State Power and Digital Surveillance in Africa

Karol Czuba

Supplementary Online Material

Contents

Part I: Description of Evidence

This part of supplemental material contains narrative description of the evidence of government digital surveillance in Africa collated in the datasets that make up supplements 6 and 7. It comprises three supplements. Supplement 1 contains a summary of the reporting on government digital surveillance in Africa by news media outlets indexed in the Factiva repository. Supplement 2 discusses the corporations reported to have supplied digital surveillance technology to African governments and the tools they develop. Supplement 3 details government use of this technology in each African country where it has been reported.

Supplement 1: Repository-catalogued Media Reporting on Government Digital Surveillance in Africa

Evidence of government digital surveillance in Africa collated in the instances datasets is suggestive of importance that authorities across the continent attach to increasing legibility and control over entire populations or their large segments through mass surveillance, largely in the form of seemingly mundane activities such as registration and CCTV camera installation; active efforts to surveil specific targets are noteworthy but relatively rare. Such prioritization of expansion of state power at scale contrasts with the distribution of media interest in government digital surveillance in Africa documented in the repository dataset.

While the number of reported instances varies considerably across the continent's regions and countries, the geographic concentration of media attention to government digital surveillance in Africa is much more pronounced. Over half of the mentions of such surveillance in Factiva-indexed articles concern countries in Eastern Africa, almost twice its share of actual surveillance deployments more accurately represented in the instances dataset (Figure 1.1). Of the 10 coun-

tries covered by at least 10 articles included in the repository dataset, six are in the region (Figure 1.2). Its relatively small number of instances notwithstanding, Ethiopia alone accounts for 17.5% of the media mentions. Government digital surveillance in Egypt (3.1%), Kenya (3.6%), Morocco (3.1%), Nigeria (12.5%); Rwanda (3.9%), South Africa (8.4%), Uganda (10.3%), Zambia (5.3%), and Zimbabwe (7.5%)—but not Ghana and Tunisia, where authorities have also subjected populations to extensive monitoring—has received considerable media attention as well. Half of the articles (49.2%) concern suppression of political opposition; they also mention government attribution of surveillance tool purchases to crime prevention efforts (8.3%, in addition to counterterrorism at 1%, national security considerations at 0.6%, and unspecified security enhancements at 1.6%) and public service improvement (1.3%; Figure 1.3).

At 56.2% of mentions, media reports have primarily focused on targeted surveillance, which makes up a much smaller fraction of documented instances (Figure 1.4). 36.7% of the articles mention mass surveillance, and 3.7%—mass-to-targeted surveillance. The most commonly reported surveillance modalities are the interception of online and SMS communications (this category excludes phone call interception), at 37.3%; spyware device infection with spyware, at 22.8%; CCTV surveillance, at 7.5% (including CCTV with facial recognition at 3.1%); SIM card registration, also at 7.5%; and phone call interception, at 7% (Figure 1.5). Of the over 50 digital surveillance tool suppliers listed in the repository dataset, the most commonly mentioned are Amesys (0.9%), Circles (3.6%), CloudWalk (2.1%), Gamma (7.8%), Hacking Team (8.1%), Huawei (8.4%), NSO Group (8.1%), Verint (1.2%), and ZTE (1.9%; Figure 1.6). Except for CloudWalk, Huawei, and ZTE, all these companies have provided African governments with tools used in targeted or mass-to-targeted surveillance.

The content of the repository articles maps very imperfectly onto the landscape of government digital surveillance in Africa revealed by the instances dataset. It does, however, evince the priorities of the media outlets indexed by Factiva, and their interest in specific regions and countries; surveillance purposes, types, and modalities; and surveillance technology suppliers.

