's person' (*ibid.*).

Similarly, in September 2022, Rida Benotmane was prosecuted for criticising the authorities on YouTube and Facebook (Amnesty International 2022b). He was interrogated over posts that called for a public march against abuses by security forces and YouTube videos in which he denounced the authorities for ignoring people's demands for social justice and warned against the potential use of Covid vaccine passes as a tool of repression. He was charged with 'insulting a body regulated by law', 'insulting public officials while carrying out their duties', and 'broadcasting and distributing false allegations without consent'. He was also charged with breaching emergency health laws.

Safe city/smart city

Morocco has been ramping up efforts to adopt digital technologies while investing millions of dollars in tech-based solutions. The authorities claim that they aim to promote economic growth, increase digitalisation, and strengthen the country's innovation ecosystem through the new Maroc Digital 2020 strategy and the creation of the Digital Development Agency.

The pandemic accelerated the adoption of digital surveillance technologies in Morocco (Navarro Amuedo 2020), with the government introducing broad measures to control the spread of Covid-19 using emerging digital technologies and biometric systems such as digital identity, a Covid-19 contact tracing app, vaccine passports, and widespread installation of facial recognition software into surveillance cameras and drones.

In April 2021, the Ministry of Interior reportedly distributed a non-public call for tenders (Darouiche 2021) worth around US$94m to equip drones and CCTV cameras with facial recognition systems in Casablanca to monitor citizens' movement, limit 'delinquency', and detect persons not wearing masks or observing Covid-19 social distancing measures. The biometric system relies on centralised data centres, databases, and algorithms that analyse citizens' movement and behaviours.

Moroccan authorities placed the regulation of biometric facial recognition software in the hands of the Moroccan National Commission for the Control of Personal Data Protection (CNDP), which had announced a moratorium on its use by public or private entities. CNDP raised concerns over the technology's impact on people's privacy and human rights and announced the need for extended consultations. The moratorium lapsed and, in August 2022, Morocco started tendering for facial recognition systems for installation in the capital's Rabat-Salé Airport (Rahhali 2022), reportedly the first time the technology will used in the country.

Biometric ID

In 2022, Morocco presented and launched its first digital identification system (*Identity Review* 2022). The Moroccan digital identity cards allow holders to prove their identity as a Moroccan citizen. As stated in a *Morocco World News* report (Rahhali 2022), 'Moroccans can use their [ID cards] as proof of identity for different places. They can physically present their electronic identity card to agents of authorized institutions to scan it and prove the holder's identity.'

Table 3.1 Supply chains of surveillance technology

Contract	Description	Dirham (MAD)	US$
Internet interception			
Amesys Bull (France)	Eagle System – can intercept countrywide communications including email, Facebook, and instant Messenger conversations (Privacy International 2016b).	20m	2m
Hacking Team (Italy)	RCS – can intercept communications, log keystrokes, and remotely control a target's device. Two purchased. Since a 2015 leak, there have been no further reports about Morocco's use of Hacking Team, and it is unclear whether the country is still a client of the company (Privacy International 2015).	4m	400,000
Gamma Group (UK/ Germany)	In 2012, there were allegations that FinFisher surveillance software had been used to spy on political dissidents. There have been no recent reports of its use, and it is unclear whether the country is still using the tool (Marczak *et al*. 2014).	Unknown	Unknown
NSO Group (Israel)	In 2021, it was reported that Pegasus spyware had been used to target journalists, human rights activists, and other public figures (Amnesty International 2022a).	~ 50m	~ 5m*
Mobile interception			
Circles Technologies (Israel)	Moroccan authorities have denied using Circles technology to monitor calls, texts, and locations of phones around the globe, but a 2020 Citizen Lab report provides evidence to the contrary (Marczak et al. 2020).	~ 30m	~ 3m†
Amesys (France)	In 2012, it was reported that Moroccan authorities had acquired a GSM/3G interception system, which can intercept phone calls and text messages (Total Secure Defence n.d.).	Unknown	Unknown
Social media monitoring			
Unknown	Although specific companies or vendors providing social media surveillance technology to Morocco are unknown, there are reports of social media surveillance leading to arrest of journalists (Human Rights Watch 2019).	Unknown	Unknown
Safe cities			
No evidence of surveillance technology			
Biometric ID			
IDEMIA (France)	MorphoWave Compact used in biometric entry-exit system launched in 2018. Uses fingerprint scanners and facial recognition technology to capture and verify the identities of people entering and leaving the country (Biotime 2020).	Unknown	Unknown
	Total	104m	10.4m

Note: *Precise figure unknown but believed to be around this figure from other Pegasus supply contracts (see Ghana report). † Precise figure unknown but believed to be around this figure from other Circles supply contracts (see Nigeria report).

Source: Authors' own, created using data from above cited sources.

4. Impacts

While most of the measures detailed are promoted by the Moroccan government as having positive consequences for safety and security, they inevitably violate key human rights recognised internationally and set out by the Moroccan state itself. For instance, Article 24 of the 2011 Constitution of Morocco[8] guarantees the right to privacy.

Morocco also has a data protection law (Law No. 09-08 of 2009)[9] in place that says that the processing of personal data can only be made if the subject has unambiguously consented to the transaction of all proposed transactions relating to their personal data. Additionally, the law stipulates that personal data cannot be disclosed to third parties without prior consent. However, the law provides for exceptions and the language is again ambiguous. For example, Article 44 states that disclosure to third parties may occur without prior consent if in the 'public interest'.[10] The law does not lay out parameters for what may be considered as public interest, leaving the law subject to abuse.

Moroccan legislation tends largely to be vaguely worded (Freedom House n.d.) and may be breached if part of a criminal investigation when a judicial order is issued. Though the law identifies specific conditions under which such orders may be granted, there remain vast grey areas regarding the discretionary powers offered to judges and intelligence agencies. The lack of an independent judiciary, and the absence of public scrutiny over the work of the intelligence services, challenge democratic oversight of these operations and leave much of the country's legislation subject to manipulation. This tactic, documented by numerous NGOs and civil society members (World Bank 2003), violates Morocco's international human rights obligations, including the right to privacy, freedom of expression and association, and the right to due process and a fair trial for those accused of a crime.

[8] See **Data Protection Factsheet**.

[9] See **Data Protection Laws of the World: Morocco**.

[10] *Ibid.*

5. Solutions

The first step to solving the problem of Moroccan digital surveillance is to understand its root causes. One of the main drivers behind digital surveillance in the country is the desire for national security. The country faces many internal and external threats that pose a risk to its stability and security. For example, Morocco faces the threat of terrorism from extremist groups, as well as threats from drug trafficking and cybercrime.

To protect its citizens, the government has implemented a surveillance system that monitors online activities. However, the government's justification for digital surveillance goes beyond the protection of national security. Morocco has a history of political repression and human rights violations, and the use of digital surveillance is seen as a tool for suppressing dissent, rights to privacy, and freedom of expression. It has led to a widespread perception among the population that the government is using digital surveillance to restrict freedom of speech and expression.

It is essential to find a balance between national security and the protection of citizens' rights. It is essential for the Moroccan government to engage in ongoing dialogue with civil society and human rights organisations, and to put in place effective oversight mechanisms and legal frameworks to ensure that digital surveillance is used in a responsible and ethical manner.

Regulation and oversight

One of the first steps in resolving the issue of digital surveillance in Morocco is to establish clear and transparent legal frameworks that govern its use. This includes clear regulations and guidelines for the government to follow when monitoring digital communications and activities, as well as clear oversight mechanisms and remedies for individuals who believe their rights have been violated. The legal framework should be guided by international human rights standards and principles, including the rights to privacy and freedom of expression. This will ensure that the use of digital surveillance is subject to appropriate checks and balances, and that individuals can challenge abuses of power. There is no single solution that will address all concerns around digital surveillance in Morocco and a multifaceted approach will certainly be needed.

Transparency and accountability

The government should engage in dialogue with citizens to build trust and confidence in digital surveillance systems to ensure transparency and accountability. This can be achieved through public consultations and engagement with CSOs that are dedicated to protecting the rights of citizens. The government should also ensure that citizens have access to information about surveillance systems and the ways in which they are used. Additionally, there should be mechanisms in place for people to challenge and hold organisations accountable for any potential misuse of their data.

In addition to advocacy for these kinds of national reforms and establishing clear legal frameworks, human rights defenders should leverage independent means of reclaiming digital spaces without putting themselves at risk.

Privacy-focused technologies

Another important step is the development of technical solutions that protect citizens' privacy and security. This can be achieved through the use of encryption technologies, such as virtual private networks (VPNs) and secure messaging apps that help prevent unauthorised access to digital information and protect sensitive data from theft or misuse.

Awareness and education

Greater awareness and education about the issue of digital surveillance is needed so that people can understand the risks and take steps to protect themselves. This could include providing information about privacy-focused technologies, as well as tips for using the internet and social media securely and confidentially. On an international level, human rights defenders should develop comprehensive archives that catalogue surveillance cases and push for litigation against suppliers of surveillance technologies that are likely to be abused.

6. Surveillance stories

There are many cases in Morocco which illustrate how human rights have come under fire from digital surveillance in recent years.

Journalists

As far back as 2013, independent journalist Ali Anouzla was accused of 'glorifying terrorism' (Amnesty International 2013) after being subject to pervasive surveillance. A target of nationalist hacker groups, Anouzla also found numerous online recordings on social media sharing his private phone conversations. After publicly stating that this was likely linked to Morocco's intelligence service, he was sued by the government. He told Privacy International:

> *Knowing your phone conversations are constantly listened to is disturbing. It restrains my private life. For instance, even though I don't drink, I know I cannot go to a place where people drink alcohol because I could be photographed and in a Muslim country this could be used to shock people. Other than that, it never prevented me from saying and writing anything.*
> (Privacy International 2018: 34)

Omar Radi is an award-winning Moroccan investigative journalist and activist who worked for national and international media outlets. His work investigated links between corporate and political interests in Morocco and it touched upon questions of corruption and human rights abuses in Morocco. His phone was hacked using Pegasus spyware in June 2020 after he uncovered a scandal implicating nearly 100 public officials of illicitly acquiring residential properties on state lands at a fraction of their worth. In March 2022, he was sentenced to six years' imprisonment on charges of espionage and rape (Amnesty International 2022c).

An investigation by Amnesty International's Security Lab found that Radi's phone had been subjected to multiple network injections (Amnesty International 2020). The attacks occurred over a period when Radi was being repeatedly harassed by the Moroccan authorities, with one attack taking place just days after NSO Group pledged to stop its products being used in human rights abuses. The attacks continued until at least January 2020.

The academic

Since 2015, French-Moroccan academic and human rights defender Maati Monjib has believed he is under digital surveillance by the authorities. This has had a detrimental impact on his activism and daily life. Constantly analysing his digital communications caused great psychological harm. He told Amnesty International:

> *I need to constantly analyse the consequences of what I say and the risk that this may lead to defamatory accusations against me. This even applies to very practical things like arranging meetings or a dinner downtown.*
> (Amnesty International 2019a)

Amnesty International investigated his case and found he had been repeatedly targeted with malicious Short Message Service (SMS) messages that carried links to websites connected to NSO Group's Pegasus spyware. In 2020, Monjib was arrested in Rabat and sentenced to one year's imprisonment for 'undermining the internal security of the state' and 'defrauding' the government.

The YouTuber

In 2019, Moroccan YouTuber Mohamed Sekkaki was sentenced to four years' imprisonment and fined around US$4,000 after being found guilty of insulting King Mohammad VI, having described the king's speeches as 'useless'. He also described Moroccans as 'donkeys' as they silently watched their rights being abused. At the end of the now-removed 12-minute-long video, Sekkaki predicted his arrest (BBC News 2019).

Human rights defenders

Mahjoub Maliha, an activist supporting human rights in the longstanding Western Sahara conflict between Morocco and Sahrawi separatists was shocked to find out that Moroccan authorities had hacked his phone. He told Amnesty International that he noticed the breach when he noticed that emails from Sahrawi human rights defenders were appearing as read on his phone. Amnesty's tech team confirmed the device was infected by Pegasus.

Human rights defender Aminatou Haidar was also found to have been targeted with Pegasus spyware. Sahrawi activist group, the Nushatta Foundation, said that Morocco employed multiple techniques, including Pegasus spyware, to extract compromising information with which to discredit Sahrawi activists:

> *Pegasus allows Moroccan intelligence to access all our data, including personal information that can be used to defame us and to block connections we try to make with outside countries… We will be accused of sleeping with people because we live in a conservative society and that is a good way to discredit us.*
> (Rickett 2022)

After receiving email security alerts from Apple saying her phones may have been targeted by spyware, Haidar was referred to Amnesty International's Security Lab. Forensic analysis confirmed that her phone had been targeted by Pegasus spyware dating back to September 2018. These findings were corroborated by Citizen Lab (Amnesty International 2019b).

The lawyer

Abdessadek El Bouchataoui, a lawyer and human rights defender, was imprisoned for participating in social justice protests during the Hirak protests of 2016–17. In February 2017, Morocco sentenced him to 20 months' imprisonment for online posts in which he criticised the excessive force used by the authorities against protesters. He told Amnesty International (2019b): 'Surveillance is a type of punishment. You can't behave freely. It is part of their strategy to make you suspect you're being watched so you feel like you're under pressure all the time', adding that he had faced death threats, been followed, and that his family and associates had been harassed. He has now sought asylum in France.

