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

DOI: 10.19088/IDS.2023.027

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 constitution[5] 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.

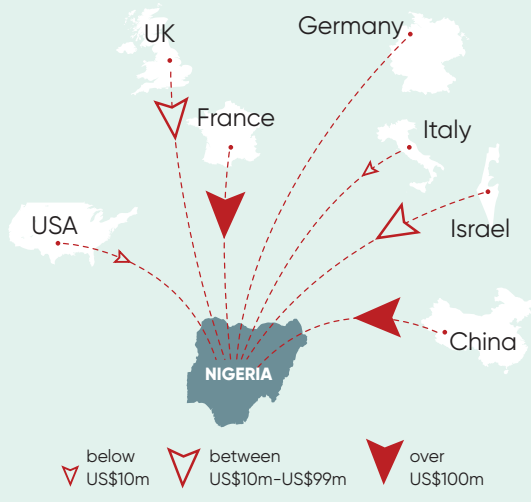
5 See **Section 37 of the Constitution of the Federal Republic of Nigeria**.
6 See **Lawful Interception of Communications Regulations, 2019**.

- **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**.

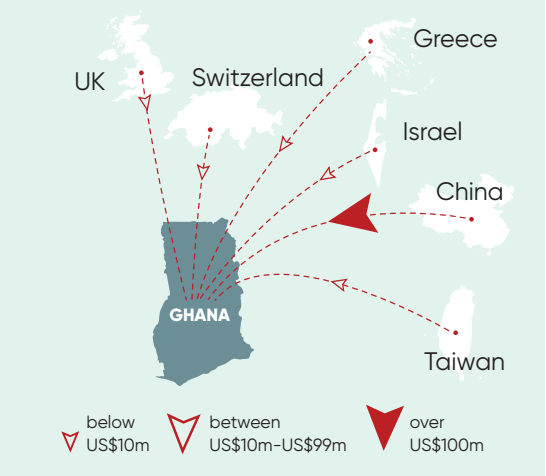
US$235m. Ghana is also implementing a US$300m comprehensive smart city project, via ArisCel (Ghana/China).

- **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**.

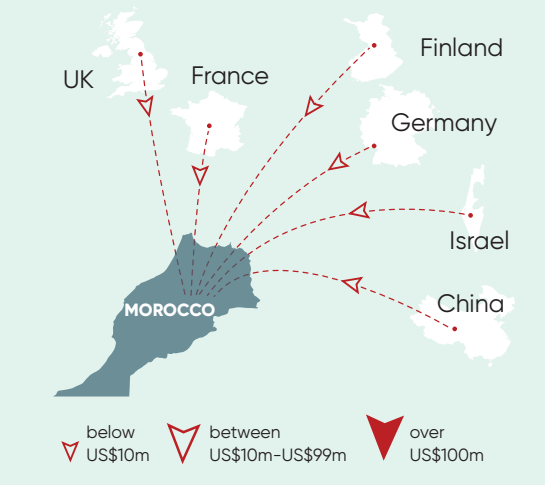
- **Biometric ID:** Biometric identification technologies in Morocco are supplied by French company IDEMIA. Biometric scanners are used to verify the identity of passengers entering and leaving Morocco. In 2022, Morocco also launched the first digital ID system which Moroccans will use as proof of citizenship.

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

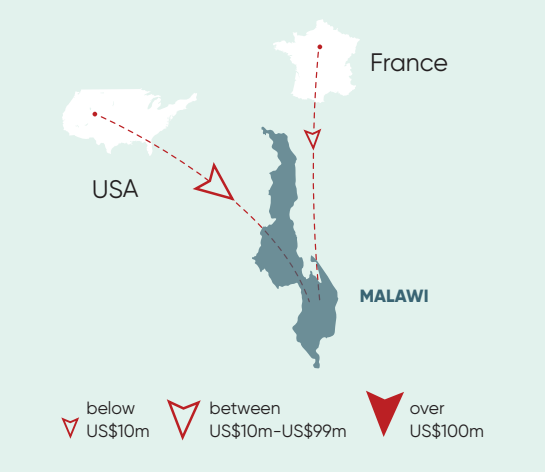
10 See **Malawi's Constitution of 1994**.
11 See **National Registration Act**.

- **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.

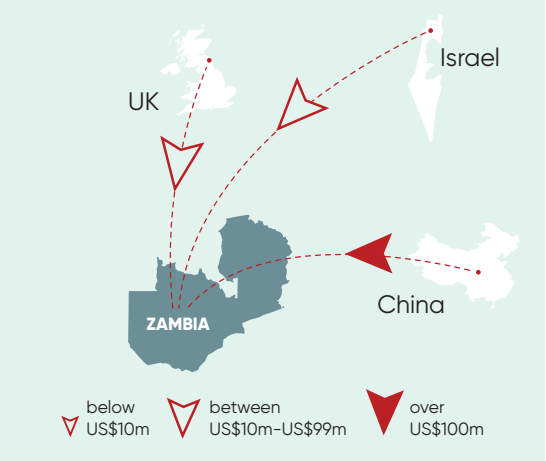
12 See **Zambia's Bill of Rights**.