Figure 1.1

Region

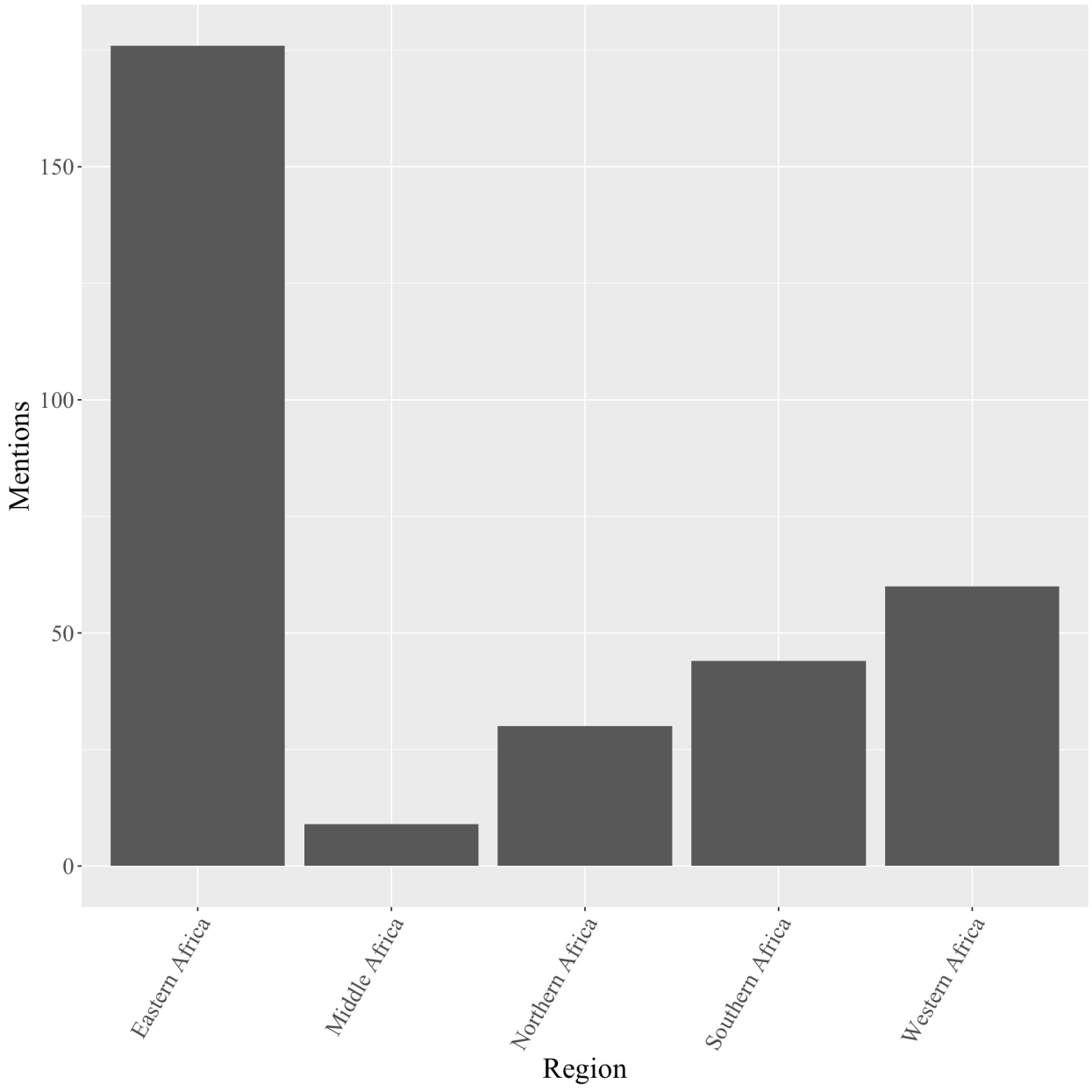


Figure 1.2

Country

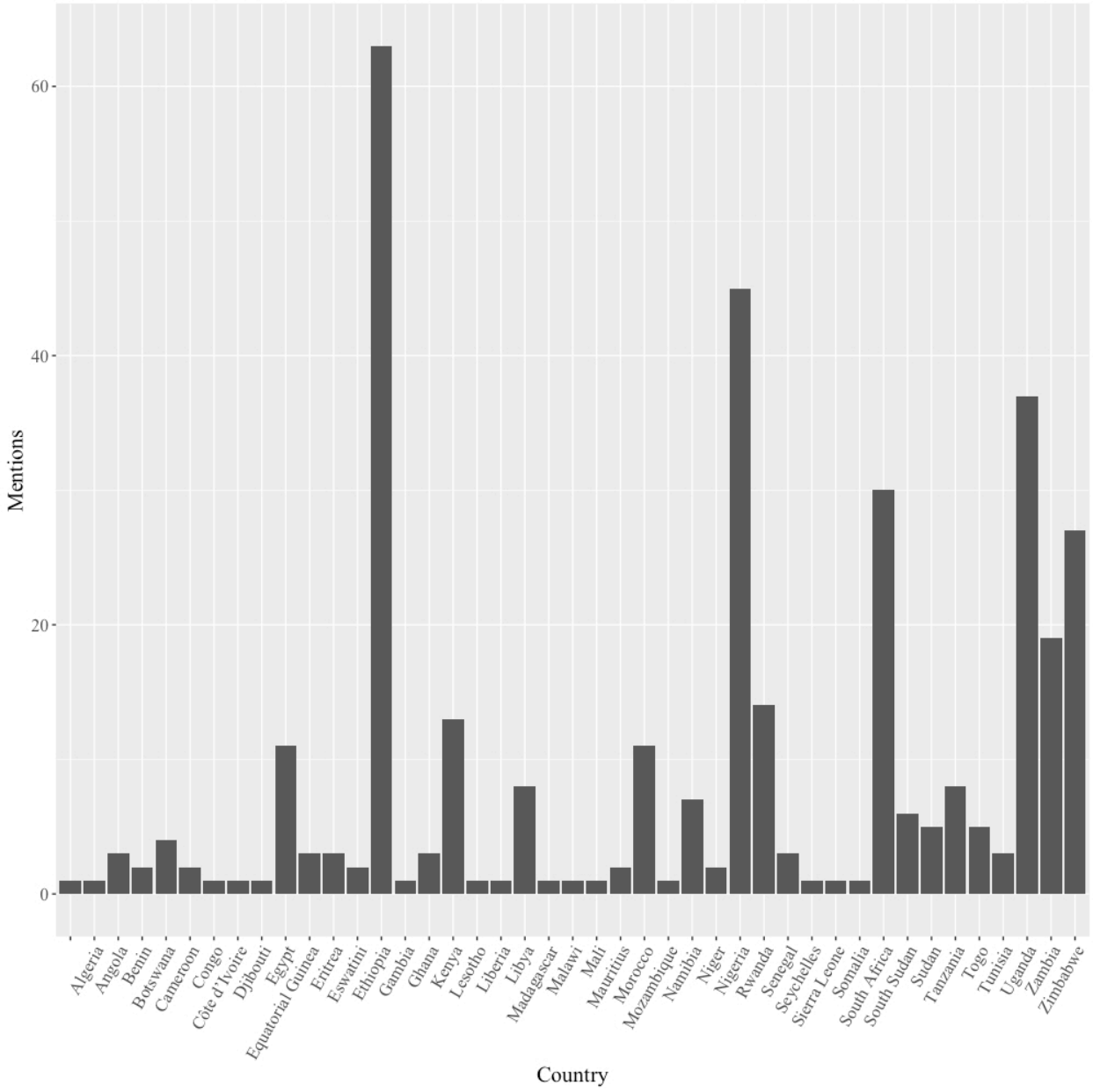


Figure 1.3

Purpose

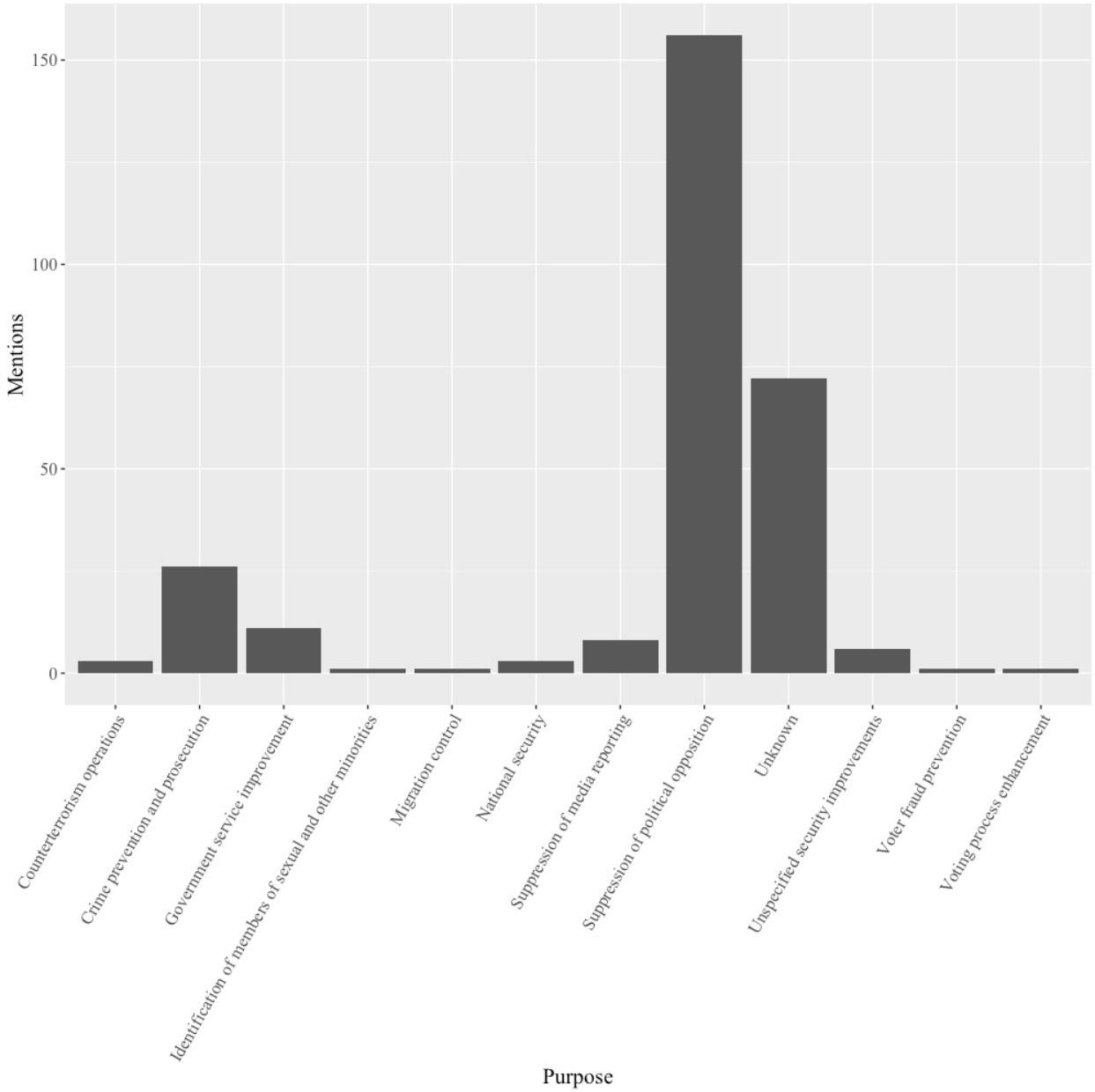


Figure 1.4

Surveillance type

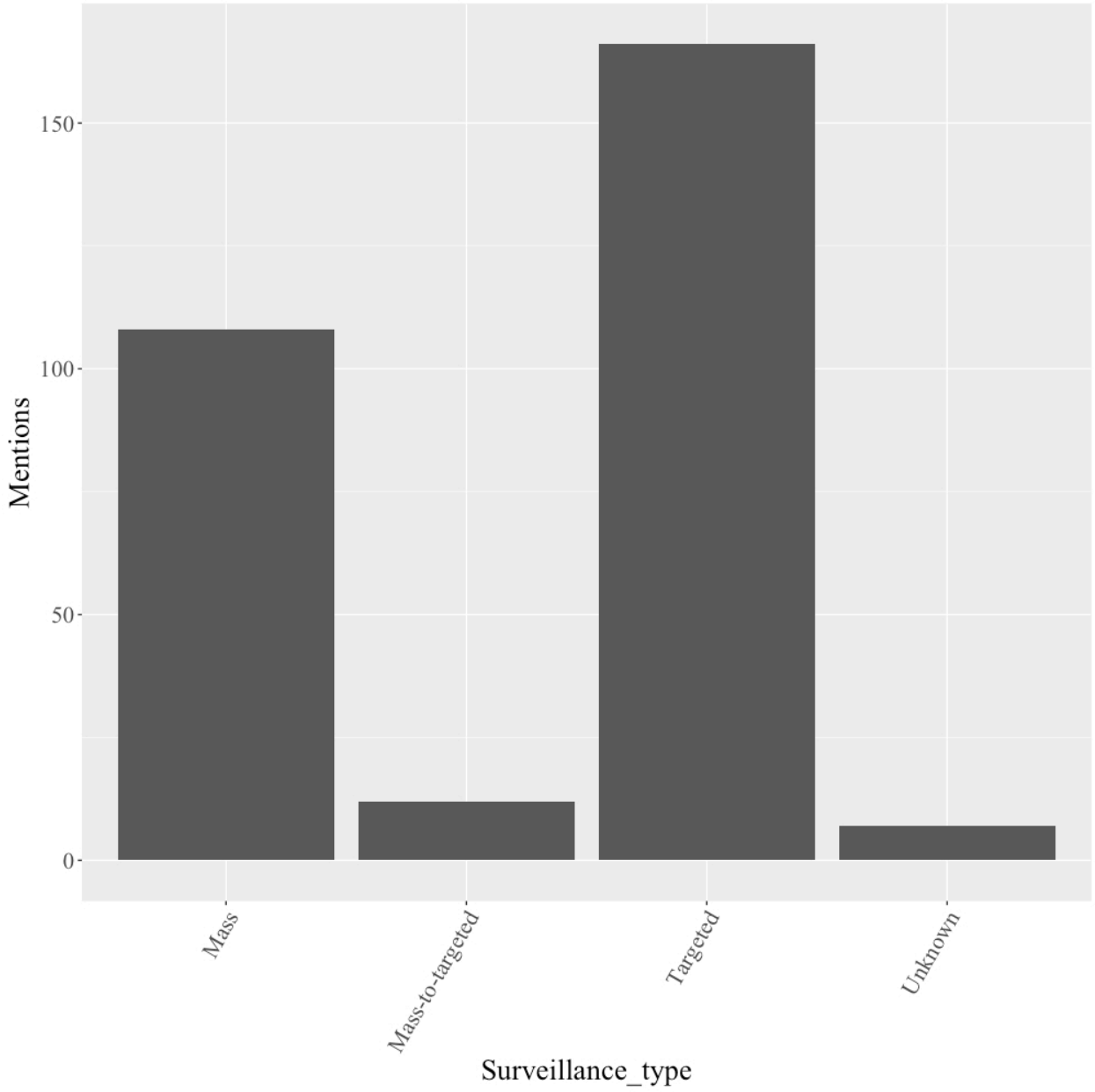


Figure 1.5

Surveillance modality

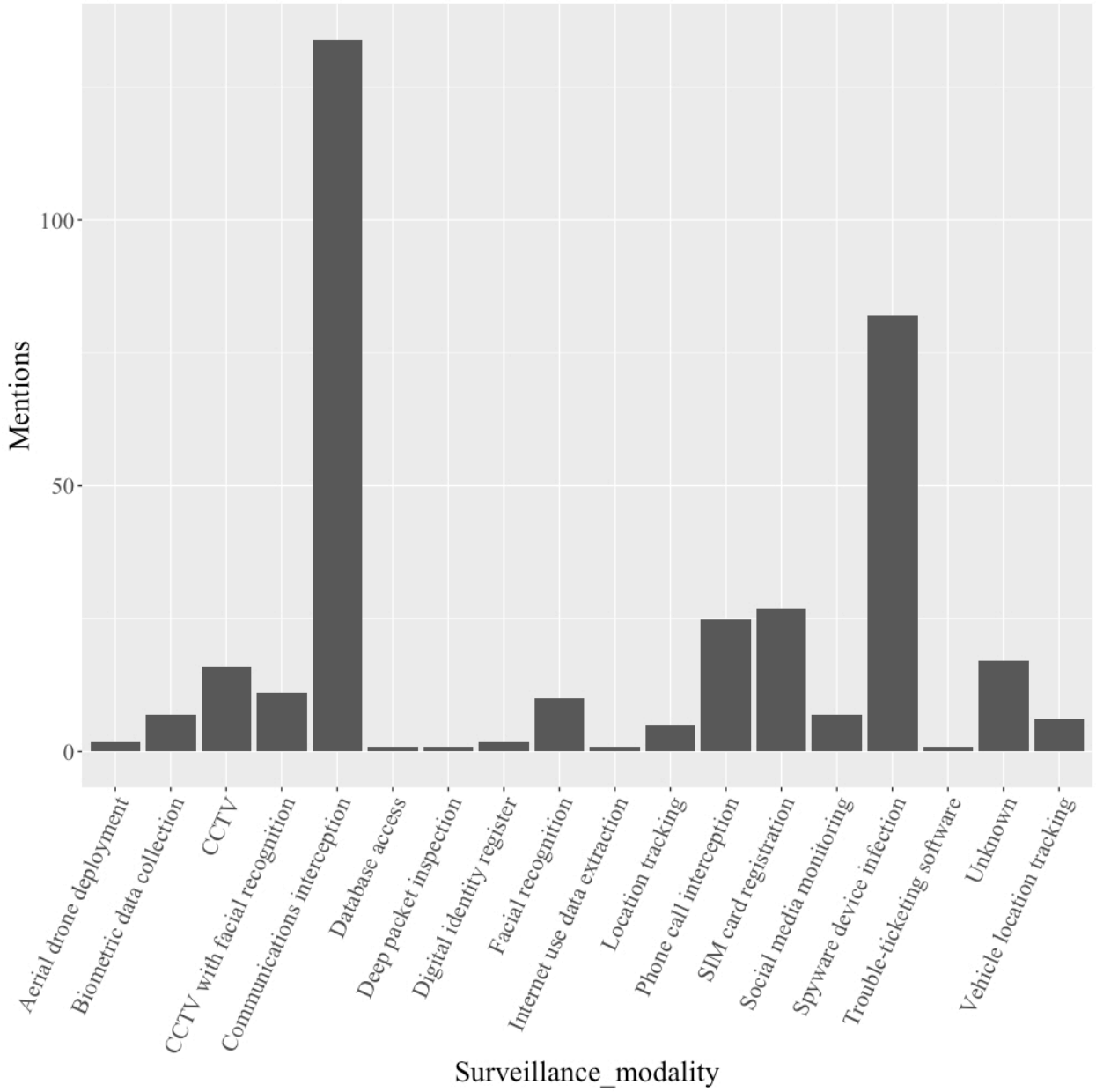
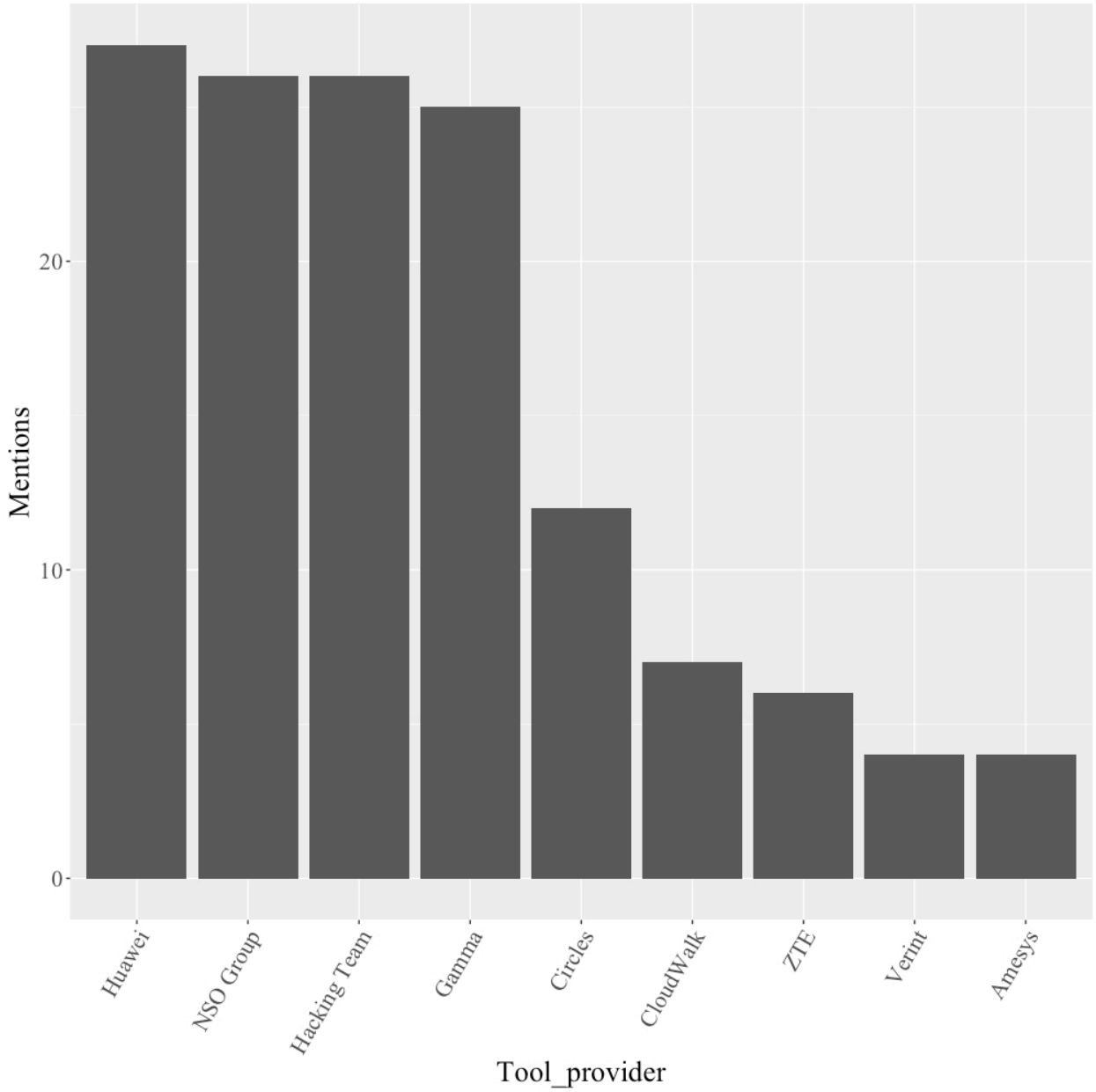


Figure 1.6

Tool provider



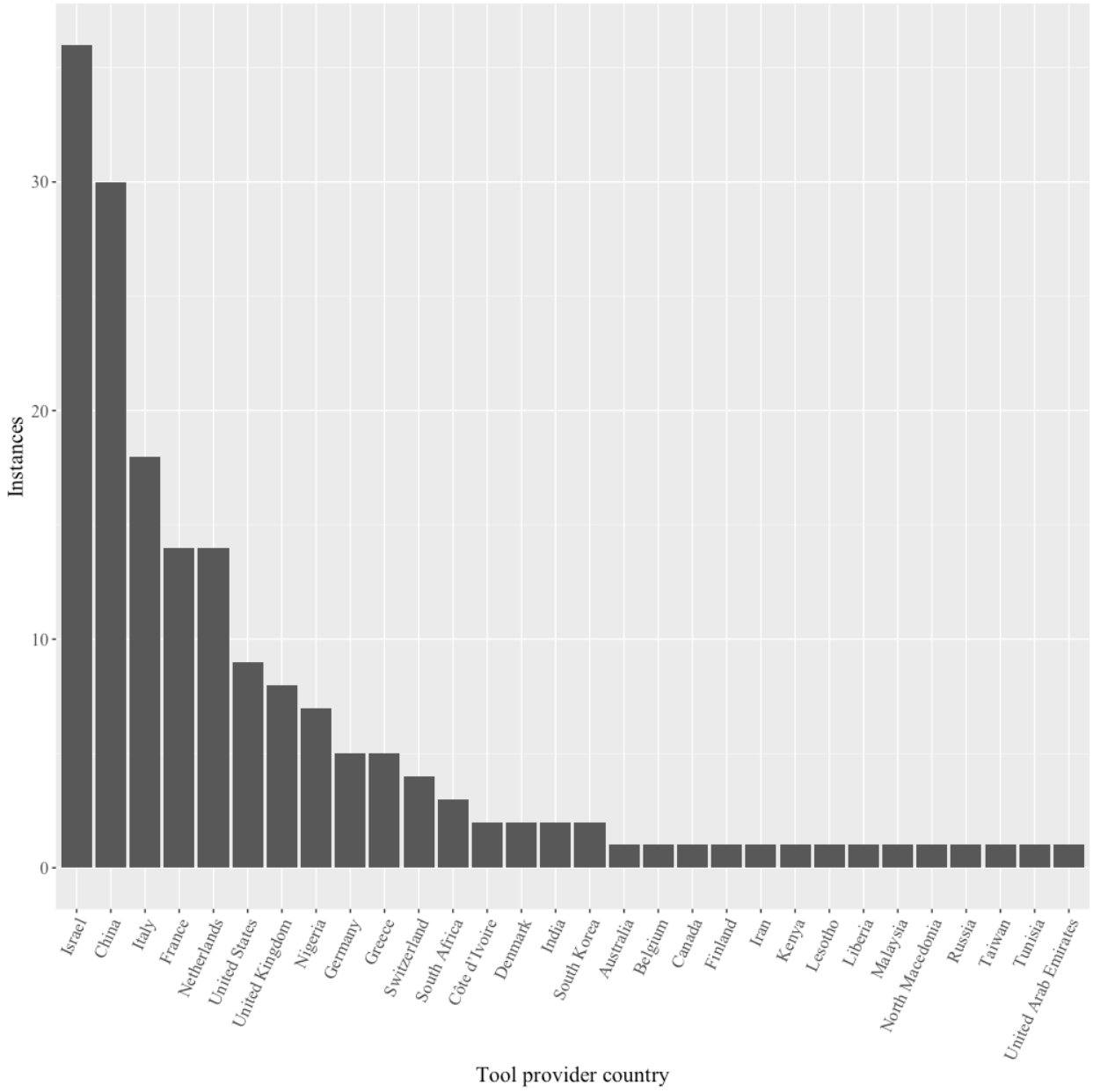
Supplement 2: Providers of Government Digital Surveillance Tools in Africa

Digital surveillance generally depend on access to sophisticated technological tools. Exceptions exist: a simple database is sufficient for non-biometric registration of people and their computing equipment—even if dedicated software, such as Ethio-Telecom's Zsmart (provided by the Chinese company ZTE), can facilitate management of large datasets—while physical searches of unlocked devices require no specialized tools at all. But biometric data collection involves deployment of fingerprint, hand geometry, face, iris, retina, palm vein, or voice identification scanners. Packet analyzers, intercepting proxy servers, social media monitoring suites, and other specialized software enable DPI and internet traffic monitoring. 'Safe' and 'smart' cities cannot exist without facial recognition-enabled CCTV cameras and other advanced sensors. And device infection depends on identification of zero-day vulnerabilities exploited by sophisticated spyware. African governments have neither the capacity nor need to develop such tools themselves. Instead, they purchase commercially available products and, with them, the ability to expand their power.