References

Africa News (2022) '**Morocco: Activist Gets Four Years in Prison for Criticising King**', 1 May (accessed 1 February 2023)

Allen, N. and Lime, M.L. (2021) ***How Digital Espionage Tools Exacerbate Authoritarianism Across Africa***, 19 November, Washington DC: Brookings Institution (accessed 6 July 2023)

Amnesty International (2022a) ***Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months – New Evidence***, 9 March (accessed 25 January 2023)

Amnesty International (2022b) ***Morocco: Free Activist Rida Benotmane Immediately and Drop All Charges Against Him***, 21 September (accessed 9 February 2023)

Amnesty International (2022c) ***Morocco: Ensure Fair Appeal Trial to Journalist Omar Radi***, 2 March (accessed 10 July 2023)

Amnesty International (2020) ***Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools***, 22 June (accessed 10 July 2023)

Amnesty International (2019a) ***Morocco: Human Rights Defenders Targeted with NSO Group's Spyware***, 10 October (accessed 25 January 2023)

Amnesty International (2019b) '**Moroccan Human Rights Defenders Targeted using Malicious NSO Israeli Spyware**', *Amnesty International*, press release, 10 October (accessed 10 July 2023)

Amnesty International (2016) '**How a Hacking Campaign Helped Shut Down an Award-Winning News Site**', 9 December (accessed 9 February 2023)

Amnesty International (2013) ***Urgent Action: Journalist Charged Under Anti-Terrorism Law***, 26 September (accessed 10 July 2023)

Bachir, M. (2021) '**Pegasus: From its Own King to Algeria, The Infinite Reach of Morocco's Intelligence Services**', *Middle East Eye*, 21 July (accessed 25 January 2023)

BBC News (2019) ***Morocco YouTuber Mohamed Sekkaki Jailed for Insulting King Mohammed VI***, 27 December (accessed 10 July 2023)

Biotime (2020) ***The Kingdom of Morocco Launches a National Digital ID Platform with IDEMIA*** (accessed 10 July 2023)

Bounani, A. (2021) '**Pegasus: une affaire marocaine, vraiment?**', *Le Point Afrique*, 28 July (accessed 25 January 2023)

Chrisafis, A. (2021) '**Emmanuel Macron Identified in Leaked Pegasus Project Data**', *The Guardian*, 20 July (accessed 25 January 2023)

Darouiche, M. (2021) '**Casablanca sous l'œil des caméras et des drones**', *Hespress*, 22 April (accessed 25 January 2023)

El Hamamouchi, A. (2023) '**Human Rights Deteriorating in Morocco: Rabat's Defamation Drive**', *Qantara*, 2 February (accessed 2 February 2023)

El Hamamouchi, A. (2022) '**Escalating Repression in Morocco**', *Sada*, 12 May (accessed 9 February 2023)

Euro-Mediterranean Human Rights Monitor (2021) '**Morocco: Euro-Med Monitor Condemns the Ill-Treatment of Hirak Rif Detainees**', press release, 25 February (accessed 1 February 2023)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Working Paper, Washington DC: Carnegie Endowment for International Peace (accessed 25 January 2023)

Freedom House (n.d.) ***Freedom on the Net 2021: Morocco*** (accessed 25 January 2023)

Human Rights Watch (2020) ***Morocco: Crackdown on Social Media Critics***, 5 February (accessed 25 January 2023)

Human Rights Watch (2019) ***Morocco: Free Outspoken Journalist Jailed Over Tweet***, 28 December (accessed 10 July 2023)

Identity Review (2022) '**Moroccan Digital Identity: Expanding Accessibility. Inside Morocco's Growth and Acceleration of Digital Identification Technologies**', 20 June (accessed 10 July 2023)

MacDonald, A. (2022) '**Western Sahara: Women Activists Say They Face Rape, House Arrest and Forced Divorce**', *Middle East Eye*, 21 April (accessed 1 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 1 February 2023)

Marczak, B. ; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) **Mapping Hacking Team's 'Untraceable' Spyware**, Citizen Lab, 17 February (accessed 25 January 2023)

Marquis-Boire, M. (2012) ***Backdoors are Forever: Hacking Team and the Targeting of Dissent?***, Citizen Lab, 10 October (accessed 9 January 2023)

Navarro Amuedo, A. (2020) '**Drones with Domestic Technology to Keep the Virus at Bay in Morocco**', *Atalayar*, 8 May (accessed 25 January 2023)

Privacy International (2019) ***State of Privacy Morocco***, 26 January (accessed 25 January 2023)

Privacy International (2018) ***Their Eyes On Me: Stories of Surveillance in Morocco***, London: Privacy International (accessed 25 January 2023)

Privacy International (2016a) ***With New Spying Powers on Horizon, Surveillance Companies Descend on UK,*** 9 March (accessed 10 July 2023)

Privacy International (2016b) '**The Right to Privacy in Morocco: Human Rights Committee 116th Session**', London: Privacy International (accessed 16 August 2023)

Privacy International (2015) ***Facing the Truth: Hacking Team Leak Confirms Moroccan Government Use of Spyware***, 10 July (accessed 25 January 2023)

Rahhali, L. (2022) '**ONDA Opens Tender for New Face ID Recognition System in Rabat Airport**', *Morocco World News*, 4 August (accessed 9 February 2023)

Rickett, O. (2022) '**Pegasus Spyware: Western Sahara Activist Aminatou Haidar Targeted**', *Middle East Eye*, 9 March (accessed 10 July 2023)

Samaro, D. (2022) '**Pandemic Tech and Digital Rights in Morocco**', *Global Voices*, 30 March (accessed 25 January 2023)

Skyline (2022) '**Morocco: Skyline Condemns the Increase in the Prison Sentence Against Activist 'Saida Al-Alami' and Calls on the Authorities to Release Her Immediately and Unconditionally**', *Skyline International for Human Rights*, press release, 26 September (accessed 9 February 2023)

The New Arab (2022) '**Morocco Demands Amnesty to Provide Evidence of Pegasus Spyware Claims**', 18 March (accessed 25 January 2023)

The Tahrir Institute (2022) *Press Freedoms in Morocco*, Washington DC: Tahrir Institute for Middle East Policy

Total Secure Defence (n.d.) ***Exporting GSM/3G Interception & IMSI Catcher to Morocco*** (accessed 9 February 2023)

United Nations (1994) ***Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, HRI/GEN/1/Rev.1 at 21*** (accessed 6 July 2023)

World Bank (2003) ***Morocco: Legal and Judicial Sector Assessment***, Washington DC: World Bank (accessed 25 January 2023)

Mapping the supply of surveillance technologies to Africa

Malawi country report

Jimmy Kainja

1. Introduction

Malawians could be sleepwalking into a surveillance state. The government has implemented data collection and centralisation programmes, including a biometric national identification card for everyone over 16 years of age and mandatory SIM card registration; a data centre has been commissioned; and the country's telecommunications regulator has announced plans for a smart city.

This report shows that, in Malawi, state surveillance operates outside any adequate legal framework, violating citizens' constitutional rights. A data protection law has remained a draft bill since 2021, despite its pressing nature, and media coverage and academic research on the worrying expansion of digital surveillance in Malawi has been scant and hard to find to date. Despite these challenges, this report breaks new ground by providing the first landscape analysis of digital surveillance in Malawi. In doing so, it provides a platform upon which other researchers can build.

In July 2022, Malawi launched a data centre in the country's commercial city, Blantyre. The Malawian State President Lazarus Chakwera registered his excitement by saying the centre would guarantee information security to investors and make Malawi a location of choice for them. However, despite the president's optimism and assurance, the data centre project is just the latest to concern data collection without regard for data protection and privacy. The Government of Malawi's partner in the project, Huawei, has a chequered reputation over similar projects with the governments of Zambia and Uganda, where its employees helped ruling parties surveil the opposition political parties.

Though Section 21 of Malawi's constitution guarantees citizens' right to privacy of communication, Malawi lacks robust data protection laws. The Communications Act No. 34 of 2016[1] and the Electronic Transactions and Cyber Security Act No. 33 of 2016[2] have data protection sections criminalising electronic communication interception. However, this legislation does not provide for legal interception of data. Section 84(2) of the Electronic Transactions and Cyber Security Act mandates a responsible cabinet minister to identify a circumstance where authorised access to interception of, or interference with, data may be permitted in specific conditions in the regulations – a worrying mandate that is prone to abuse, as the minister is not a politically neutral person. Through the draft Data Protection Bill of

[1] **Communications Act No. 34 (2016)**.

[2] **Electronic Transactions and Cyber Security Act No. 33 (2016)**.

2021,[3] it is clear that the Government of Malawi is aware of legal gaps in the present provisions for data protection. The draft bill aims 'to make provision for the protection of personal data, for regulation of the processing of personal data, and matters connected therewith or incidental thereto'.[4]

Using desk research and a literature review, this report takes a historical approach to examine surveillance programmes and supply chains of surveillance technologies in Malawi. In particular, it examines companies supplying five types of surveillance technologies to Malawi and looks at whose rights are being violated and who is being (dis)advantaged the most. The report also provides case studies and offers possible solutions to the problems associated with surveillance technologies.

[3] **Draft Data Protection Bill 2021**.
[4] *Ibid.*

2. Background

Malawi is in southern Africa, bordering Zambia to the west, Tanzania to the north and northeast, and Mozambique to the east, south, and southwest. It became a British protectorate in 1891 as Nyasaland. It later formed part of the Federation of Nyasaland and Rhodesia, the other countries being Zambia and Zimbabwe. The country gained independence in 1964 and became a republic in 1966, with Kamuzu Banda as its founding president. Upon independence, Malawi returned to the Penal Code of 1936, with its vagrancy laws in sections 180 and 184 (Ó Drisceoil 2022) aimed at monitoring people's movements. Although sections 38 and 39 of the Constitution of the Republic of Malawi 1994[5] provide for freedoms of assembly and movement, respectively, the vagrancy laws were still in force until outlawed in 2017 by the High Court, when it was challenged by a citizen, Mayeso Gwanda.[6]

The legacy of such colonial legal frameworks meant independence did not guarantee human rights and civil liberties for Malawians. Instead, power shifted from white rule to Kamuzu Banda's dictatorship, whose regime outlawed all political parties other than his Malawi Congress Party (MCP). The state-controlled Malawi Broadcasting Corporation was the only broadcaster in the country; there was no television in Malawi for the 30 years that Kamuzu Banda was in power; and the only newspapers allowed to publish belonged to Banda's publishing company, with any other publications belonging to the missionary press, dedicated to the interests of missionaries. Malawi was a police state with heavy censorship, according to Human Rights Watch (1994), overseen by the Malawi Censorship Board established under the Censorship Act of 1968.[7]

Censorship typifies much of Kamuzu Banda's rule. The Malawi Censorship Board dealt with publishing and broadcast materials, overseeing heavy surveillance in the country. In his book *Political Prisoner 3/75* (Mpasu [1995] 2014), the former political prisoner Sam Mpasu narrates how the MCP, with its Youth League wing and the Malawian police's Special Branch, itself a carryover from the colonial administration, created a physical surveillance network through the use of informers, monitoring what people were saying about Kamuzu Banda and the MCP and compliance with MCP's four cornerstones: unity, loyalty, discipline, and obedience. Mpasu's account also shows how ordinary citizens were empowered to surveil one another. Anyone could be a spy: it was a panopticon, Big Brother society.

[5] **Constitution of the Republic of Malawi 1994**.

[6] **Gwanda v S (Constitutional Cause 5 of 2015) [2017] MWHC 23 (10 January 2017)**.

[7] **Censorship and Control of Entertainments Act 1968**.

Data centre

In July 2022, Malawi became the latest African country to commission a data centre in partnership with the Chinese technology giant Huawei (Huaxia 2022). The data centre is part of the Government of Malawi's efforts to get a foothold in the 'fourth industrial revolution', to include embracing big data, artificial intelligence, and the internet of things. State President Lazarus Chakwera said the data centre would guarantee information security for investors, thus making Malawi a location of choice for them (RegTech Africa 2022). However, the specifications of Malawi's data centre were not shared, although it is known that similar projects in Zambia and other countries where the Chinese are funding and building data centres as part of their safe city model come as part of a wider package with hundreds of CCTV cameras enabled with facial recognition, and the new facility will host all government-wide systems (Swinhoe 2022).

The president may be right in his observation about the benefits of the data centre. However, as with Malawi's national digital ID project and SIM card registration, the authorities only pay attention to the benefits of the projects, overlooking safeguards required for the safety of citizens and human rights. Despite optimism for the data centre, the project is concerning for two reasons. First, Huawei, as the Malawi government, has a chequered reputation over surveillance. For example, *The Wall Street Journal* reported that Huawei employees embedded in cybersecurity forces helped ruling parties in Zambia and Uganda intercept encrypted communications and used cell data to track political opponents (Parkinson, Bariyo and Chin 2019). What happened in these countries can easily be replicated elsewhere; African countries are good at imitating each other.

Second, Malawi lacks robust data protection laws. This has complications. Contrary to the president's belief, the data centre is unlikely to attract investors when the country has no data protection laws; robust data protection legislation is a prerequisite to attract investors. Also, without data protection legislation, the data centre could make people's data vulnerable to abuse; without data protection legislation, there is no way this project can guarantee information security. Additionally, it is unclear if Huawei would have access to information at the data centre. The cases of communication interception in Zambia and Uganda mean that these fears are legitimate, more so that Malawi has no clear provisions for legal interception of data.

Hersey (2020) has documented how Malawi established the national ID system at 'breakneck speed'. Led by the United Nations Development Programme (UNDP), the project was touted as necessary because Malawi was the only country in sub-Saharan Africa without a fully implemented national registration system. The UNDP (2022) said the national ID would enable Malawians to 'prove their identity and benefit from their rights'. In addition, Tariq Malik (2020: 6), who worked on the project as a UNDP consultant, said the ID would be critical in combating electoral fraud, and enhancing transparency in elections that enable 'one person, one identity, one vote'. Before the implementation of the ID programme, Malawians primarily relied on driver's licences and passports as forms of identification. Few people held these, making it easy for people to accept the IDs. By only emphasising the programme's positives and the lack of questions and critical oversight from civil society organisations (CSOs), it was not difficult to convince Malawians that the national ID was essential.

As with the national ID, SIM card registration was promoted on safety grounds: SIM card registration would reduce mobile phone-based crime, especially mobile money fraud. However, the country's telecommunication regulator has confirmed that mobile money fraud has actually increased since implementing SIM card registration (Gausi 2022). Unlike the surveillance during the colonial and one-party dictatorship eras, today's digital world means governments are dealing with considerable amounts of data that even the government can lose control of to external players.

Further, the involvement of the donor community in the conceptualisation and implementation of the digital ID brings awkward questions: how much input did the Malawi government have? Has the government got the will to address the legal gaps? What about the ownership of the programme? These questions may be the subject of further inquiry. Still, it is known that since its implementation, the Malawi government has struggled to replace expired IDs and issue IDs to new applicants (Chitsulo 2021). This defeats the reasons given for the importance of the card. For example, the hiccups in issuing new IDs and replacing expired ones could affect people's right to vote. In their study, Kunyenje and Chigona (2019) established that one problem with policy implementation in most African countries is that policies are mostly initiated and funded by donors, while African governments, which may not fully appreciate the policies, have to implement them. This could explain why the Zambian and Ugandan governments had to have Huawei employees embedded in their systems.

3. Supply of surveillance technology

Internet interception

There is no evidence that the Malawi government has ever unlawfully intercepted internet traffic in ways that violate citizens' rights.

Mobile interception

Evidence shows that the Malawi government monitors citizens' private mobile phone communications and the state has used mobile phone communications as evidence in court. Any surveillance of mobile phone communication violates citizens' constitutional right to privacy. No statute allows the state to violate a citizen's rights in this way.

In 2010, the Malawi Communications Regulatory Authority (MACRA) procured a Consolidated ICT Regulatory Management System (CIRMS). According to MACRA, the system would help the regulator verify telecommunication companies' service quality, and revenue and tax levels (Chitsulo 2020). CIRMS equipment was purchased from US firm Agilis International in 2010 at US$6m (MWK6.2bn), and an additional US$20m (≈MWK21.1bn) had been paid to the company in subsequent contracts (Priezkalns 2022). Although MACRA said the equipment would be used for lawful interception, there are no details on which law provides for lawful interception. However, a court order stopped the implementation of the system after the High Court agreed with a petition by private citizens, arguing that despite MACRA's assurances, the technology could be used to eavesdrop on people's communication, contravening section 21 of the constitution, which guarantees privacy. The court ruling shows that MACRA procured CIRMS for lawful interception of communication, internet interception, and equipment identity registry (Kainja 2021).