- **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.

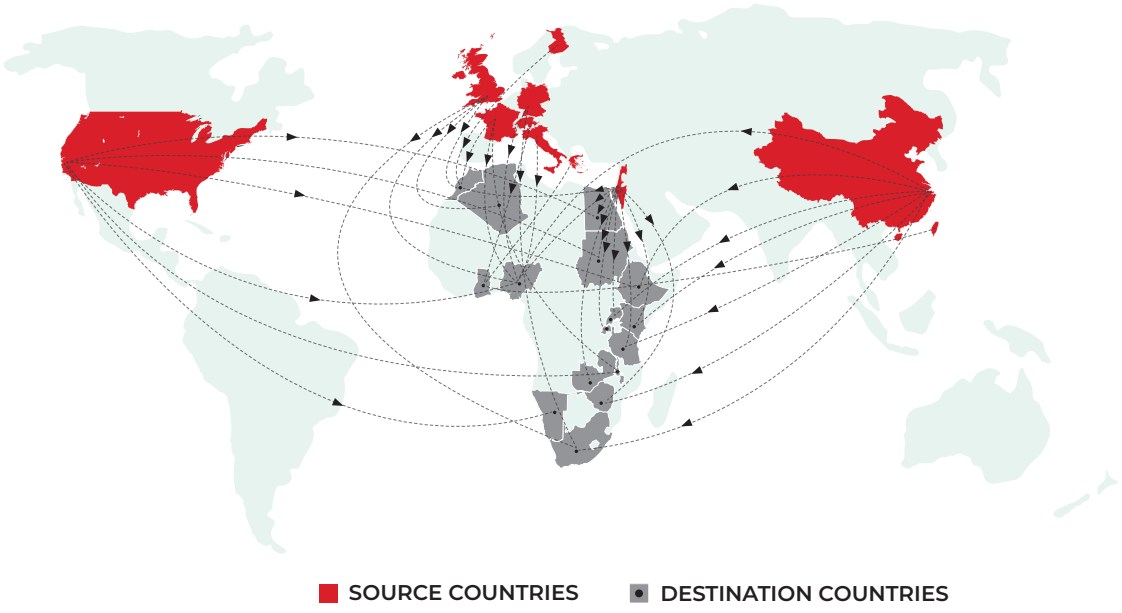
Germany: The UK/German company Gamma supplied its FinFisher mobile phone spyware across Africa including Nigeria and Morocco.

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: 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.

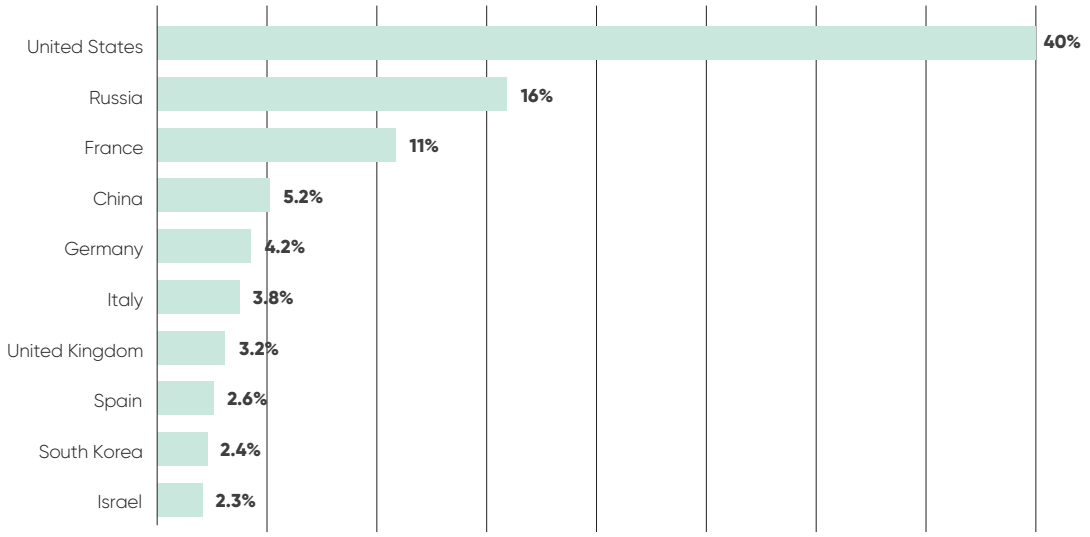
This raises civil society concerns about surveillance creep and a possible descent into digital authoritarianism. Social media monitoring combined with safe city facial recognition of public space introduces the potential (not yet fully operationalised) for state data centres to monitor in real time 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