Included articles identify 71 different technology providers located in 30 countries (Figure 2.1). Israel is home to companies involved in the largest number—36 (9.6%)—of the reported instances of government digital surveillance. Chinese suppliers have sold tools deployed in 30 (8%) instances. Companies based in France (14, 3.7%), Italy (18, 4.8%), the Netherlands (14, 3.7%), the United Kingdom (eight, 2.1%), and the United States (nine, 2.4%) have also repeatedly provided digital surveillance technology to African governments. The dataset also lists 16 African digital surveillance tool developers, based in Côte d'Ivoire (two), Kenya (one), Lesotho (one), Liberia (one), Nigeria (seven, 1%), South Africa (three), and Tunisia (one).

Figure 2.1

Tool provider countries

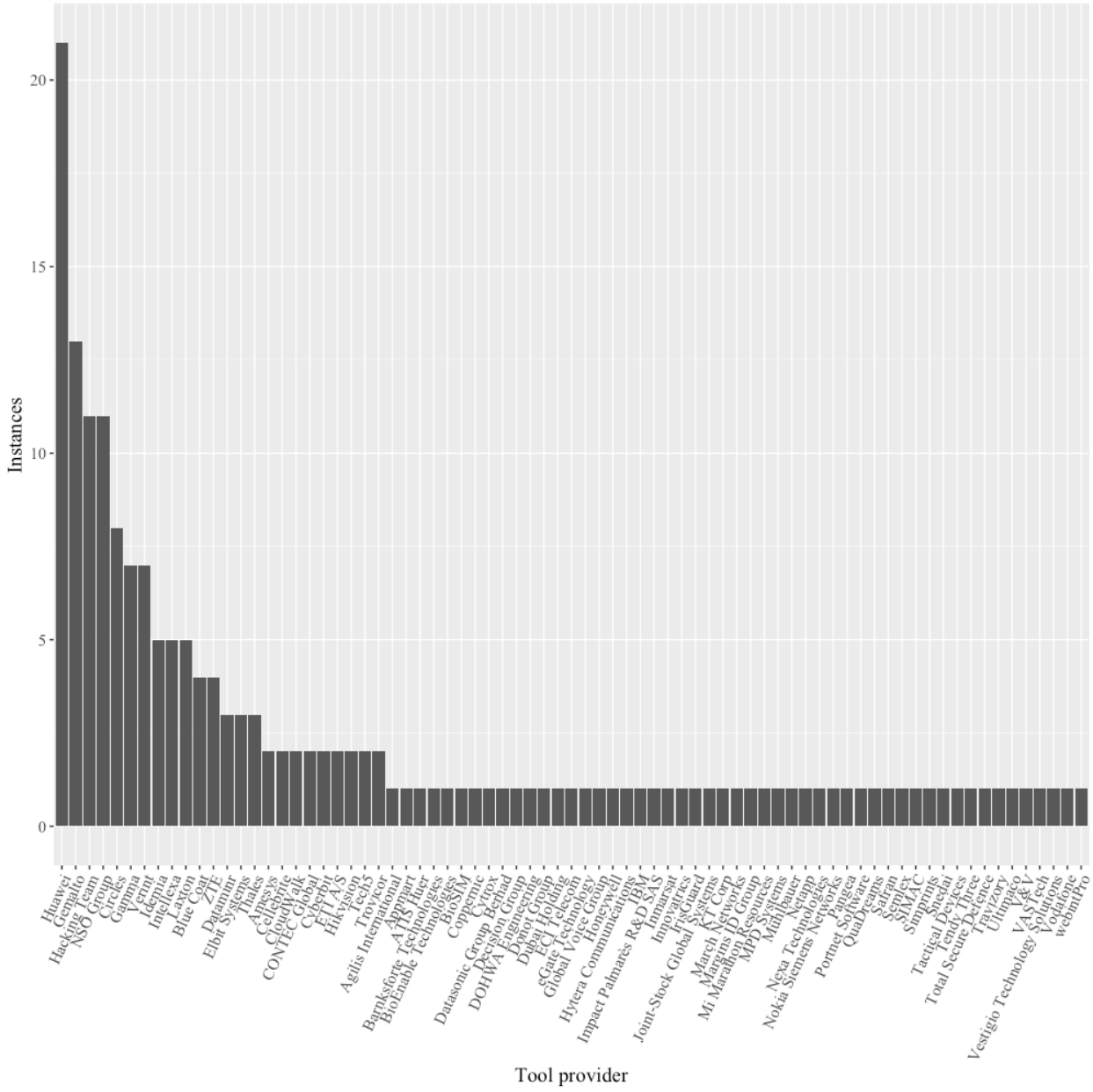


China's Huawei has supplied tools used in 21 instances (5.6%), more than any other company (Figure 2.2). It has sold 'smart city' systems in Algeria, Cameroon, Egypt, Kenya, South Africa, and Uganda; built government data centres in Cameroon, Kenya, Malawi, Senegal, Zambia, and Zimbabwe; and intercepted the online communications of government opponents in Uganda and Zambia. Huawei has also engaged in negotiations to sell its technology to the governments of Burkina Faso and Mauritius. Eleven instances (2.9%) of government digital surveillance in Africa involve deployment of the Israeli spyware developer NSO Group's Pegasus. Botswanan, Equatorial Guinean, Kenyan, Moroccan, Nigerian, Zambian, and Zimbabwean authorities have used technology purchased from another another Israeli company, Circles, which exploits vulnerabilities in the Signaling System 7 protocol used in 2G and 3G mobile networks, in eight instances (2.1%). The European spyware developers Gamma, Hacking Team (both headquartered in Italy), and Intellexa (based in Greece) have sold tools used in seven (1.9%), 11 (2.9%), and five (1.3%) instances, respectively. Governments of Egypt, Kenya, Nigeria, and Sudan have used DPI software procured from the US-based Blue Coat in four instances (1%). Three European providers of biometric identification systems—Gemalto (13, 3.5%), Laxton (five, 1.3%; both have head offices in the Netherlands), and (France-based) Idemia (five, 1.3%) —close out the top ten. Gemalto has sold such systems to government clients in Algeria, Benin, Côte d'Ivoire, Gabon, Morocco, South Africa, and Tunisia; Laxton—in Malawi, Mozambique, Nigeria, and Zimbabwe; and Idemia—in Egypt, Guinea, Kenya, and Morocco. Of the African developers of digital surveillance technology, five—Côte d'Ivoire's Snedai, Kenya's BioSIM, and Nigeria's Appmart Integrated, Barnksforte Technologies, and eGate Technology—have provided governments with digital registration technologies. V&V, based in Nigeria (but Israeli-

owned), has sold spyware (likely sourced from Circles, rather than developed in-house). Another Nigerian company, Vestigio, has received a contract to build a ‘safe city’ system. South Africa’s Global Voice Group and VASTech have supplied internet traffic monitoring and interception tools. This supplement provides information about these corporations and the technology they have supplied to African governments.