The High Court ruling was overturned on appeal in 2017, paving the way for MACRA to implement CIRMS. However, the CIRMS is not in use because, as Chimjeka (2016) reported, the ruling came a year after MACRA had terminated its contract with CIRMS supplier Agilis International, preferring to give the contract to Global Voice Group, a South African company. Priezkalns (2022) recently reported that the country's anti-corruption body had halted attempts to procure a new CIRMS system through an unnamed supplier because of suspected offences under the country's procurement laws. It is unclear if this unnamed supplier is a South African company, as reported by Chimjeka. MACRA reportedly said that one motivation for replacing CIRMS with a new system was to surveil mobile money transactions. There are

8 million mobile money users in Malawi out of a total population of 19 million (*ibid.*).

Malawi also implemented mandatory SIM card registration in 2018, enabled under the Communications Act No. 34 of 2016. Compulsory registration means that all SIM cards must be registered on a central database and the customer requires their national ID to be verified when purchasing, replacing, or swapping a SIM (Sangala 2018). Although the policy is that SIMs can be registered using identification documents such as a passport or driver's licence, in practice only the national ID is allowed; some agents only accept the national biometric digital ID. SIM card registration is against the Human Rights Council's Special Rapporteur (2015) assertion that countries should refrain from identifying users as a condition for access to digital communications and online services and requiring SIM card registration for mobile users.

The MACRA has provided justification for why it is essential to have SIM card registration. However, the reasons involve policing functions. The police use the Criminal Procedure and Evidence Code (Act No. 36 of 1967)[8] to obtain search warrants and this law was made with a physical search of persons and property in mind. However, its use remains in the digital era to access phone call logs, and telecommunication service providers are requested to appear in court as expert witnesses to telecommunication activities.

The MACRA has provided the following justifications for SIM card registration (MACRA n.d.):

- To prevent SIM boxing. SIM boxing allows individuals to set up a device that can take more than one SIM card (a SIM box). This can be used to make international calls received as voice calls over the internet and, in turn, serve them to in-country mobile network subscribers as local traffic;
- To help recover stolen phones;
- To provide protection from hate texts, threats, and incitement of violence;
- To create a conducive environment for all phone users and 'instil discipline' in those that 'abuse phones'. (Note: the language used here is subjective and without clear definition of what 'discipline' and 'abuse phones' mean. It is itself open to abuse);

[8] **Criminal Procedure and Evidence Code (Act No. 36 of 1967)**.

- To help law enforcers track down criminals who use phones for illegal activities;
- To curb fraud and theft through the use of phones.

As noted by Kainja (2021), while CIRMS implementation faced resistance, the mandatory SIM card registration, implemented in June 2017, did not face notable resistance. There are two possible reasons for this: first, citizens may have been content with the justifications for its implementation; second, CSOs may have failed to see and articulate the potential of SIM card registration to violate human rights. Wanyama (2018) asserts that it is essential that governments carefully reconcile the state's interests, personal data, and privacy rights – which has not been the case in Malawi.

Social media monitoring

Security agents still use physical ways of monitoring people's communications, including on social media networks. For example, Kainja (2022) has documented that several people in the past two years have been arrested for WhatsApp conversations, allegedly for insulting the state president, although WhatsApp has end-to-end encryption. Likewise, in 2016, two members of parliament were charged with sedition for their WhatsApp conversation (Gwede 2016).

Smart city/safe city

Malawi does not have a smart city, or facial recognition CCTV for surveillance. However, MACRA's director general, Daud Suleman, recently told the Parliamentary Committee on Public Accounts that the telecommunications regulator had identified a piece of land to establish a smart city in Dowa District, about 50km from Malawi's capital, Lilongwe. Without disclosing the source of funding and supplier of the technologies, the local media cited the director general as having told the committee that 'this is a place where the digital economy and technologies will be built up. For all the technologies the country intends to have, there is a need for this smart city to coordinate all the works of technology' (Gausi 2023).

Biometric ID

In 2016, the Government of Malawi hired a French company specialising in scratch cards, SELP (SELP Group n.d.), to supply, deliver, instal, and commission training of National Registration Bureau (NRB) staff to implement a biometric digital ID programme (National Registration Bureau n.d.). The Government of Malawi paid US$1.27m (≈MWK1.4bn) for these services. SELP is also active in Senegal, Spain, France, the United Arab Emirates, and India.

The NRB programme is governed by the Malawi National Registration Act, No. 13 of 2010 (World Bank 2017).

The total cost of the national biometric ID could not be found. However, the Government of Malawi contributed 40 per cent of the biometric digital ID project costs. The remaining 60 per cent was funded by the UK's former Department for International Development (DFID), the European Union, Irish Aid, the Government of Norway, the United States Agency for International Development, and UNDP (Citizens Rights in Africa Initiative 2017). The national ID registration targets those aged 16 and over. As of May 2020, the biometric digital ID programme had registered 9.9 million Malawians, representing over 98 per cent of the target population (Chenjezi 2020).

The NRB uses Malawi's National Registration and Identification System, also used by several government agencies, replacing previously siloed ID programmes within a brief period (Malik 2020). According to the NRB, the system was introduced to address the lack of identification in Malawi associated with the lack of universal and compulsory registration in the national register. Since 2019, the Electoral Commission has used biometric digital IDs to register voters. The Malawi Revenue Authority uses it to record taxpayers; it is used to pay public and civil servants; and the immigration department uses it to verify applicants for travel documents. The finance ministry also uses the digital ID to consider households for inclusion in social protection programmes. Government ministries, departments, and agencies have integrated digital ID into financial development and inclusion programmes, farm subsidies, health care, and other social protection services (*ibid.*).

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Malawi kwacha (MWK)	US$
Internet interception			
No evidence of surveillance technology			
Mobile interception			
Agilis International (USA)	Consolidated ICT Regulatory Management System equipment at US$6m (2010, MACRA). A further US$20m paid in subsequent contracts	27bn	26m
Social media monitoring			
No evidence of surveillance technology			
Safe cities			
No evidence of surveillance technology			
Biometric ID			
SELP Group (France)	Supply, delivery, installation, and training of NRB staff to implement the biometric digital ID programme (2016, Government of Malawi)	1.4bn	1.3m
	Total	**28.4bn**	**27.3m**

Source Authors' own. Created using data from Priezkalns (2022).

4. Impacts – the chilling effect of surveillance

Through the National Registration and Identification System, the state has built a centralised identification registry containing the biometrically verified digital ID of 10 million registered Malawians. As the digital biometric ID is linked to the registration of the SIM card, which is mandatory, the government has the potential to surveil its citizens. This is more so than in other cases as most Malawians access the internet and social media platforms, use mobile phones, and have mobile money accounts and electronic banking services attached to their mobile phones. Most smart mobile phone users have their GPS switched on, which makes monitoring mobiles possible, potentially providing the state and telecommunication companies with real-time surveillance of citizens' communications, including calls, text messages, financial transactions, location, and interaction.

Thus, data centralisation paves the way for surveillance, and in the absence of data protection law, the state and non-state actors can abuse personal information. Privacy International (2019) says compulsory SIM card registration undermines citizens' ability to 'organise and associate with others; it infringes their rights to privacy and freedom of expression'. Registering a SIM card makes it 'easier for law enforcement authorities to track and monitor people; these laws threaten vulnerable groups and facilitate generalised surveillance'. A good example is the case of investigative journalist Gregory Gondwe (see section 6 of this report). Glenn Greenwald says:

> *It's really in the private realm where dissent, creativity and personal exploration lie. When we think we're being watched, we make behaviour choices that we believe other people want us to make… it's a natural human desire to avoid societal condemnation. That's why every state loves surveillance – it breeds a conformist population.*
> (Miles 2014)

Surveillance has a chilling effect on investigative journalists, dissidents, CSOs, and political opposition, among others.

5. Solutions – data protection and citizen action

There is a clear need for the Malawian government to take a human rights-based approach to implement legislation and ICT policies. In the current case, the country needed data protection legislation before embarking on personal data collection programmes such as the digital biometric ID. The government must ensure the enactment and implementation of data protection laws.

In addition, the country needs to have clear provisions for lawful communication interception. The Criminal Procedure and Evidence Code (Act No. 36 of 1967) must be amended to align with technological changes and follow good practices concerning human rights.

There is a shortage of research in this area. Malawian academics and researchers must undertake more research and provide intellectual leadership on digital and communication surveillance, which is not fully understood in the country. This has become evident in this research. There is now a digital rights coalition in the country lobbying for digital rights legislation – a move in the right direction because local CSOs have to date largely been absent on digital rights, despite being vibrant on other issues. Thus, CSOs must lobby and demand urgent enactment and implementation of data protection law.

The involvement of CSOs will also help with mapping surveillance technologies and their supply chains in Malawi. This will help researchers with critical information about surveillance programmes. Information currently is scant and not written from a human rights perspective. For example, much remains unknown about the Malawi data centre, in part because CSOs did not demand the information when the centre was being launched.

CIPESA (2023) noted that among key issues identified by digital rights activists at the Forum on Internet Freedom in Africa, held in Lusaka, Zambia in 2022, was that CSOs are often absent when legislation is being made, only to cry foul when flawed legislation is made. Thus, CSOs must be present and influential when legislation is being drafted. At best, CSOs must demand that they are both consulted and their proposal considered. This will ensure that there is human rights-based legislation. The evidence from this study is that there is too much at stake to leave lawmaking to the lawmakers only. That is why the 1967 Criminal Procedure and Evidence Code law is used in the digital age.

6. Surveillance stories – exercising power via interception

There have been several cases in Malawi that indicate the government's willingness to surveil its citizens. People have been arrested for their posts on Facebook and encrypted, closed WhatsApp groups. Those detained have one thing in common: they are accused of insulting influential people or powerful institutions. This shows that surveillance always involves exercising power – and it invariably serves the interests of vested power groups. Kainja (2022) captured the following cases:

Chidawawa Mainje was arrested on 1 May 2022 over a WhatsApp conversation in which Mainje allegedly insulted the state president. WhatsApp is an encrypted service, but it is believed that security agents used old-fashioned spies to monitor conversations and take screenshots. Screenshots have been used as evidence to prosecute people. Mainje was charged under section 86 of the Electronic Transactions and Cyber Security Act No. 33 of 2016, which prohibits cyber-harassment. So the president is said to have been harassed even if he was unaware of the conversation. Arresting someone for a discussion in a closed space shows the state's intent and capacity to use people to monitor conversations on social media.

Gregory Gondwe, a renowned investigative journalist in Malawi, was arrested in April 2022. According to Gondwe's account of events surrounding his arrest, the police had been tracking his phone conversations. The police were aware that Gondwe had been talking to his sister on a mobile phone and they knew his exact location. There is no known technology that the police use to track or eavesdrop on people's phone calls, but it could have been aided by his registered SIM card as SIM registration is mandatory in the country and linked to national digital ID. The police also confiscated his mobile phone, suggesting a clear surveillance case. A few weeks later, the Platform for Investigative Journalism website, where Gondwe's work is published, was hacked, which MISA Malawi (2022) believe was connected to Gondwe's arrest.

References

Chenjezi, T. (2020) '**Malawi Reaping Fruits of Digital Identification**', *The Nation*, 16 May (accessed 25 April 2023)

Chimjeka, R. (2016) '**MACRA to Terminate CIRMS Supplier Deal**', *The Nation*, 28 May (accessed 25 April 2023)

Chitsulo, L. (2021) '**NRB Explains National ID Renewal Delays**', *The Nation*, 9 October (accessed 25 April 2023)

Chitsulo, L. (2020) '**MACRA Speaks on CIRMS**', *The Nation*, 27 July (accessed 25 April 2023)

CIPESA (2023) ***Move Fast and Fix Policy: African Digital Rights Advocacy in an Era of Rapid Policy Change***, CIPESA blog, 2 January (accessed 25 April 2023)

Citizens Rights in Africa Initiative (2017) ***Public Statement: Mass Registration of Malawian Citizens for National Identity Cards***, 25 April (accessed 25 April 2023)

Gausi, W. (2023) '**MACRA Identifies Smart City Land**', *The Daily Times*, 9 January (accessed 25 April 2023)

Gausi, W. (2022) '**Malawians Duped K120 Million Monthly through E-Cash Transfers**', *The Daily Times*, 4 November (accessed 25 April 2023)

Gwede, W. (2016) '**Kabwila Arrested: Malawi Police May Arrest More "WhatsApp Coup Plotters"** ', *Nyasa Times*, 22 February (accessed 25 April 2023)

Hersey, F. (2020) '**How Malawi Established a Biometric National ID System at Breakneck Speed**', *Biometric Update*, 12 October (accessed 25 April 2023)

Huaxia (2022) '**Malawi Government, Huawei Commission National Data Center**', *Xinhua*, 22 July (accessed 15 May 2023)

Human Rights Council (2015) '**Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye**', Human Rights Council, Twenty-ninth Session, Agenda Item 3, 22 May (accessed 25 April 2023)

Human Rights Watch (1994) ***Human Rights Watch World Report 1994 – Malawi***, 1 January (accessed 25 April 2023)

Kainja, J. (2022) '**Arrests Mar Malawi's Digital Rights Landscape**', *Southern Africa Digital Rights 1* (accessed 25 April 2023)

Kainja, J. (2021) ***Mapping Digital Surveillance and Privacy Concerns in Malawi***, Media Policy and Democracy Project (accessed 25 April 2023)

Kunyenje, G. and Chigona, W. (2019) '**External Actors in Forming National ICT Policy in Malawi: A Cause for Concern in Low-Income Countries?**', *African Journal of Information Systems* 11.1: 2 (accessed 25 April 2023)

MACRA (n.d.) ***Frequently Asked Questions*** (accessed 25 April 2023)

Malik, T. (2020) ***Malawi's Journey Towards Transformation: Lessons from its National ID Project***, Washington DC: Center for Global Development (accessed 25 April 2023)

Miles, K. (2014) '**Glenn Greenwald on Why Privacy is Vital, Even if You "Have Nothing to Hide"** ', *HuffPost*, 20 June (accessed 25 April 2023)

MISA Malawi (2022) '**Hacking of Platform for Investigative Journalism Website Not a Mere Coincidence**', 15 April (accessed 25 April 2023)

Mpasu, S. (1995) *Political Prisoner 3/75 of Dr. H. Kamuzu Banda of Malawi*, rev. ed. (2014), Balaka: Montfort Media

National Registration Bureau (n.d.) ***Articles*** (accessed 26 April 2023)

Ó Drisceoil, M. (2022) '**Post-Colonial Theory**', *Law Society Gazette*, 8 June (accessed 26 April 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019) '**Huawei Technicians Helped African Governments Spy on Political Opponents**', *The Wall Street Journal*, 15 August (accessed 26 April 2023)

Priezkalns, E. (2022) '**Anti Corruption Bureau Halts Purchase of National Revenue Assurance System in Malawi**', *Comms Risk*, 3 August (accessed 26 April 2023)

Privacy International (2019) ***Timeline of SIM Card Registration Laws***, 11 June (accessed 26 April 2023)

RegTech Africa (2022) '**Malawi: Malawi Opens First National Data Centre in Blantyre**', RegTech Africa, 2 August (accessed 26 April 2023)

Sangala, T. (2018) '**MACRA Sets New SIM Card Registration Deadlines**', *The Times Group*, 4 June (accessed 26 April 2023)

SELP Group (n.d.) ***About Us*** (accessed 26 April 2023)

Swinhoe, D. (2022) '**Malawi Launches National Data Center: African Country Partners with Huawei for New Facility**', *DCD*, 28 July (accessed 26 April 2023)

UNDP (2022) ***Malawi's Foundational Legal Identity System Sets the Stage for a More Efficient and Responsible Digital Future***, *United Nations Development Programme, 20 May* (accessed 26 April 2023)

Wanyama, E. (2018) ***The Stampede for SIM Card Registration: A Major Question for Africa***, CIPESA blog, 18 April (accessed 26 April 2023)

World Bank (2017) ***The State of Identification Systems in Africa: Country Briefs***, Washington DC: World Bank (accessed 23 May 2023)

Mapping the supply of surveillance technologies to Africa

Zambia country report

Sam Phiri and Kiss Abraham

1. Introduction

This report documents the supply of surveillance technologies to Zambia. It is the most comprehensive analysis to date of the companies which supply these technologies to Zambia and of the countries the technologies come from. It also takes stock of the capacities, or actions, of local civil society to hold the Government of Zambia to account, and further examines whether the Zambian surveillance architecture raises concerns about human rights and whether it is illegal or has the potential to enhance state excesses while diminishing the ability of citizens to hold power to account.