Figure 2.2

Tool providers



African Providers

Most African suppliers of government digital surveillance technology are telecom companies—such as 9mobile, Ethio-Telecom, Safaricom, Telkom, and Vodacom—that have obtained it from actual developers of surveillance tools. In this section I only list such developers.

VASTech, headquartered in Stellenbosch and generously funded by the South African government (Privacy International, 2019f), provided the Muammar Gaddafi regime in Libya tools to wiretap and log all international phone calls to and from the country. VASTech's Zebra spyware "capture[d] and store[d] massive volumes of traffic" and offered filters that regime functionaries could use to "access specific communications of interest from mountains of data" (Coker & Sonne, 2011). The Nigerian government appears to have contracted the Cape Town-based Global Voice Group SA "to install a telecommunications device known as the Intelligence Signaling Management System (ISMS) to tap people's private conversations"; the same company is involved in the planned installation of a device management system in Malawi (Roberts et al., 2023, p. 110; Sackey & Mahama, 2010). Tendy Three, headquartered in Johannesburg, has installed a vehicle tracking system in Bulawayo in Zimbabwe (Munhende, 2021).

Snedai, which operates out of Abidjan, has provided a range of digital registration technologies to the government of Côte d'Ivoire (Hersey, 2022a), while Appmart Integrated, Barnksforte Technologies, and eGate Technology, based in Abuja, have supplied similar tools to Nigerian authorities (Macdonald, 2022n, 2023t, 2023w). V&V Nigeria, Israeli-owned but also based in Abuja, has provided spyware, seemingly sourced from Circles, to the Nigerian Police Force (Roberts et al., 2023, p. 51). Vestigio Technology Solutions, which has offices in Abuja, Kano, and Lagos, has received a contract to build a 'safe city' system in Kano (Roberts et al., 2023, p.

53). BioSIM, a Kenyan company, has sold biometric identification technology to some public schools in the country (Privacy International, 2019d). Tunisia's SIMAC has sold a biometric payroll management system to the government of Cameroon (Macdonald, 2024x).

North American Providers

North American suppliers of digital surveillance technology to African governments have only provided tools of mass surveillance.

As early as in the 1970s, the apartheid regime purchased computer equipment from IBM to populate South Africa's pioneering biometrics-based digital population register (Breckenridge, 2014, p.170–181). The Ugandan government has retained the services of Viisage (now L-1 Identity Solutions), headquartered in Littleton, Massachusetts, to implement and maintain a biometric voter registration system (*Business Wire*, 2001). Blue Coat Systems, a Sunnyvale, California-based cybersecurity company that Symantec bought in 2016, has sold deep packet inspection (DPI) technology, used to censor and surveil internet traffic, to the governments of Egypt (*News Press*, 2017), Kenya (*BBC*, 2013), Nigeria (*BBC*, 2013; Ogala 2014), and Sudan (Roberts, 2021, p.113). NetApp, which operates out of San Jose, California, has provided a similar DPI system to Tunisian authorities (Privacy International, 2019g). Egypt has purchased CCTV surveillance technology for its New Administrative Capital from Honeywell, the multinational conglomerate headquartered in Charlotte, North Carolina (*Reuters*, 2023). Malawian authorities have contracted Rockville, Maryland-based Agilist International (subsequently acquired by Infogix, headquartered in Naperville, Illinois) to deploy a device management system in the country (Roberts et al., 2023, p. 110). Dataminr, which operates out of New York City, has provided its social media

monitoring tools to the governments of Kenya, Nigeria, and South Africa (Roberts et al., 2023, p. 157).

Ottawa-based March Networks, the only Canadian company reported to have sold digital technology to African authorities, has supplied a similar CCTV surveillance system deployed on government-operated public transport in South Africa (*Canada Stockwatch*, 2009).

European Providers

African governments have procured mass surveillance technology from several European suppliers. Amsterdam-headquarted Gemalto—since 2019, when it was sold to the French multi-national Thales Group, known as Thales DIS (Digital Identity and Security)—has provided biometric voter registration systems to the governments of Benin, Algeria, Côte d'Ivoire, Gabon, Morocco, South Africa, and Tunisia. It has also sold digital identity technology to Cameroonian authorities and supplied other, unspecified, tools to the governments of the Democratic Republic of Congo, Niger, Nigeria, and Senegal (*ENP Newswire*, 2010; Macdonald, 2023h). According to allegations under investigation by French authorities, "Gemalto paid bribes or used other unfair channels like intermediaries or lobbyists to secure at least 10 contracts between 2015 and 2019 to produce different ID documents" for African governments (Macdonald, 2023h). The government of Nigeria has also acquired biometric technology from Hamburg-headquartered Dermalog Identification Systems GmbH (Roberts et al., 2023, Roberts et al., 2023, p. 55). Laxton, based in the Hague, has sold biometric identity registration technology to the governments of Malawi, Mozambique, Nigeria, and Zimbabwe (Lee, 2017b; Macdonald, 2023ad; Mayhew, 2017, 2018). The governments of Egypt, Guinea, Kenya, and Morocco have procured biometric identification products from Idemia (previously known as OT-Morpho and, prior to a merger, Safran), head-

quartered in the Paris suburb of Courbevoie. Tech5 and Innovatrics—which operate out of Geneva and London, respectively—have supplied analogous tools to Guinean authorities; the former is also involved in Mauritania's digital identity project (Burt, 2019c; Hersey, 2021b; 2022b; Opiah, 2024b). Ethiopia has purchased iris recognition technology from IrisGuard, headquartered in Milton Keynes (Macdonald, 2023n). Brussels-based Semlex, Coppernic, from Aix-en-Provence, Cambridge-headquartered Simprints, Mühlbauer, based in Roding in Bavaria, and Smartmatic, which operates out of London, have sold biometric identification technology to the governments of Côte d'Ivoire, Guinea, Mozambique, Uganda, and Zambia, respectively (Hersey, 2022a; Roberts et al., 2023, p. 128). CONTEC Global, which has offices in London and Lagos, provides biometric documents to the government of Burundi (CIPESA, 2022, p. 19). Margins Group, based in London, prints similar documents for the Ghanaian government (Macdonald, 2023j). Ultimaco, with head offices in Aachen and Campbell, California has provided a DPI system used by the government of Tunisia (Privacy International, 2019g). Travizory, headquartered in Neuchâtel, has sold biometric migrant entry gates to the government of Seychelles (Karapetyan, 2021a). It is not clear to what use the Egyptian government has put the unspecified "monitoring devices" it purchased from Nokia Siemens Networks—now Nokia Networks—an Espoo-headquartered subsidiary of Nokia Corporation (but at the time a joint venture with Siemens; Privacy International, 2019d; *Sputnik News*, 2016).

Other European companies have sold to African governments software used exclusively or mostly to target specific individuals and groups of people. Amesys, a subsidiary of Bull SAS, a computer company that operates out of Les Clayes-sous-Bois near Paris, supplied Eagle, its DPI system, to the governments of Libya—then ruled by Muammad Gaddafi—and Morocco; a

decade after Gaddafi's death in 2011 the former Amesys chief executive Philippe Vannier was charged in a Paris court with "complicity in acts of torture" committed by the regime (Al Jazeera, 2017a; Coker & Sonne, 2021; Lee, 2021; Privacy International, 2015b; Valentino-DeVries et al., 2011). Paris-headquartered Nexa Technologies later sold "an updated version of Amesys's software called 'Cerebro,' capable of real-time message or call tracing, to the government of Egypt's President Abdel Fattah al-Sisi" (*AFP*, 2021). French prosecutors have charged Nexa's head Olivier Bohbot and two other executives with "complicity in acts of torture and forced disappearances" in Egypt (*AFP*, 2021).

While DPI systems marketed by Amesys and Nexa are tools of mass surveillance used by governments to target specific regime opponents, Digivox, Gamma, Hacking Team, and Intellexa—also European companies—have provided African governments with spyware capable of infiltrating (only) individual devices. Rotterdam-headquartered Digivox, which specializes in "lawful and tactical interception systems, secure GSM communication, GPS tracking devices and voice logging," has sold its technology to the Nigerian government (Ogala, 2014). Frankfurt-based ATIS Huer; Trovicor, a Munich-headquartered former subsidiary of Siemens AG and Nokia Siemens Networks; and ETI A/S, a BAE Systems subsidiary that operates out of the Copenhagen suburb of Sundby, have provided surveillance systems to Moroccan and Tunisian governments (Privacy International, 2019g). Trovicor has also worked for the Ethiopian government (Roberts et al., 2023, p. 148). Gamma Group, a technology company headquartered in Bologna, has two branches—Gamma International Ltd in Andover, England and Gamma International GmbH in Munich (the latter later known as Vilicius Holding GmbH) —that develop FinFisher/FinSpy spyware marketed by Lench IT Solutions plc. Detected and examined by the

University of Toronto's Citizen Lab, FinFisher/FinSpy takes advantage of vulnerabilities in software update systems to covertly install malware that monitors computer use (Marquis-Boire et al., 2013). In Africa it has been used by the governments of Egypt (Matsiko, 2015; Perlroth, 2013; Valentino-DeVries et al., 2011), Ethiopia (*AFP*, 2014; Tekle, 2013; Vermeer, 2014), Nigeria (Ogala, 2014), and Uganda (*Canadian Press*, 2015; Marks, 2019; Oluka, 2015). In addition, BlackOasis, likely an external nation-state threat actor, has deployed FinFisher/FinSpy in Angola, Libya, and Tunisia (*Business Wire*, 2017). Other FinFisher/FinSpy deployments have taken place in Gabon, Kenya, and Morocco (Marczak et al., 2015). Before it ceased operations in 2019, the Milan-based Hacking Team developed remote control systems (RCSs) Da Vinci and Galileo —the subject of another Citizen Lab investigation (Marczak et al., 2014)—which enabled covert collection of emails, text messages, phone call history, address books, and browser search history; keystroke logging; recoding of audio from both in-person conversations and phone calls as well as audio and video from Skype calls; device camera activation; and location monitoring through device GPS access on devices running a range of operating systems: Android, BlackBerry, iOS, Linux, OS X, Symbian, and Windows (on both desktop and mobile). Hacking Team sold this spyware to governments in Egypt (Gibbs, 2015; Loveluck, 2014; Ouma, 2015), Ethiopia (*All Africa*, 2015; Amahazion, 2015; Peterson, 2015), Libya (Gibbs, 2015), Morocco (Gibbs, 2015; Hajjaj, 2019), Nigeria (where, unusually, the governor of the Bayelsa state, rather than federal authorities, procured Hacking Team's software; *BBC*, 2015; Ogala, 2014, 2015a), South Sudan (*Al Jazeera*, 2017a, 2017b), and Sudan (Gibbs, 2015). In 2014 and 2015, the governments of Algeria, Namibia, and Uganda were engaged in negotiations with Hacking Team, but it is unclear if they obtained its spyware (Finnan, 2015; Katusiime, 2021; Links, 2018). Hacking Team declined

to sell Galileo to Kenya (Finnan, 2015). The otherwise unknown Tactical Devices, apparently located in Switzerland, has supplied unspecified telecommunications interception equipment to the government of Ghana (Roberts et al., 2023, p. 21). Similarly limited is the information about Total Secure Defence, apparently based in the United Kingdom and responsible for supplying IMSI catchers to the Moroccan government (Roberts et al., 2023, p. 91). Athens-headquartered Intellexa appears to control Cytrox, which develops Predator spyware that takes advantage of operating system vulnerabilities to infiltrate Android and iOS and appears to have been used by the governments of Côte d'Ivoire, Egypt, Ghana, and Madagascar (*NF News*, 2022b; Roberts et al., 2023, p. 21). In addition, Intellexa's owner Tan Dilian has sold Predator to Sudan's Rapid Support Forces, which were at that time part of the Sudanese Armed Forces (Black, 2022).

Israeli Providers

The large number of Israeli developers of digital surveillance technology procured by African governments merits its own section. Almost all of these tools have been used for targeted surveillance.

Intellexa's Tan Dilian had previously founded Circles, which has been investigated by Citizen Lab (Marczak et al., 2017b) and exploits vulnerabilities in the Signaling System 7 protocol used in 2G and 3G mobile networks. It has been used in Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria (including by state governors), Zambia, and Zimbabwe (where three different Circles platforms have been detected; Dadoo, 2021). In 2014 Circles was sold to Francisco Partners, which at that time also owned NSO Group, the Herzliya-headquartered cyber-intelligence firm that develops Pegasus spyware.

Pegasus, also inspected by Citizen Lab (Marczak et al., 2021), takes advantage of mobile operating system vulnerabilities to enable covert and remote installation on devices running Android and iOS using zero-click exploits. It can read text messages, record calls, collect passwords, track device locations, access device cameras and microphones, and harvest information from apps. Pegasus infections have been detected in in Algeria, Burundi, Côte d'Ivoire, Egypt (Allison, 2018; *NF News*, 2021b), Ghana (*NF News*, 2022c), Kenya, Libya (Allison, 2018), Morocco (Chown, 2020; *M2 Presswire*, 2022; Neugeboren, 2020; *NF News*, 2021b), Rwanda (*Deutsche Presse-Agentur*, 2021; Kirchgaessner & Taylor 2022), South Africa (Allison, 2018; *Deutsche Presse-Agentur*, 2021; Gavaza, 2021), Togo, Tunisia (Allison, 2018), and Uganda (Dahir, 2021; Katusiime, 2021; Marks, 2019; *NF News*, 2021d). The governments of Ghana (*NF News*, 2022c), Morocco (Chown, 2020; *M2 Presswire*, 2022; Neugeboren 2020; *NF News*, 2021b), Rwanda (*Deutsche Presse-Agentur*, 2021; Kirchgaessner & Taylor 2022), and Uganda (Katusiime, 2021; Marks, 2019) are known to have purchased Pegasus from NSO Group; other infections in individual countries may not be the work of their governments, especially given the spyware's use for foreign espionage as well as domestic surveillance. In particular, the Moroccan intelligence service appears to have used Pegasus in Algeria and France, where the mobile phones of President Emmanuel Macron, former premier Édouard Philippe, and 14 ministers were apparently infected (Chown, 2020; *M2 Presswire*, 2022; Neugeboren, 2020; *NF News*, 2021b); Rwanda may have spied on South Africa's president Cyril Ramaphosa and several prominent Ugandans, including the former prime minister Ruhakana Rugunda (*Deutsche Presse-Agentur*, 2021; Gavaza, 2021; Kirchgaessner & Taylor 2022); while the Ugandan government is likely responsible for the infection of devices used by American diplomats (*NF News*, 2021d).