2. Background

Zambia's civic space has over the years narrowed as the result of a combination of factors. These include government's political and legal actions on one side, and a weak civil society base on the other. In promoting a better understanding of the digital rights situation in Zambia, this report builds upon existing knowledge of the political and social dynamics in Zambia and seeks to ensure that citizens continue advocating for the expansion of local civic spaces (Phiri and Zorro 2020; Roberts 2021).

Political history

Zambia was a British protectorate from the 1800s until 1964 when it gained independence. Since then, its political and social systems have evolved exponentially. From 1964 to 1972, Zambia was a multi-party democracy with several political parties freely contending for governmental leadership. The post-independence government, to a large degree, observed and respected the rights of Zambian citizens.

However, in 1972, other political parties were proscribed, leaving the then governing party, the United National Independence Party (UNIP), under Kenneth Kaunda, as constitutionally the sole and only political party (Phiri 2006). Oppositional and dissenting voices were muted and proscribed, and the opposition went underground. Respect for human rights was suspended. The state of emergency, which had been declared on 12 March 1959 by the outgoing British authorities, was never lifted but re-enforced (Phiri 2006; Phiri 2019; Roberts, Hobson and Williams 2023). Human rights were violated at will and the status quo remained unchanged until the dramatic upheavals in the Soviet Union and Eastern Europe transcended into Africa and Zambia from 1989. Thereafter, Zambia reverted back to multi-party politics in 1990.

Since then, Zambia has remained a multi-party democracy of varying degrees and colours. However, the tradition of tight state control of citizens' lives, a lack of respect for oppositional views, controls of the media, public suspicion, political injustice, and police surveillance of citizen activities have continued, although to varying degrees.

With the emergence and popularisation of the internet and social media after 2000, the Zambian state sought new ways of controlling its citizens and for the governing class to continue retaining political power: enter the Chinese and their panoptic, surveillance smart city, facial recognition, and internet and social media interception technologies. In 2022, Zambia constructed a Chinese-built national surveillance command centre, with 36 communication towers across the country, e-government, and radio communication and video surveillance systems at a cost of K4.2bn (US$210m). The funds from China were to be paid to Chinese technology firm ZTE (Chisalu 2022). The project, largely based on the Chinese safe city model, is the foundation for a wide range of national security infrastructure in Zambia under the Ministry of Home Affairs and Internal Security.

It is disquieting that the safe city infrastructure, implemented with the support of communist China, betrays a pattern which seems to strengthen state control of the public through the authoritarian methods pervasive in mainland China. Further, the secretive nature of this undertaking and the potential assault on privacy that borders on illegalities mean that the data and methods of data gathering through this new infrastructure require close examination by civil society and the public. Unfortunately, civil society organisations (CSOs) are generally weak and there is an absence of, or potentially slow development of, local legal frameworks to protect citizens from the fast pace of technological developments in the surveillance realm under the control of the Zambian government (Chiumbu 2021).

Pre-digital surveillance

Zambia, now with a population of 18 million, has gone through five major political phases in the colonial and postcolonial period which influence contemporary Zambian life. It started with political control by one commercial firm, the British South Africa Company owned by Cecil John Rhodes. This was followed by direct colonial rule from London. Then, after independence in 1964, the country went through the eras of multi-party democracy, one-party rule, and then back to Western-style multi-party democracy with all its limitations (Phiri 2006). Since then, for the past 32 years, Zambia has had a relatively free and peaceful political environment, albeit with many economic and other social problems.

Throughout these periods, whether pre-independence or after, what has remained constant is the powerful position occupied by the executive wing of government over all other sectors, including parliament, the judiciary, the media, and civil society. This has especially been so since 1964. Zambia has essentially been governed by an authoritative, patrimonial, and almost imperial presidency, which in this instance is ably reinforced by a governing party and looms large across all sections of society. This is despite Zambia having had three different constitutions and two additional major constitutional amendments, in 1964, 1969, 1973, 1991, and 1996 respectively (ZIS 1991; Chinyere and Hamauswa 2016). However, the basics of the winner-takes-all one-party-rule paradigm have remained unchanged.

This history has impacted Zambia's human rights ethos and resulted in a weak participative culture in civic activities (Phiri and Zorro 2020).

The challenge from human rights defenders has been weak too. For example, an overview of Zambia by CIVICUS states that civil society's challenges include limited capacity for networking and high dependency on external resources (CIVICUS 2017). It therefore stands to reason that in addition to the more general challenges civil society is facing, the additional test of state surveillance and the threat of authoritarianism which comes with it promises to bring yet more challenges.

3. Supply of surveillance technology

As indicated above, China is one of the known countries supplying surveillance equipment to Zambia. Further, Privacy International, which monitors surveillance technology supply chains, has identified the entry of other forms of equipment to Zambia in addition to equipment intended for the safe city initiative.[1] This section documents five types of surveillance technologies used in Zambia.

Internet interception

The Zambian government, through its Financial Intelligence Centre (FIC), reportedly received services from the Israeli surveillance technology company Cyberbit in 2017 (Lungu 2021). The FIC was established in November 2010 by the Financial Intelligence Centre Act, No. 46 of 2010. It is the sole designated national agency legally mandated to receive, request, analyse, disseminate and disclose information about money laundering, terrorist financing, and other serious offences to competent authorities for investigations.

A revealing question was raised in parliament by Imanga Wamunyima MP who, in September 2021, asked the Minister of Technology and Science, Felix Mutati, whether the government was aware that citizens' phones, WhatsApp, Skype calls, and Short Message Service (SMS) were tapped by the FIC. Wamunyima also wanted to know whether such surveillance was an infringement of citizens' right to privacy as enshrined in the constitution and whether there were any measures taken to ensure that citizens' rights to privacy were protected (National Assembly of Zambia 2021). Minister Mutati responded that the government was not aware that any citizen's phone, WhatsApp, Skype calls, or SMS were tapped by the FIC, adding that the FIC operates within the confines of the law. But in contrast, in 2013, the then president, Michael Sata, told an opposition chief that as president, he was aware of what happened in the chief's bedroom. More specifically, President Sata said, '*A Jumbe lekani nimiuzeko* [Let me warn you (Chief) Jumbe], every day, 24 hours, I know what you say and I know what goes on in your bedroom… [asking that] why have I mentioned you and why have I not mentioned any other chief?' Further, Sata threatened to dethrone Chief Jumbe (*Daily Nation* 2013) if he did not stop opposing him.

[1] Privacy International internal document.

Mobile interception

There is recorded use of Circles surveillance technology in Zambia in 2018. Circles Technologies is a surveillance firm that reportedly exploits weaknesses in the global mobile phone system to surveil calls, texts, and the location of phones around the globe. Circles is affiliated with the Israeli NSO Group, which developed the oft-abused Pegasus spyware. Circles, whose products work without hacking the phone itself, says they sell their technologies only to states. Investigation of the extent of use of this technology and the cost is required to establish the full extent of its impact on laws and citizens. According to leaked documents, Circles customers can purchase systems that connect to local telecommunications companies' infrastructure, or can use another separate system called the 'Circles Cloud'. This interconnects with telecommunications companies around the world. 'We identified what appears to be a single Circles system in Zambia, operated by an unknown agency', states a report by University of Toronto's Citizen Lab (Marczak *et al*. 2020). However, it is yet to be established whether the Circles technology deployed is state-sponsored mobile phone surveillance of citizens.

Social media monitoring

In March 2020, the Zambian government warned social media and internet 'abusers' that it had installed equipment that enables the information and communication technology (ICT) regulator, ZICTA, and other law enforcement agencies such as the police, to track down suspects (Lwizi 2020). ZICTA Director-General Patrick Mutimushi later confirmed that there were indeed circumstances that permitted ZICTA to intercept people's communication:

> *I really think that some pieces of legislation that deal with privacy, don't* [allow us to] *tap into people's phones. We don't tap into people's messages but within the ICT Act, there is lawful interception and there is a whole section on how this can apply and we follow what the law says.* (Sakala 2020)

In 2022, the UK *Guardian* newspaper made startling revelations that Zambia's current government had received assistance to win general elections from a mining lobby firm called the CT Group. The revelations raised concerns about the implications of state capture arising from the control of government by business interests who are interested in the nation's mineral resources. The CT Group, which has deep ties to the UK Conservative party, helped the United Party for National Development (UPND) win elections in exchange for millions of pounds from a mining company, said the article. According to *The Guardian*, CT Group, co-owned by Lynton Crosby, a veteran Conservative strategist, planned secretive African campaigns on behalf of First Quantum Minerals in Zambia and the Democratic Republic of Congo. The files suggest CT Group also worked under the radar on a political influencing campaign in Zambia on behalf of mining interests while working on a campaign to oust the country's president (Waterson and Davies 2022).

Smart city/safe city

In 2022, the Zambian government, under the Chinese government-supported safe city project, completed the construction of a national surveillance command centre, 36 communication towers, and radio communication and video surveillance systems costing some US$210m (K42bn). These funds were obtained from China and paid to Chinese technology firm ZTE. The infrastructure, fashioned on the smart city and safe city initiatives, is implemented by Huawei and ZTE.

Smart cities rely heavily on collecting enormous amounts of citizen data. Seemingly, to augment the deployment of the safe city programme, there is a framework for developing state capacity to implement biometric systems through a smart Zambia project. This will integrate biometric data into the national registration citizenship system, the electoral system, and the health-care system. The system, known as the Integrated National Registration Information System (INRIS), will be implemented at an approximate cost of US$54.8m (K1bn) (National Assembly of Zambia 2021).

Stakeholders have already raised concern about the national SIM registration requirement, which compulsorily collects biometric data of users. Such a system is considered a way of silencing and targeting potential dissent (Chiumbu 2021). Additionally, citizens' free speech is threatened on platforms such as social media networks, with arrests for basic offences such as bringing the name of the president into disrepute (*Lusaka Times* 2022).

On 3 March 2023, the Road Transport and Safety Agency in a press statement informed the public that it was undertaking road transport enforcement through surveillance cameras. The function of the agency includes reducing traffic violations and road traffic accidents. The cameras are installed on major roads and in city centres and are connected to the safe city system. The statement further stated that the use of the cameras is part of the Smart Enforcement Initiative. This little known initiative was only announced through the statement, which included the information that the system was in the initial testing phase (*Zambian Observer* 2023).

Biometric ID

In 2022, it was clear that Zambia was taking strides towards the implementation of citizen biometric identification systems. Internal Security Minister Jack Mwiimbu told parliament that the country would invest K1.1bn in biometrics. According to Mwiimbu, this would ensure enhanced security systems through proper identification of citizens (Lusaka Times 2022).

The biometric system would be under the umbrella of INRIS, which would be the national and civil registration management system affecting all citizens. Thus, Zambians would have biometric-enabled national registration cards (NRCs), birth and death certificates, and passport and citizenship registrations (National Assembly of Zambia 2022a). This new venture would replace the current system in which Zambians get laminated paper NRCs which they use to access public and social services.

Mwiimbu averred that when the new system was in place, citizens could not easily change their identity, especially repeat offenders. He further claimed that the new system would contribute towards the promotion of good governance, it would strengthen and broaden tax administration and national health insurance, reduce the cost of voter registration, minimise wasteful expenditure by ministries, provinces, and other state spending agencies, and contribute towards the financial inclusion of the unbanked population.

Meanwhile, the Electoral Commission of Zambia (ECZ) has also implemented a robust biometric voter registration system based on Smartmatic equipment, supplied by the UK, at a cost of US$16m (K301m). The biometric voter registration and verification system primes a digital reconciliation process as well as ensuring fast processing of voters.

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Kwacha (K)	US$
Internet interception			
Cyberbit (Israel)	Cyber-surveillance	200m	10m
Mobile interception			
NSO Group (Israel)	Surveillance systems, including Pegasus spyware	Unknown	Unknown
Social media monitoring			
No evidence of surveillance technology			
Safe cities			
Huawei (China)	CCTVs and command & control centre	4,200m	210m
Biometric ID			
INRIS (Zambia)	Biometric identification	1,100m	55m
Smartmatic (UK)	Voter registration biometrics	320m	16m
	Total	**5,820m**	**291m**

Source: Authors' own. Created using data from *Zambian Observer* (2021), Marczak *et al*. (2018), National Assembly of Zambia (2022a, 2022b), *Lusaka Times* (2022).

4. Impacts

Chiumbu (2021) states that Chinese digital infrastructure, smart cities, and surveillance systems in Zambia exist without suitable legal architecture that would fence off human rights against ever-encroaching surveillance practices. In Chiumbu's view, smart cities are surveilled settlements where enormous amounts of citizen data are collected. Moreover, digital rights organisations have observed that CCTV cameras installed under the smart city initiative were mounted in the absence of guidelines for surveillance camera systems in public spaces. Such systems are expected to balance privacy rights, public safety, and security imperatives. It is noteworthy that although the Zambian cabinet approved in 2019 the introduction of a bill in parliament to control the use of CCTV in private and public premises, this bill has stalled and has yet to be gazetted (*ibid*.).

5. Solutions

The use of surveillance technologies to protect citizens against the most serious criminals is a legitimate function of government and public service. To balance this power of the state, citizens have a legitimate right to know what surveillance technologies are being imported and by whom, to protect their constitutional right to privacy. This report set out to increase knowledge in this regard.

A lack of existing research and limited government transparency about surveillance technologies procurement in Zambia serve as a limitation to this report. In many cases, there is evidence that surveillance is taking place but no public information on the contracts. Despite these limitations, this report succeeds in advancing our understanding by producing the most comprehensive record to date of which companies, from which countries, are supplying which technologies to conduct surveillance on Zambian citizens. Further research is necessary to adequately inform citizens about how public resources are being expended on this government function. Without adequate transparency it is impossible for civil society to hold elected officials and civil servants accountable as required in an open democracy. At this stage, actors who stand up for citizens' rights may already have been compromised or weakened, paving the way for the establishment of a pervasive surveillance architecture that needs to be checked.

Massive expenditure into surveillance technology should not be a priority for highly indebted, poor countries such as Zambia. At least Zambia's new government agrees. As the new Internal Security Minister Mwiimbu said in 2022, the safe city surveillance programme, worth US$210m, which was initiated by the previous Patriotic Front government, was too expensive and unnecessary. Had it not been for the new UPND, they would never have signed it. He said:

> *If at the time this contract was being considered for award and that the UPND government was the one in place, we would have not gone for such a contract considering the level of financial depression in this country and the levels of development… this was a missed priority by those who were in government at that time.*
> (National Assembly of Zambia 2022b)

However, the prying infrastructure is in place. Surveillance itself may already be in full swing while the question as to whom or what institution is checking on the surveillance system itself lingers.

Apart from seeking to unveil who supplies these technologies, our study wishes, in the first instance, to understand what these technologies are now used for in Zambia. Could the system be shut down? Moreover, what is the legal basis for safe surveillance activities, or the intended INRIS in Zambia? In other words, we seek to know who ‘bells’ the cat; or in plain language, who monitors the surveillers? Do CSOs have the countervailing capacity to hold government to account?

6. Surveillance stories

There are records of arrests of journalists following state surveillance on citizens such as the case of Thomas Zgambo and Clayson Hamasaka who were arrested after raids by the police and the Drug Enforcement Commission. The agency said they were looking for drugs and seditious material and accused the duo of publishing stories for the Zambian Watchdog – a Zambian online news blog (CPJ 2013). On 9 July 2013, they were charged with sedition. Hamasaka is now media director in the presidency at State House after the assumption to power of the UPND government which was in opposition at the time of his arrest.

References

Chinyere, P.R. and Hamauswa, S. (2016) 'A Critique of the Constitutional History of Zambia', in R. Mukwena and F. Sumaili (eds), *Zambia at Fifty Years*, Kabwe: Partridge Publishing

Chisalu, P. (2022) '**We Wouldn't Have Signed $210m Safe City Project – Mwiimbu**', *News Diggers*, 31 March (accessed 19 September 2022)

Chiumbu, S. (2021) ***Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia***, Johannesburg: Media Policy and Democracy Project (accessed 21 September 2022)

CIVICUS (2017) '**Zambia: Overview**', 1 January (accessed 24 August 2020)

CPJ (2013) '**Two Journalists Detained Without Charge in Zambia**', *Committee to Protect Journalists*, 9 July (accessed 26 May 2023)

Daily Nation (2013) 'Judi Online - I Know What You do in Your Bedroom'

Lungu, E. (2021) '**FIC in $2.5m Corruption Scandal**', *Daily Nation*, 18 September (accessed 29 April 2023)

Lusaka Times (2022) '**Government Begins Implementation of the Biometric Enabled National Registration Cards**', 15 March (accessed 28 April 2023)

Lwizi, G. (2020) '**Social Media Abuse Suspects Can Now Be Tracked Down – Police**', *Zambian Business Times*, 14 March (accessed 28 April 2023)

Marczak, B.; Scott-Railton, J.; McKune, S.; Razzak, B.A. and Deibert, R. (2018) ***Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries***, Citizen Lab Research Report 113, Toronto: University of Toronto (accessed 20 March 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

National Assembly of Zambia (2022a) '**Ministry of Home Affairs and Internal Security: On the Implementation of the Integrated National Registration Information System**', 10 March (accessed 19 September 2022)

National Assembly of Zambia (2022b) '**Question for Oral Answer, Street Cameras Safe City Project**', 30 March (accessed 19 September 2022)

National Assembly of Zambia (2021) '**Questions for Oral Answer, Tapped Citizens' Phones**', 30 September (accessed 28 April 2023)

Phiri, B.J. (2006) *A Political History of Zambia: From the Colonial Period to the 3rd Republic*, Trenton NJ: Africa World Press

Phiri, S. (2019) 'Youth Participation in Politics: The Case of Zambian University Students', in J. Kurebwa and O. Dodo (eds), *Participation of Young People in Governance Processes in Africa*, Hershey PA: IGI Global

Phiri, S. and Zorro (2020) ***Zambia Digital Rights Landscape Report***, Brighton: Institute of Development Studies, **DOI: 10.19088/IDS.2021.007** (accessed 24 August 2020)

Roberts, A.D.; Hobson, R.H. and Williams, G.J. (2023) '**Zambia**', in *Encyclopedia Brittanica*, Chicago IL: Britannica (accessed 19 March 2023)

Roberts, T. (ed.) (2021) ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries***, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.003** (accessed 26 May 2023)

Sakala, N. (2020) '**We Don't Pry into People's Phones but There's Lawful Interception – ZICTA**', *News Diggers*, 4 February (accessed 28 April 2023)

Waterson, J. and Davies, H. (2022) '**Tory-Linked Lobbying Firm Agreed to Help Swing DRC Election, Leak Suggests**', *The Guardian*, 3 November (accessed 7 March 2023)

Zambian Observer (2023) '**Enforcement Through Surveillance Cameras Still at Test Stage**', 3 March (accessed 26 May 2023)

Zambian Observer (2021) '**Supplier of $10m Cyber Surveillance System to FIC Disappears after Getting $2.5m**', 17 September (accessed 20 March 2023)

ZIS (1991) *Zambia in Brief*, Lusaka: Zambia Information Services

Mapping the supply of surveillance technologies to Africa

Supply-side report

Sebastian Klovig Skelton and Anand Sheombar

1. Introduction

The goal of this supply-side report is to map which companies from which countries are exporting surveillance technologies to African governments. The report does not set out to be comprehensive due to finite resources and the limitations of desk-based research into companies that are strategically secretive about their operations. The authors have paid particular attention to exports of surveillance technologies to the five countries featured in the accompanying country reports: Nigeria, Ghana, Morocco, Malawi, and Zambia. Exports to other African countries are mentioned where they help to illustrate wider patterns.

Despite the limitations of the research, our literature review suggests that this report is the most complete mapping to date of surveillance technology exports to the five target countries. Further research is needed to deepen analysis of exports to these five countries and to expand the mapping to other countries on the continent.

This report reviews prior research to provide an overview of what is already known, and it highlights research gaps and opportunities. By collating this information in one place, it is hoped that other researchers will be able to use it as a basis for further, more in-depth investigations.

Our initial review of published accounts of surveillance technology supply contracts revealed that the majority came from the world's largest arms exporters, that is, the countries with the most advanced military and digital technology sectors (Wezeman, Kuimova and Wezeman 2021). The USA, Russia, France, China, and Germany together accounted for 77 per cent of all arms exports between 2017 and 2021. The next largest arms-exporting governments were Italy, the UK, South Korea, Spain, and Israel.

Given the number of European Union (EU) countries in the top ten arms exporters, this report analyses their exports to African governments as a bloc, while highlighting some examples from each as a member state.

Otherwise, the only large arms-exporting country not properly investigated by this report is South Korea, due to time constraints. Israel was included because of the high-profile news stories and extensive research availability following the exposé of Israeli company NSO Group's supply of Pegasus mobile spyware that was employed in several of the focal countries in Africa.

To inform the content of this report, researchers used a variety of open-source databases, including news cuttings, open data on export licences published by governments, academic research into the spread of surveillance equipment, and information openly published by digital surveillance companies, such as press releases and brochures.

2. China

China is a major and growing supplier of digital surveillance technologies to Africa, particularly through the transfer of smart city and telecommunications infrastructure. Although precise figures are hard to verify, China competes head-to-head with the USA to dominate the multibillion-dollar global market for surveillance technologies that use artificial intelligence (AI) (Feldstein 2019). These technologies use AI to conduct keyword searches on big data sets created by intercepting the internet communications and mobile phone calls of all citizens. These technologies are often made available to African governments as part of multimillion-dollar soft-loan-assisted packages that include closed-circuit television cameras (CCTV) that have facial recognition and car number plate recognition capabilities. These surveillance packages, branded variously as 'Safe City' by the Chinese company Huawei, or as 'Smart City' by rival Chinese company ZTE, transmit these multiple streams of surveillance data to a central command and control 'data centre' where citizens can be monitored and tracked in public spaces and online. This mass surveillance system represents a substantive threat to citizens' constitutional rights to privacy, and freedom of association and expression (Gagliardone 2020; Woodhams 2020). These surveillance systems are already operational in whole or in part in Ghana, Zambia, and Malawi (see country reports elsewhere in this publication).

According to Steven Feldstein, technologies linked to Chinese companies are found in at least 63 countries worldwide, and Huawei alone is responsible for providing AI surveillance technology to at least 50 countries (Feldstein 2019: 2). He noted: 'Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment.'

The primary vector for the transfer of digital surveillance technology from Chinese firms to African governments is the 'Digital Silk Road' (DSR), which is the part of China's 'Belt and Road Initiative' (BRI) that focuses on improving information and communications technology infrastructure capabilities in other states. The DSR cuts across multiple areas of technology, including 5G, data centres, e-commerce, smart cities, smartphones, undersea fibre-optic cables, the 'internet of things' (IoT), AI, and financial technology (fintech). According to the Green Finance Development Centre, 147 countries globally had joined the BRI as of March 2022 after signing a memorandum of understanding (MoU) with China, including 43 countries from sub-Saharan Africa and 18 from the Middle East and North Africa (Nedopil 2023). This includes all the countries in the scope of this report.

China's involvement in Africa also predates the BRI and can be traced back to the government's 'go out policy', which was launched in 1999 with the aim of promoting the internationalisation of Chinese companies. Participation in the BRI does not automatically mean a country is also involved in the DSR, although it does mean there is potential for them to be.

The supply of large digital systems from China is often enabled by soft loans from China. According to the Chinese Loans to Africa (CLA) database – an interactive data project developed by Boston University Global Development Policy Center that tracks loan commitments from Chinese entities to African governments and state-owned enterprises – there have been a total of 1,188 loans amounting to US$159.9bn since 2000 (Boston University Global Development Policy Center 2022). It is impossible to tell which are specifically DSR-related.

The CLA database shows that, of the total, 148 loans collectively worth US$13.5bn were related to information and communication technologies. The database only contains information from publicly available sources. Many of these loans are for IT infrastructure projects, rather than direct surveillance capabilities, although many of the technologies being transferred could potentially be repurposed for surveillance. There are also no IT loans to Morocco mentioned in the database.

Significant loans include:

- **Ghana:** US$150m and US$199m respectively for Phase I and Phase II of the Integrated National Security Communications Enhancement Network (ALPHA) Project, a nationwide safe city project in Ghana. The Ghanian government signed an MoU with China's Ministry of National Security, Huawei, and China Machinery Engineering Corporation (CMEC) (Ofori-Atta and Kan-Dapaah 2019). In November 2013, Ghana received a US$129m loan from the Export–Import Bank of China (China Exim Bank) for the extension of dedicated security information infrastructure, including an 'intelligent video surveillance' component, implemented by Huawei and ZTE (AidData n.d.).
- **Nigeria:** US$200m for a Nigerian Communications Satellite (NIGCOMSAT) in 2006; a 'replacement project' for the satellite worth US$20m in 2010; a Public Security Communication System Project worth US$400m in 2010; and two phases of a National ICT Infrastructure Backbone project in 2013 and again in 2018, respectively worth US$100m and US$334m (Abdulaziz 2023).
- **Zambia:** Eight different IT-related loans worth US$958m, including for fibre-optic cables, a public security network, communication towers,

and a Smart Zambia National ICT Development Project. Huawei (2022) noted on its website that it is 'the primary project supplier'.

- **Malawi:** There is one IT loan for a National Fibre Backbone in 2016 worth US$23m.

These loans come from a variety of sources within China, including 'policy banks' (which are the biggest lenders at US$125bn) and commercial banks (such as the Industrial and Commercial Bank of China (ICBC), China Exim Bank, and China Minsheng Bank), various Chinese government entities, the China International Development Cooperation Agency (CIDCA), and individual 'contractors' such as Huawei and ZTE.

- Huawei is active in Ghana, Nigeria, Zambia, Malawi, and Morocco, and is most associated with the deployment of safe/smart city technologies (Huawei 2020, 2021, 2022; Burkitt-Gray 2022).
- In 2015, Huawei launched a US$1.5bn fund to support the development of smart cities across Africa (Takouleu 2018), which has been used to support projects in Ghana (such as ALPHA), Nigeria, Rwanda, South Africa, and Kenya, and has been extensively involved in setting up digital infrastructure in Zambia (*China Daily* 2022), where *The Wall Street Journal* reported it helped authorities intercept encrypted communications and use mobile data to track political opponents (Parkinson, Bariyo and Chin 2019a). Huawei emphatically denied the allegations (Parkinson, Bariyo and Chin 2019b).
- ZTE, on the other hand, has subsidiaries in Ghana, Nigeria, and Zambia (ZTE 2021). Major ZTE contracts include a US$82m construction project in 2002 for a rural telephone service in Nigeria and a US$95m follow-up for the second phase in 2005.

Table 2.1 Chinese companies supplying digital surveillance technologies

Supplier country: China

Technology	Supplier	Government	Examples
Mobile interception	ZTE	Zambia	Via subsidiaries in Ghana, Nigeria, and Zambia – and also Côte d'Ivoire. Construction of a rural telephone service in Nigeria.
Internet interception			
Social media monitoring			
Smart cities	Huawei	Ghana, Malawi, Morocco, Nigeria, and Zambia. Also Côte d'Ivoire.	Huawei launched a US$1.5bn fund to support the development of smart cities across Africa; e.g. setting up digital infrastructure in Zambia where *The Wall Street Journal* reported it helped authorities intercept encrypted communications and use mobile data to track political opponents.
Biometric ID	Huawei and ZTE	Ghana	Ghana received a US$129m loan from China Exim Bank for extension of dedicated information infrastructure, including implementation of intelligent video surveillance by Huawei and ZTE.

Source: Authors' own. Created using data from Takouleu (2018); Ofori-Atta and Kan-Dapaah (2019); Parkinson *et al*. (2019a,b); Huawei (2020, 2021, 2022); ZTE (2021); Burkitt-Gray (2022); Abdulaziz (2023).

3. European Union

In the EU, exporting companies are expected to register sales of 'dual-use' equipment and are required to conduct human rights assessment to ensure that equipment they are exporting is not used to violate citizens' rights. Key European agencies are involved in the funding and coordination of the transfer of surveillance equipment (and associated training to use it), including the European Commission (EC), the European Border and Coast Guard Agency (Frontex), the European Union Agency for Law Enforcement Training (CEPOL), and the European External Action Service (EEAS). Two of these institutions – Frontex and the EEAS – are currently being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries. A recent investigation into the EC by the European Ombudsman found that it had failed to ensure the protection of human rights in the transfer of surveillance technology to African governments (European Ombudsman n.d.).

Like China, the EU also uses soft loans to transfer technologies to the continent. This includes the Global Gateway Investment Package, which is focused on accelerating digital transformation through investments and is valued at €150bn (US$164bn) (EC n.d.b). It specifically aims to facilitate projects in fibre-optic cables, cloud computing, and data infrastructure.

The EU also controls the export, transit, brokering, and technical assistance of dual-use items. According to a September 2022 report prepared by the EC with input from member states in the Dual Use Coordination Group (DUCG), while it remains difficult to 'obtain reliable information on overall dual-use exports (including non-listed dual-use items) as there is no official category of "dual-use items" in official economic/trade statistics', the EC and member states collect some information that makes dual-use export estimations possible (EC 2022: 8). While the report – which includes data collected by member states from regulators and statistics for export declarations to EU customs – only provides aggregated export control data for 2020, it notes that 97 licences were granted for telecommunications and information security, 21 for computers, and 234 for electronics generally.

However, under the EU's dual-use export regulation, data about transfers are only offered to the EU by member states on a voluntary basis. On 24 January 2023, the EC's Directorate-General for Trade launched a consultation on new requirements for the collection and preparation of dual-use export data so the EU can more accurately report what is happening (EC n.d.a). Each member state's export licence authorities are subject to freedom of information legislation, meaning public access requests are an avenue for further investigation (EC 2022).

Border surveillance technologies

The EU has several funding mechanisms dedicated to border control and surveillance. Europe is engaged in a process of externalising[1] and digitalising its border control and surveillance, in part through programmes designed to provide technical and financial support to non-EU countries on migration issues. Such initiatives include the AENEAS Programme (EuropeAid 2008), the B7-667 budget line (EC 2002) and, most notably, the EU Trust Fund for Africa (EUTFA), which was established in 2015 to 'address the root causes of instability, forced displacement and irregular migration' (EUTF 2023).

A funding overview by NGO Statewatch highlights some of the projects funded via these mechanisms, breaking it down into three phrases: creating border infrastructure between 2001 and 2010; improving integration between 2011 and 2018; and the current phase of 'enhancing security', which began in 2018 and runs to the present (Statewatch 2019).

Significant EUTFA projects include:

- A €44m project titled 'Support for Integrated Border and Migration Management in Morocco' in 2018, which included the acquisition of equipment for the surveillance of sea and land borders, as well as improving use of data and cooperation with EU authorities. In 2019, the EC committed a further €101.7m to Morocco's border management, noting in a press release that it would include the use of 'new technologies' as well as 'analysis and collection of data on migration' (EC 2019).
- A €65m 'Border Management Programme for the Maghreb Region' which involves the transfer of equipment and training to Morocco between 2018 and 2024.
- A €15m project titled 'Dismantling the Criminal Networks Operating in North Africa and involved in Migrant Smuggling and Human Trafficking' to support 'the specialization of law enforcement agencies by establishing solid knowledge and skills on the use of special investigation techniques, including criminal intelligence analysis, forensics and digital forensics' (EUTF 2017).
- A €5m project for 'Strengthening Border Security in Ghana' designed to enhance the border checking and surveillance capacities of the Ghana Immigration Service (GIS).

[1] Border externalisation refers to the practice of outsourcing the responsibility for preventing migration to third countries and private entities.

Other avenues through which surveillance technologies are transferred to African governments include: the EU Agency for Law Enforcement Training (CEPOL), which facilitates training sessions for law enforcement officials throughout northern Africa, including Morocco (CEPOL 2020); and EU coastguard agency Frontex, which runs the Africa-Frontex Intelligence Community (AFIC) to conduct 'training and capacity building activities to develop national and regional strategies to fight cross-border crime and setting up integrated border management systems, as well as improving the collection, sharing and analysis of relevant data' in African countries, including Morocco, Ghana, and Nigeria (Frontex 2017).

A 2016 Joint AFIC report noted that the project has 'reached an enhanced level of maturity', which 'is mostly evident in the Community's capacity to generate analysis and knowledge, build trust between its participating partners, expand geographically and extend its product portfolio' (Frontex 2016: 8).

For Ghana specifically, it noted 'the authorities are addressing document and identity fraud by introducing biometric passports, birth and death certificates, and more effective arrest and prosecution of offenders' (*ibid*.: 30).

As part of a project launched under AFIC in 2017, Frontex is also helping Ghana and Nigeria set up Risk Analysis Cells, to 'collect and analyse strategic data on cross-border crime such as illegal border crossings, document fraud and trafficking in human beings' (Riehle 2019).

Member states: France, Germany, and Italy

Aside from surveillance transfers at the EU level, many EU member states have their own relationships and surveillance export arrangements with the five African countries.

France

France has a long colonial history of presence on the African continent and has maintained economic and political ties, including through military bases, control of monetary systems, and close trading relationships following a 'Françafrique' doctrine (Chrisafis 2023). Although French military presence may be reduced, increasing military training and equipment may signal a repacking of that doctrine (France24 2023). In the slipstream of French government politics come French surveillance technology companies that have hired former French officials to facilitate business in Francophone Africa (Braun 2022).

French technology transfers to Africa tend to be focused around signal intelligence technologies capable of intercepting mobile phone and internet data.

Founded in 2002, Altrnativ claims to have sold surveillance technologies to the governments of Benin, Chad, Cameroon, Comoros, Gabon, and the Republic of the Congo. One of the products offered by Altrnativ is their tailor-made search engine Targets. According to the company, this search service can retrieve publicly available data to analyse and identify connections between places, people, and organisations and thus provide information on people and their whereabouts.

Another French cyber-surveillance firm, Nexa Technologies, stated it had received permission from the French government and export licences for selling its surveillance software CEREBRO to repressive regimes such as the Egyptian government (Canet *et al*. 2021). CEREBRO provides real-time surveillance of the mobile phones of targeted citizens and the collection of personal data and metadata (Mada Masr 2021).

Germany

Germany is Europe's largest arms exporter and has at least 41 firms active in the high-tech surveillance industry (Privacy International 2016).

A company that has now shut operations and filed for bankruptcy was FinFisher. This surveillance technology company had a track record of selling to authoritarian regimes monitoring human rights defenders and journalists. Citizen Lab found evidence for the presence of FinFisher Command and Control servers in South Africa (Singh 2015). The company sold FinSpy, a 'surveillance software suite, capable of intercepting communications, accessing private data, and recording audio and video, from the computer or mobile devices it is silently installed on' (Amnesty International 2020). After years of public and legal pressure by non-governmental organisations (NGOs), the company was dissolved. It is worth mentioning that all staff moved to other technology firms and remain active in security or surveillance services (AccessNow 2022). The use of FinFisher's technology by state authorities has been documented in Nigeria and Morocco (Marczak *et al*. 2015).

Another German surveillance technology company is the Munich-headquartered Trovicor, which offers monitoring centres to government and law enforcement clients worldwide to capture, monitor, analyse, and store data from various networks (mobile and internet). The company, formerly part of Nokia Siemens Networks (NSN), delivered communications surveillance equipment to the Ethiopian government (Privacy International 2015a).

Italy

Italy has a large defence and security sector. In addition, the surveillance technology sector is growing, with over 20 active companies (Privacy International 2016). Historically, the Italian surveillance industry was fostered due to domestic demand for monitoring organised crime. The Italian Ministry of Economic Development (MISE), under Legislative Decree No. 221 of 2018 is tasked with granting export licences for dual-use technologies (TIMEP 2019).

Four companies seem often to be present in deals: AREA, RCS, SIO, and INNOVA, while others have resurfaced after scandals that involved them, such as Hacking Team, now active under the name of Memento Labs (Coluccini 2023). For example, the Moroccan intelligence services made use of Hacking Team's spyware Remote Control System and spent more than €3m on Hacking Team equipment (Privacy International 2015b). Other customers of this spyware were agencies of African governments of Egypt, Ethiopia, Morocco, Nigeria, and Sudan (Marczak *et al.* 2014).

Table 3.1 EU and EU member state companies supplying digital surveillance technologies

Supplier country: EU and member states France (F), Germany (DE), and Italy (IT)

EU institutions, Frontex, and the EEAS are being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries

Technology	Supplier	Government	Examples
Mobile interception			
	Altrnativ (F)	Côte d'Ivoire	Deal worth €13.8m for radio surveillance equipment and intelligence training
	Nexa Technologies (F)	Egypt	Surveillance software CEREBRO, which provides real-time surveillance of the mobile phones of targeted citizens and the collection of personal data and metadata
	Finfisher (DE)	South Africa	FinFisher Command and Control servers in South Africa
	Hacking Team, now active under the name Memento Labs (IT)	Morocco	Moroccan intelligence services used spyware Remote Control System and spent more than €3m on Hacking Team equipment
Internet interception			
	Trovicor (DE)	Ethiopia	Communications surveillance equipment to the Ethiopian government
Social media monitoring			
	Altrnativ (F)	Multiple countries	Tailor-made search engine Targets, to retrieve publicly available data to analyse and identify connections between places, people, and organisations
Smart cities			
Biometric ID	EUTFA (EU)	Ghana	€5m project for 'Strengthening border security in Ghana' to enhance border checking and surveillance capacities of the Ghana Immigration Service
	EUTFA (EU)	Morocco	A €44m 'Support for integrated border and migration management in Morocco' project in 2018, including the acquisition of surveillance equipment for sea and land borders, as well as improving data use and cooperation with EU authorities

Source: Authors' own. Created using data from Marczak *et al*. (2014); Privacy International (2015a,b); Singh (2015); EUTF (2017); EC (2019); Canet *et al*. (2021); Mada Masr (2021); Braun (2022); Coluccini (2023); EUTF (2023).

4. Israel

In 2022, a consortium of journalists and civil society organisations revealed that Israeli Pegasus spyware was used to target some 50,000 journalists, human rights defenders, and foreign heads of state around the world (Amnesty International 2022). For Israel, the export of military-grade surveillance tools acts as a form of 'spyware diplomacy', providing a diplomatic bargaining chip for the country's political goals (Bergman and Mazzetti 2022; Dadoo 2022; Robinson 2022). The ongoing occupation of Palestine provides 'an open-air laboratory for Israel to test techniques of espionage and surveillance before selling them to repressive regimes around the world', states Dr Shir Hever, author of *The Privatisation of Israeli Security* (Shtaya 2022). These field-tested products are monetised via exports. The exported products and services cover a broad range from spyware and digital tools for surveillance to espionage, psychological operations, and disinformation (Loewenstein 2019, 2023).

In terms of its relationship to the African continent, prominent suppliers include Briefcam, whose 'video synopsis technology' has been incorporated into smart city surveillance networks in suburban areas throughout South Africa (Kwet 2019; Murray 2022); and Circles, a mobile interception firm, which is 'affiliated with NSO Group, which develops the often-abused Pegasus spyware' (Marczak *et al*. 2020: 1), and which is active in Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria, Zambia, and Zimbabwe.

NSO Group itself is active in 45 countries worldwide, including Algeria, Egypt, Côte d'Ivoire, Kenya, Morocco, Rwanda, South Africa, Togo, Uganda, and Zambia (Mwesigwa 2019); while Team Jorge helped hack into the phones of opposition leaders during the 2015 Nigerian election.

The Israeli surveillance industry sees growth potential in the African market: 'African countries that have already bought Israeli security equipment represent a potential for further deals, such as the need to upgrade systems' (Salman 2021). 'The commercial aspect is an important driver for Israel's arms sales. The Israeli arms industry is extremely export dependent, and maintaining the industry is considered vital for both Israel's economy and security' interests, Wezeman (2011: 14) argues.

Dadoo (2022) argues that, 'For power-hungry African leaders looking to Israel as a blueprint for surveilling their own citizens, these technologies are ideal. They are relatively cheap, easily distributed and can be deployed with little consequences to their regimes.'

The country's 'military-innovation ecosystem' creates a continuous pipeline of surveillance tools which, according to Abdelnour (2023: 334), consists of a 'constellation of industries, infrastructures and organisations involved' in (digital) surveillance and 'weapons development, testing and sales'. This includes 'military and state agencies, tech start-ups and private companies, universities and research institutes, as well as banks and venture financing, including public research funding agencies for "dual-use" technologies' (*ibid*.).

In this ecosystem, the distinction between private and public space is blurred (Cook 2019), with former military personnel from Israel's cyber-surveillance units working for weapons companies and digital surveillance technology start-ups (Abdelnour 2023). US-based venture capital funds and technology firms are some of the biggest investors of Israeli surveillance firms (Kortum and Lerner 2000).

Table 4.1 Israeli companies supplying digital surveillance technologies

Supplier country: Israel			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception			
	Circles	Morocco, Nigeria, and Zambia Also Botswana, Equatorial Guinea, Kenya, and Zimbabwe	
	NSO Group	Morocco, Nigeria, and Zambia Also Côte d'Ivoire, Egypt, Kenya, Rwanda, South Africa, Togo, and Uganda	Developers of the Pegasus spyware
	Team Jorge	Nigeria	Hacked into the phones of opposition leaders during the 2015 Nigerian election
Internet interception			
Social media monitoring			
Smart cities			
	Briefcam	South Africa	'Video synopsis technology' incorporated in smart city surveillance networks in suburban areas.
Biometric ID			

Source: Authors' own. Created using data from Kwet (2019); Mwesigwa (2019); Marczak *et al*. (2020); Murray (2022).

5. Russia

Like China, the EU, and the US, Russia is attempting to project its own influence over the African continent. Since 2015, for example, Russia has signed military-technical agreements with 21 African countries (Hedenskog 2018), including Nigeria (Ojoye 2021), Zambia, and Ghana, which allow for technology transfers. There is, however, no evidence of which surveillance technologies might be included in such agreements.

In June 2021, Russian state defence company Rosoboronexport – which sells a range of biometric identification technologies (Rosoboronexport 2021a) – announced it had signed contracts worth US$1.7bn with 17 sub-Saharan African countries (Rosoboronexport 2021b). While the press release does not mention which countries, the 'partner countries' section of its website notes that the company is known to have been cooperating with Nigeria since 1960 (Rosoboronexport 2023).

The main body in Russia responsible for export control over dual-use items is the Russian Federal Service for Technical and Export Controls (FSTEC), but it publishes no information on export licences granted. The Federal Service for Military-Technical Cooperation (FSVTS) also exists under the Ministry of Defence to manage military-technical cooperation with foreign states. While it does not publish information about technology exports or transfers, the director of the FSVTS noted in September 2018 that sub-Saharan African states have ordered US$3bn of military equipment from Russia (Interfax 2019).

According to the Stockholm International Peace Research Institute (Wezeman *et al*. 2021), Russia has supplied arms to 18 countries in sub-Saharan Africa over the past 10 years, including Ghana, Nigeria, and Zambia, although it is unclear whether any surveillance technologies were included in this.

However, World Bank data from 2020 shows that Russia's overall exports to sub-Saharan Africa are dwarfed by those from Germany, India, the US, and especially China (which accounted for 20.5 per cent of all imports into the region) (WITS 2019). In February 2023, the UK newspaper *Financial Times*, in a series on Russian involvement in the continent, also reported that 'Russia lacks the economic muscle to compete head-to-head with China, the US or EU when it comes to trade and investment in Africa' (Wilson 2023). Writing in October 2019 for the Carnegie Endowment for International Peace, Paul Stronski (2019) also noted that 'the modest size of Russia's technology sector and lack of investment resources hardly make it an attractive partner for African countries seeking to modernize or build new infrastructure'.

Despite this, a number of Russian companies are prominent in the surveillance technology space, particularly around Systems for Operative Investigative Activities (SORM), which refers to hardware and software that can intercept and monitor internet and telecommunications network traffic (Whittaker 2019). It is essentially the Russian equivalent of 'lawful interception' technology and was initially developed by the KGB in the mid-1980s during a project to intercept landline communications. SORM systems are now capable of targeted surveillance of specific individuals across the whole spectrum of internet and telephone communications technologies (see Box 5.1).

Box 5.1 What is a lawful interception technology?

The term 'lawful interception technologies' refers to the functionality that internet service providers and phone companies are required to build into their systems to allow surveillance that a court has warranted in accordance with legislation. A society may wish state agencies to conduct surveillance of the most serious criminals to prevent atrocities. Legislation can stipulate narrow circumstances in which this may take place, with democratic oversight and protection for the privacy of other citizens[1]. OpenDemocracy noted in 2012 that three SORM systems are currently in use which are capable of targeted surveillance of specific individuals across the whole spectrum of internet and telephone communications technologies (Soldatov and Borogan 2012).

However, there is very little open-source or public domain information about Russian SORM suppliers' involvement in supplying digital surveillance technologies to the five African countries that are part of this study: Nigeria, Ghana, Morocco, Malawi, and Zambia.

The chief commercial officer of Speech Technology Centre (STC) – a provider of facial, voice, and biometric identification systems – noted in 2016 that, 'Attention to biometric technologies on the African continent is raising rapidly', adding that 'South Africa and Nigeria are the key revenue generating countries in the African biometrics market' (Mayhew 2016).

[1] For more information on lawful interception, surveillance law, and how it can be subverted for unlawful interception, see Roberts *et al.* (2021).

Table 5.1 Russian companies supplying digital surveillance technologies

Supplier country: Russia			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception			
Internet interception			
Social media monitoring			
Smart cities			
Biometric ID	Rosoboronexport	17 sub-Saharan African countries, including Nigeria	Signed contracts worth US$1.7bn

Source: Authors' own. Created using data from Hedenskog (2018); Ojoye (2021); Rosoboronexport (2021b).

6. United Kingdom

The UK has a long and brutal colonial history in Africa going back centuries. Some colonial surveillance systems, including those operated by the Special Branch, were adopted by post-independence governments and continue in modernised forms today. The UK government has also continued to have close political and economic ties with many of those governments, which has sometimes involved the transfer of surveillance equipment and training.

The easiest way to find data on these technology transfers is to look at the data regularly published by the Department for International Trade and the Export Control Joint Unit on the types of dual-use technologies being transferred overseas. This includes both quarterly and annual licensing statistics. This data can also be used to generate reports on, for example, specific licence types or export destinations, via a government portal.

By searching for specific 'control entries' related to the technologies being investigated by this project, we can see that the UK government greenlit the transfer of:

- 16 licences worth £669,880 to Malawi
- 79 licences worth £3,685,770 to Zambia
- 91 export licences worth £5,279,676 to Ghana
- 227 licences worth £49,176,911 to Morocco
- 572 licences worth £66,061,548 to Nigeria (DIT 2021).

The data here covers exports between 1 January 2013 and 1 February 2023, which were the furthest and most recent dates the function would allow. The licences granted specifically allow for the transfer of drones, camera equipment (6A003), telecommunications interception software and equipment, internet protocol (IP) network surveillance, various forms of cryptography, and information security technologies.

In terms of overall exports, however, Africa generally represents only a fraction of the total. The most recent UK defence and security exports data (GOV.UK n.d.b), for example, shows that between 2012 and 2021, Africa as a region accounted for just 1 per cent of UK defence exports (GOV.UK n.d.a). Technology transfers are included in this data.

Comparing this to data collected via freedom of information (FOI) by Campaign Against the Arms Trade (CAAT n.d.), the total value of dual-use goods (including those not specifically related to digital surveillance technologies) exported to each country since 2008 are as follows:

- Malawi, £789,000
- Zambia, £4.7m
- Ghana, £36m
- Morocco, £115m
- Nigeria, £348m

However, while the UK government openly publishes more dual-use export licensing data than many other governments, there are still severe limitations in the level of detail and transparency the data provides. For example, it does not show whether the goods were actually exported, only that the licence holder has been permitted to export them; and it does not disclose specific suppliers or technologies. More information can be gathered about suppliers through FOI requests.

An FOI from Motherboard in 2016, for example, found that companies involved in transferring surveillance technology include the billion-dollar arms exporter BAE Systems, as well as Pro-Solve International, ComsTrac, CellXion, Cobham, and Domo Tactical Communications (DTC) (Cox 2016). Motherboard noted that 33 licences were explicitly marked as being for IMSI catchers (see Box 6.1). While all these firms are UK-based, DTC is headquartered in the US. According to a joint investigation by BBC Arabic and the Scandinavian newspaper *Dagbladet* from 2017, BAE Systems has sold a mobile and internet interception system called Evident (developed by a firm called ETI that BAE purchased in 2011) to authorities in Morocco, as well as Saudi Arabia, the UAE, Qatar, Oman, and Algeria (BBC 2017). An anonymous former employee of ETI told the BBC:

> [With Evident], *you'd be able to intercept any internet traffic. If you wanted to do a whole country, you could. You could pin-point people's location based on cellular data. You could follow people around. They were quite far ahead with voice recognition. They were capable of decrypting stuff as well.*
> (BBC 2017)

Box 6.1 Explainer: What is an IMSI catcher?

An IMSI catcher is a surveillance technology that allows users to hack into mobile phone traffic (calls, text messages, instant messaging, and anything sent from your mobile phone). The hacker catches this data by imitating a mobile phone cell tower to intercept the data. The hacker can catch mobile data without the knowledge of the caller and without needing access to the handset. Note that the IMSI equipment is sometimes called a Stingray and the type of hack is often referred to as a man-in-the-middle attack. IMSI stands for International Mobile Subscriber Identity: an identifier unique to each mobile phone that is used to identify it to cell towers. Any single phone is constantly sending out signals to find the nearest cell tower to optimise signal strength and identify itself – and this provides the opportunity for the hack to imitate a cell tower and catch the phone's data.

A follow-up report from Motherboard in 2018 noted that the UK government has since been reluctant to release information about suppliers, claiming the information needs to be protected for 'commercial interests' (Cox 2018).

Table 6.1 UK companies supplying digital surveillance technologies

Supplier country: UK			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception **Internet interception**	ETI (purchased by BAE)	Morocco, also Algeria, Qatar, Oman, Saudi Arabia, and the UAE	Mobile and internet interception system called Evident
Social media monitoring			
Smart cities			
Biometric ID		Ghana and Nigeria, also Côte d'Ivoire	Border and coastal surveillance

Source: Authors' own. Created using data from BBC (2017).

7. United States of America

There are 122 surveillance companies headquartered in the US. Due to the vast apparatus of US secret service, domestic intelligence, and security agencies, a large domestic market for surveillance technology fosters an ecosystem of surveillance companies (Privacy International 2016). US companies supply AI-related surveillance technologies to at least 32 countries worldwide, the most significant being IBM, Palantir, Clearview AI, Clarifai, Intel, and Cisco (Feldstein 2019; Peterson and Hoffman 2022). According to Feldstein (2019), the most significant US exporters worldwide are IBM (11 countries), Palantir (nine countries), and Cisco (six countries), but they have been eclipsed in Africa by China's Huawei and ZTE (see China section of this report). In the safe city market for urban surveillance systems, US company Honeywell has advanced projects in Bangaluru, India, and Cairo, Egypt, but it is again China's Huawei and ZTE who look like dominating the African market with large projects in Ghana, Malawi, and Zambia (see those country reports in this publication).

Although not related to governmental use of data collection or surveillance, the United Nations (UN) World Food Programme (WFP) agreement with Palantir for biometric data collection may affect migrants and refugees in Africa. 'Data collection is not an apolitical exercise, especially when powerful global North actors collect information on vulnerable populations with no regulated methods of oversights and accountability', states UN special rapporteur on racism, racial discrimination, xenophobia, and related intolerance Professor Tendayi Achium (Klovig Skelton 2020). International aid funds are used to increase the digital surveillance of migrants and refugees.

US companies are also active in social media surveillance. Dataminr, for example, specialises in advanced real-time social media monitoring and provides the UN with its First Alert service to alert first responders on breaking news (Dataminr 2023). The company has also helped US law enforcement agencies track protests (Levin 2016) and public authorities in South Africa to monitor student demonstrations in Cape Town (Dataminr 2016). Dataminr's customers in Africa also include governmental agencies in Kenya (used during the 2017 elections) and Nigeria (Thorpe 2019). *The Intercept* reports:

> And despite Dataminr's claims that its law enforcement service merely 'delivers breaking news alerts on emergency events, such as natural disasters, fires, explosions and shootings,' as a company spokesperson said, the company has facilitated the surveillance of protests, including nonviolent activity, siphoning vast amounts of social media data from

> across the web and converting it into tidy police intelligence packages. (Biddle 2020)

The US Department of Commerce's Bureau of Industry and Security oversees the licensing of export of surveillance technologies (Export Controls Act of 2018), while the departments of Commerce, Defense, State, and Energy may approve or deny a licence as long as it is 'consistent with national security and foreign policy interests' (TIMEP 2019).

Collaboration between state actors and private partners is increasing. The US, 'Big Tech', and the US military apparatus are increasingly intertwined in research, development, and delivery of surveillance products and services and using them for geopolitical goals (González 2023). Similar patterns can be recognised in their adversarial counterparts.

Despite the sheer size, the US surveillance companies are less visible than other countries' suppliers across the African countries investigated for this ADRN study. However, as Duncan (2018) argues, surveillance is a serious issue on the African continent, and the US has been actively developing the internet as a global spy machine for its own interests. This has led to other countries challenging that hegemony and pursuing different governance of the internet and their own surveillance interests.

Table 7.1 US companies and UN entities supplying digital surveillance technologies

Supplier country: USA (and UN entities)			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception	Israeli branch of US-based Verint Systems	South Sudan	Surveillance equipment to intercept communication
Internet interception			
Social media monitoring	Dataminr	Nigeria Also Kenya and South Africa	Monitoring student demonstrations in Cape Town, South Africa
Smart cities	Honeywell	Egypt	Surveillance systems for large smart city projects
Biometric ID	Palantir	UN World Food Programme	International aid funds are used for digital surveillance of migrants and refugees

Source: Authors' own. Created using data from Dataminr (2016); Thorpe (2019); Feldstein (2019); Biddle (2020); Peterson and Hoffman (2022).

8. Conclusion

1. This is a global industry facilitated by governments of competing rich countries, and African governments are buying from all of them with little regard for their geopolitical rivalries.
2. Publicly available information from governments and suppliers is superficial. While it will show that surveillance transfers are taking place, most detail can be found in investigative reports by journalists and NGOs. Even governments that do provide a higher degree of insight into their transfers, like the UK, still operate their export regimes with a high level of opacity. Most offer no meaningful insights.
3. China is by far the most scrutinised exporting country when it comes to volume of research on its surveillance transfers. Equivalent research scrutiny is not being applied to the USA, their main competitor, or others, despite the same perils to human rights.
4. Surveillance technologies are being transferred, but the surveillance element is being downplayed. For example, the EU's transfers are often under the guise of helping African states manage migration, while smart city technologies are pitched by suppliers as a way of boosting the local economy or administering local government functions, i.e. the stated purpose is not surveillance, even though the capabilities are provided.

African governments are not discriminating between competing powers when accepting surveillance technology, and all of these powers are engaged in providing it. We also note that suppliers themselves may not distinguish their customers based on geopolitical alliances and they sell to non-allied or adversarial countries (DeSombre, Gjesvik and Ole Willers 2021). Israeli firm Cellebrite, for example, despite being headquartered in a country with strong links to the US and NATO, regularly sells to Russian and Chinese buyers. Another example is Swedish mobile forensic software company MSAB, which also markets to Russian and Chinese buyers despite being in an EU/NATO country.

While many technology firms do not sell surveillance equipment directly, they do supply technology and services that have the capacity to be used for surveillance.

Looking at the exporting governments, Russia is a massive global arms exporter, but there is little evidence to suggest it is a major supplier of digital surveillance technologies to African states. Even though the Russian state has the capacity to supply these technologies, its counterparts from the US, China, and Europe are far more active in this regard. There is evidence, however, that Russia is supplying these technologies elsewhere, particularly in Central Asia (Bourgelais 2013).

Given China's growing geopolitical significance, there has also been significantly more research conducted into its technology exports than other governments. The scale of China's investment on the continent, however, and its advanced technology sector, with at least dozens of active firms, means further research is needed to fully understand the web of actors involved.

Further research is also particularly needed into EU surveillance technology transfers, which are carried out by a complex web of institutions at both the supranational and national levels, as well as those from the UK which, while providing a higher level of transparency than other governments, does not provide any public information on exact technologies or suppliers. More research is also needed into specific member states' technology transfers; something we could not fully cover given the number of countries involved and lack of transparency in many, which necessitates alternative, more time-consuming research methods.

The EU is currently in the process of updating its export licence controls, which could potentially mandate greater transparency around dual-use exports, opening up further avenues of research into both the bloc and specific member states.

In terms of the specific technologies being transferred, each exporting country tends to have a focus area, at least within the five technology types covered by this report. The UK, for example, is involved in the transfer of mobile and internet interception technology, but not the provision of biometric ID or smart city technologies.

Exporting governments also tend to be focused on particular countries, even if some, like the UK and China, are active in all of them. The EU, for example, is heavily involved in Morocco and other North African countries, but it is much less involved in Malawi and Zambia. China, on the other hand, is active in Morocco but to a much lesser extent than it is in Nigeria and Ghana.

Table 8.1 Summary of suppliers of digital surveillance technologies to African countries by country

China	China is a major and growing supplier of digital surveillance technologies, particularly those that use AI. Many of the loans provided by China to African countries are for IT infrastructure projects, rather than direct surveillance capabilities, although many of the technologies being transferred could be repurposed for surveillance.
EU	Like China, the EU and its agencies use foreign investment mechanisms to transfer technologies to Africa. Aside from surveillance transfers at the EU level, many member states have their own relationships and surveillance export arrangements with the five countries covered in this report, including Germany, France, and Italy.
Israel	Israel's 'military-innovation ecosystem' creates a continuous pipeline of surveillance tools. In this ecosystem, the distinction between private and public space is blurred.
Russia	Russia is attempting to project its influence over Africa, but there is little evidence to suggest it is a major supplier of digital surveillance technologies to African states.
UK	The UK government has close political and economic ties with many of the former African colonies. This has sometimes involved the transfer of surveillance equipment and training.
USA	There are over 120 surveillance companies headquartered in the US. The US government agencies, 'Big Tech', and the US military apparatus are increasingly intertwined in research, development, and delivery of surveillance products and services and are using them for geopolitical goals.

Source: Authors' own.

References

Abdelnour, S. (2023) '**Making a Killing: Israel's Military-Innovation Ecosystem and the Globalization of Violence**', *Organization Studies* 44.2: 333–37 DOI: 10.1177/01708406221131938 (accessed 11 August 2023)

Abdulaziz, I. (2023) '**With Kano Centre, Nigeria Pushes For Data Sovereignty, Better Security**', *NAN News*, 15 February (accessed 12 May 2023)

AccessNow (2022) '**Victory! FinFisher Shuts Down**', press release, 29 March (accessed 12 May 2023)

AidData (n.d.) ***Project ID: 30956. China Eximbank Provides $123.4 Million Preferential Buyer's Credit for Phase 2 of Dedicated Security Information System Project (Linked to #1862)*** (accessed 12 May 2023)

Amnesty International (2022) ***The Pegasus Project: How Amnesty Tech Uncovered the Spyware Scandal – New Video***, 23 March (accessed 12 May 2023)

Amnesty International (2020) ***German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed***, 25 September (accessed 12 May 2023)

BBC (2017) ***How BAE Sold Cyber-Surveillance Tools to Arab States***, 15 June (accessed 12 May 2023)

Bergman, R. and Mazzetti, M. (2022) '**The Battle for the World's Most Powerful Cyberweapon**', *The New York Times*, 28 January (accessed 12 May 2023)

Biddle, S. (2020) '**Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr**', *The Intercept*, 9 July (accessed 12 May 2023)

Boston University Global Development Policy Center (2022) ***Chinese Loans to Africa Database*** (accessed 12 May 2023)

Bourgelais, P. (2013) ***Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia, Access*** (accessed 12 May 2023)

Braun, E. (2022) '**Destination Africa: The Scramble to Sell Cyberweapons to Dictators**', *Politico*, 7 December (accessed 12 May 2023)

Burkitt-Gray, A. (2022) '**Malawi Government Sets Up National Data Centre with Huawei**', *Capacity*, 26 July (accessed 12 May 2023)

CAAT (n.d.) ***UK Export Licences Approved for Dual-Use Goods Since 2008***, Campaign Against Arms Trade (accessed 12 May 2023)

Canet, J-P.; Destal, M.; Labed, R.; Lavrilleux, A. and Livolsi, G. (2021) '**Surveillance Made in France**', *Egypt Papers*, 23 November (accessed 12 May 2023)

CEPOL (2020) ***EUROMED Police***, European Union Agency for Law Enforcement (accessed 12 May 2023)

China Daily (2022) '**Huawei-Supported 5G Network Launched in Zambia**', 26 November (accessed 12 May 2023)

Chrisafis, A. (2023) '**Macron Pledges to Reduce French Military Presence in Africa**', *The Guardian*, 27 February (accessed 12 May 2023)

Coluccini, R. (2023) '**Gli Spyware Italiani sul Mercato Internazionale**', *RPI Media*, 8 February (accessed 12 May 2023)

Cook, J. (2019) '**Israeli Spyware Technology, Tested on Palestinians, Now Operating in a City Near You**', *Washington Report on Middle East Affairs*, 9 December (accessed 12 May 2023)

Cox, J. (2018) '**UK Government is Cozy with Companies Selling Spytech**', *Vice*, 17 April (accessed 12 May 2023)

Cox, J. (2016) '**British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes**', *Vice*, 26 August (accessed 12 May 2023)

Dadoo, S. (2022) '**Israel's Spyware Diplomacy in Africa**', *Orient XXI*, 12 September (accessed 12 May 2023)

Dataminr (2023) ***Real-Time Alerts Inform UN Response and Humanitarian Aid Delivery***, First Alert (accessed 12 May 2023)

Dataminr (2016) ***Product Update: Geospatial Analysis Application*** (accessed 30 May 2023)

DeSombre, W.; Gjesvik, L. and Ole Willers, J. (2021) ***Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets***, Washington DC: Atlantic Council (accessed 12 May 2023)

DIT (2021) ***UK Strategic Export Controls***, London: Department for International Trade (accessed 12 May 2023)

Duncan, J. (2018) '**Taking the Spy Machine South: Communications Surveillance in Sub-Saharan Africa**', in B. Mutsvairo (ed.), *The Palgrave Handbook of Media and Communication Research in Africa*, Cham: Palgrave Macmillan (accessed 12 May 2023)

EC (n.d.a) ***Guidelines for Data Collection and Preparation of the EU Annual Report on Dual-Use Export Controls Under Regulation (EU) 821/2021***, European Commission (accessed 12 May 2023)

EC (n.d.b) ***EU-Africa: Global Gateway Investment Package***, European Commission (accessed 12 May 2023)

EC (2022) ***Cover Note: Report from the Commission to the European Parliament and the Council on the Implementation of Regulation (EU) 2021/821 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items***, European Commission (accessed 12 May 2023)

EC (2019) '**The EU is Boosting its Support to Morocco with New Programmes Worth €389 Million**', *European Commission*, press release, 20 December (accessed 30 May 2023)

EC (2002) '**European Commission: Integrating Migration Issues into the EU's External Relations**' *European Commission*, press release, 3 December (accessed 12 May 2023)

EuropeAid (2008) ***Aeneas Programme: Programme for Financial and Technical Assistance to Third Countries in the Area of Migration and Asylum. Overview of Projects funded 2004–2006***, European Commission (accessed 12 May 2023)

European Ombudsman (n.d.) '**Decision on How the European Commission Assessed the Human Rights Impact Before Providing Support to African Countries to Develop Surveillance Capabilities (Case 1904/2021/MHZ)**', (accessed 12 May 2023)

EUTF (2023) ***Emergency Trust Fund for Africa: Sahel and Lake Chad***, European Union, Trust Fund for Africa (accessed 12 May 2023)

EUTF (2017) ***Dismantling the Criminal Networks Operating in North Africa and Involved in Migrant Smuggling and Human Trafficking***, European Union Trust Fund for Africa (accessed 30 May 2023)

Feldstein, S. (2019) *The Global Expansion of AI Surveillance*, Washington DC: Carnegie Endowment for International Peace

France24 (2023) '**France Must Demonstrate "Profound Humility" Towards Africa, Macron Says Ahead of Four-Nation Trip**', 27 February (accessed 16 May 2023)

Frontex (2017) ***Strengthening of AFIC as an Instrument to Fight Serious Cross-Border Crimes Affecting Africa and the EU***, Warsaw: Frontex (accessed 11 August 2023)

Frontex (2016) ***Africa-Frontex Intelligence Community Joint Report***, Warsaw: Frontex (accessed 16 May 2023)

Gagliardone, I. (2020) '**The Impact of Chinese Tech Provision on Civil Liberties in Africa**', *Policy Insights* 99: 1–20 (accessed 16 May 2023)

González, R.J. (2023) '**Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry**', *TNI*, 7 February (accessed 16 May 2023)

GOV.UK (n.d.a) ***UK Defence and Security Exports for 2021*** (accessed 16 May 2023)

GOV.UK (n.d.b) ***Chart 7: Total UK Defence Exports (Based on Orders/Contracts Signed) by Region 2012 to 2021*** (accessed 16 May 2023)

Hedenskog, J. (2018) ***Russia is Stepping Up its Military Cooperation in Africa***, FOI Memo 6604, Stockholm: Swedish Defence Research Agency (accessed 16 May 2023)

Huawei (2022) ***New ICT Helps Build Smart Zambia*** (accessed 16 May 2023)

Huawei (2021) ***West Africa's CloudExchange Rapidly Transforms into a Leading ISP with Huawei*** (accessed 16 May 2023)

Huawei (2020) ***Ghana Commercial Bank Implements a Mobile Money Strategy*** (accessed 16 May 2023)

Interfax (2019) ***РФ анонсировала новые соглашения о военном сотрудничестве со странами Африки*** [Russia Announces New Agreements on Military Cooperation with African Countries] (accessed 16 May 2023)

Klovig Skelton, S. (2020) 'Humanitarian Data Collection Practices Put Migrants at Risk', *Computer Weekly*, 13 November

Kortum, S. and Lerner, J. (2000) '**Assessing the Contribution of Venture Capital to Innovation**', *RAND Journal of Economics* 31.4: 674–92, DOI: 10.2307/2696354 (accessed 16 May 2023)

Kwet, M. (2019) '**Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa**', *Vice*, 22 November (accessed 16 May 2023)

Levin, S. (2016) '**Twitter Blocks Government "Spy Centers" From Accessing User Data**', *The Guardian*, 15 December (accessed 16 May 2023)

Loewenstein, A. (2023) *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*, London: Verso Books

Loewenstein, A. (2019) '**Exporting the Technology of Occupation**', *The New York Review*, 4 January (accessed 16 May 2023)

Mada Masr (2021) 'French Tech Executives Indicted After Selling Surveillance Software to Libya, Egypt', 23 June

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) ***Mapping Hacking Team's 'Untraceable' Spyware***, Citizen Lab, 17 February (accessed 16 May 2023

Marczak, B.; Scott-Railton, J.; Rao, S.P., S.; 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 16 May 2023)

Marczak, B.; Scott-Railton, J.; Senft, A.; Poetranto, I. and McKune, S. (2015) *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, Citizen Lab Research Report 64, Toronto: University of Toronto

Mayhew, S. (2016) '**STC Demos Latest Multimodal Biometric Solutions at Africa Aerospace and Defence Expo**', *BiometricUpdate.com*, 27 September (accessed 16 May 2023)

Murray, M. (2022) *The Infrastructures of Security: Technologies of Risk Management in Johannesburg*, Ann Arbor MI: University of Michigan Press

Mwesigwa, D. (2019) ***Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy***, CIPESA blog, 9 December (accessed 16 May 2023)

Nedopil, C. (2023) *Countries of the Belt and Road Initiative*, Shanghai: Green Finance & Development Center (accessed 17 May 2023)

Ofori-Atta, K. and Kan-Dapaah, A. (2019) ***Joint Memorandum for the Approval of the Commercial Contract, Facility Agreement and Tax Exemption for the Implementation of the Integrated National Security Communications Enhancement (ALPHA) Project (Phase 11)***, Accra: Parliament of Ghana Library (accessed 17 May 2023)

Ojoye, O. (2021) '**Nigeria Signs Military-Technical Cooperation Agreement with Russia**', Ministry of Defence, Federal Republic of Nigeria, press release, 29 August (accessed 17 May 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019a) '**Huawei Technicians Helped African Governments Spy on Political Opponents**', *The Wall Street Journal*, 15 August (accessed 17 May 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019b) ***The Wall Street Journal Claims Huawei Technologies Staff Helped Zambia & Uganda Govts. Spy on Opponents; Company Denies Allegations***, Business & Human Rights Resource Centre, 15 August (accessed 17 May 2023)

Peterson, D. and Hoffman, S. (2022) *Geopolitical Implications of AI and Digital Surveillance Adoption*, Brookings Institution Policy Brief, Washington DC: Brookings Institution

Privacy International (2016) ***The Global Surveillance Industry***, July (accessed 17 May 2023)

Privacy International (2015a) ***Ethiopia Expands Surveillance Capacity with German Tech Via Lebanon***, 23 March (accessed 17 May 2023)

Privacy International (2015b) ***Facing the Truth: Hacking Team Leak Confirms Moroccan Government Use of Spyware***, 10 July (accessed 17 May 2023)

Riehle, C. (2019) '**Risk Analysis Cell in Niger**', *Eucrim*, 18 February (accessed 17 May 2023)

Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) ***Surveillance Law in Africa: A Review of Six Countries***, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.059** (accessed 17 May 2023)

Robinson, K. (2022) ***How Israel's Pegasus Spyware Stoked the Surveillance Debate***, Council on Foreign Relations, 8 March (accessed 17 May 2023)

Rosoboronexport (2023) ***Partner Countries and Joint Projects*** (accessed 17 May 2023)

Rosoboronexport (2021a) ***Forensic Equipment*** (accessed 17 May 2023)

Rosoboronexport (2021b) **'Rosoboronexport Increased its Order Portfolio in Sub-Saharan Africa by $1.7 Billion**', press release, 7 June (accessed 17 May 2023)

Salman, Y. (2021) 'The Security Element in Israel-Africa Relations', *Strategic Assessment* 24.2: 38–53

Shtaya, M. (2022) ***Nowhere to Hide: The Impact of Israel's Digital Surveillance Regime on the Palestinians***, Middle East Institute, 27 April (accessed 30 May 2023)

Singh, A. (2015) ***FinFisher Research Referenced in Articles on German Court Investigation, South African Servers***, Citizen Lab, 25 February (accessed 17 May 2023)

Soldatov, A. and Borogan, I. (2012) '**Project_ID: Who's Bugging the Russian Opposition?**', *Open Democracy*, 24 February (accessed 17 May 2023)

Statewatch (2019) ***Aid, Border Security and EU-Morocco Cooperation on Migration Control***, 24 November (accessed 17 May 2023)

Stronski, P. (2019) ***Late to the Party: Russia's Return to Africa***, Washington DC: Carnegie Endowment for International Peace (accessed 17 May 2023)

Takouleu, J.M. (2018) '**AFRICA: Huawei Sets Up a $1.5 Billion Fund to Boost African Smart Cities**', *Afrik21*, 6 June (accessed 17 May 2023)

Thorpe, J. (2019) '**ISJ Exclusive: Be Ready for Anything with Dataminr**', *International Security Journal*, 14 November (accessed 17 May 2023)
TIMEP (2019) ***TIMEP Brief: Export of Surveillance to MENA Countries***, Tahrir Institute for Middle East Policy, 23 October (accessed 17 May 2023)

Wezeman, S.T. (2011) ***Israeli Arms Transfers to Sub-Saharan Africa***, SIPRI Background Paper, Solna: Stockholm International Peace Research Institute (accessed 17 May 2023)

Wezeman, P.D.; Kuimova, A. and Wezeman, S.T. (2021) ***Trends in International Arms Transfers***, SIPRI Fact Sheet, Solna: Stockholm International Peace Research Institute (accessed 17 May 2023)

Whittaker, Z. (2019) '**Documents Reveal How Russia Taps Phone Companies for Surveillance**', *TechCrunch*, 18 September (accessed 17 May 2023)

Wilson, T. (2023) 'Russia's Growing Trade in Arms, Oil and African Politics', *Financial Times*, 14 February

WITS (2019) ***Sub-Saharan Africa Imports, Tariffs by Country and Region 2020***, World Integrated Trade Solution (accessed 17 May 2023)

Woodhams, S. (2020) '**China, Africa, and the Private Surveillance Industry**', *Georgetown Journal of International Affairs* 21: 158–65 (accessed 17 May 2023)

ZTE (2021) '**Announcement: Provision of Performance Guarantee Limits for Overseas Subsidiaries for 2021**', Overseas Regulatory Announcement, ZTE Corporation (accessed 17 May 2023)