Cognyte Software, earlier Cognyte Technology, also operates out of Herzliya. A subsidiary of the Melville, New York-headquartered analytics company Verint Systems, Cognyte "sells all manner of spy tools, including one that can locate any individual to the nearest cell tower with just their telephone number" (Brewster, 2020), which appears to describe an IMSI catcher. In Africa, it has had contracts with the governments of Angola, Botswana, Eswatini, Ethiopia, Mozambique, Kenya, Nigeria, South Sudan, and Uganda. South Sudan's deployment of Cognyte/Verint's tools is intended "for eavesdropping on opponents of the regime"; elsewhere, they have been used "to check sexual inclinations via Facebook […] for persecuting the [LGBTQ+] community" (Shezaf, 2018). In contrast, Botswana and Mozambique appear to have contracted with Verint for non-political purposes, to contain wildlife poaching and civilian abductions, respectively (Shezaf, 2018).

The last major Israeli provider of targeted surveillance tools to African governments, Elbit Systems, a defense electronics company headquartered in Haifa, has sold the Hermes 450 surveillance system to Botswana (Marczak et al., 2017b; *Sunday Standard*, 2014, 2018) and unnamed spyware to Nigeria (*BBC*, 2013; Ogala, 2014; Shezaf, 2018), while its subsidiary Cyberbit has provided Ethiopia and, possibly, Zambia with access to its PC Surveillance System (in 2017 renamed PC 360) used to infect and extract data from personal computers of users who have opened links to malicious websites (*All Africa*, 2017a; Marczak et al., 2017a; Shezaf, 2018).

In addition, the Bnei Zion-headquartered WebintPro has provided a "media monitoring and management" system to the Kenyan government (Privacy International, 2017a) and Pangea IT, based in Herzliya, has sold transaction monitoring software to Madagascan authorities (Hersey, 2020a). Black Cube, which operates primarily out of Tel Aviv (in addition to secondary

headquarters in London and Madrid), allegedly "hacked the emails and medical records of Muhammadu Buhari" when he was a candidate for Nigeria's presidency; a private intelligence agency, Black Cube is likely to have purchased technology used in the operation from another company (*Sputnik News*, 2018). Also in Nigeria, Tel Aviv-based MPD Systems apparently provided the government with a C4i (Command, Control, Communications, Computers, and Intelligence) system (Ogala, 2015b). The use of Reign, zero-click-exploit spyware developed by QuaDream, headquartered in Ramat Gan, has been detected in Ghana (Marczak et al., 2023). Petah Tikva-based Cellebrite has provided its Universal Forensics Extraction Devices (UFEDs) to Ghanaian, Nigerian, Senegalese, and Ugandan authorities (*All Africa*, 2024; Popoviciu, 2023; Roberts et al., 2023, pp. 50, 72). Mauritian authorities have contracted with ECI Telecom, also headquartered in Petah Tikva, to surveil political opponents (Khan, 2019). Team Jorge, a group of Israeli hackers, has been active in Nigeria, although it is unclear if it has operated at the behest of the country's government (Roberts et al., 2023, p. 149).

Chinese Providers

Four Chinese companies complete the list of major suppliers of digital surveillance technology used by African governments. They offer mass surveillance tools but have on occasion worked with African governments to target individuals.

Huawei, the Shenzhen-headquartered technology conglomerate, has sold facial recognition-enabled 'smart city' CCTV mass surveillance systems in Algeria (*AFP*, 2019), Cameroon (Macdonald, 2024b), Egypt (Allen, 2019), Kenya (*ENP Newswire*, 2016; Van Der Made, 2021), South Africa (Roberts, 2021, p. 135), and Uganda (Mutisi, 2022; Woodhams, 2019). The governments of Burkina Faso (Van Der Made, 2021) and Mauritius (Robertson, 2020) have engaged

in negotiations with Huawei to purchase these systems. Huawei complements its 'smart city' offerings with data centers that collate "all data and information from government and sectors of the economy," including those from telecoms, surveillance cameras, and financial institutions (Ndlela, 2020b). It has built such data centers in Cameroon (*NF News*, 2021a; Van Der Made, 2021); Kenya (*ENP Newswire*, 2016; Van Der Made, 2021), Malawi (Roberts et al., 2023, p. 105), Senegal, Zambia (*NF News*, 2021a), and Zimbabwe (Ndlela, 2020b). According to a classified report written by Algerian and Ugandan intelligence services, Huawei's "advanced system […] provides one of the best surveillance applications" (Marks, 2019). In addition, the company has intercepted the online communications of government opponents in Uganda and Zambia (Latham, 2020; Marks, 2019; Woodhams, 2019).

Three other Chinese companies specialize in video surveillance. CloudWalk Technology, a Guangzhou-based developer of facial recognition software, has built an extensive system of facial recognition-enabled CCTV surveillance cameras in Zimbabwe, where it trains its software on Black faces to enhance the accuracy of this technology (Chimhangwa, 2022; Gross et al., 2019). The state-owned Hikvision, headquartered in Hangzhou, has supplied facial recognition cameras in South Africa (*NF News*, 2019). Along with Huawei, both companies are also involved in the construction of Zimbabwe's National Data Centre (Ndlela, 2020b).

ZTE, the partially state-owned technology company headquartered in Shenzhen, "provided technology for Libya's monitoring operation" before the collapse of the Gaddafi regime (Coker & Sonne, 2011); it has also built a 'safe city' system for the Nigerian government and ZSmart, a comprehensive "customer management system" that collates personal information, financial records, phone call metadata, text message content and metadata, and device locations

of all users of Ethio-Telecom, until 2022 Ethiopia's only telecom provider, in addition to enabling the recording of phone calls (HRW, 2014, pp. 36–37; Roberts et al., 2023, p. 53). Hytera Communications, also based in Shenzhen and partly owned by the Chinese state, has been involved in a planned 'smart city' project in Nigeria (Roberts et al., 2023, p. 53).

Other Asian and Asia-Pacific Providers

Australian, Emirati, Indian, Malaysian, and Taiwanese companies have only been linked to one instance of government digital surveillance each. They join two South Korean providers of surveillance tools. They have mostly provided African governments with biometric registration technology used for mass surveillance.

BioEnable Technologies, headquartered in Magarpatta City in Maharashtra, has been involved in Burkina Faso's biometrics-based national identity register (Burt, 2023e). Spyware developed by the Indian hacker group Donot Team has been used to surveil a human rights activist in Togo (*M2 Presswire*, 2021). The government of Guinea has contracted with the Kuala Lumpur-based Datasonic Group Berhad to supply it with biometric identification system (Hersey, 2022b). KT Corporation, based in Seongnam near Seoul, has built a "digital national identification data center," which includes "a fingerprint identification and management system, a network control system, and a resident registration website" for the government of Tanzania (*PR Newswire*, 2018). Seoul-headquartered DOHWA Engineering and Dubai Holding, based in Dubai and controlled by Dubai's ruler Sheikh Mohammed bin Rashid al-Maktoum, have been involved in 'smart city' projects in Nigeria (Roberts et al., 2023, p. 53). Ghanaian authorities have deployed unspecified network monitoring technology supplied by Decision Group, which operates out of Taipei (Roberts et al., 2023, p. 21). Australia's Mi Marathon Resources, which

may or may not be connected to the Sydney-headquartered miner Marathon Resources, has provided Nigerian authorities with a Verint IMSI catcher and the Fiber Optic Landing Solution, which enables backend access to fibre-optic cables (Roberts et al., 2023, p. 50).

Supplement 3: Instances of government digital surveillance in Africa

Most African countries are reported to have used digital surveillance technology. This supplement describes all the instances of such government digital surveillance catalogued in Supplement 3. The instances are arranged per country, with the countries listed in alphabetic order.

Algeria

The government of Algeria has procured Gemalto's biometric voter registration system (*ENP Newswire*, 2010*)* and biometric passports (Lee, 2017a) in addition to installing a Huawei-operated video and cyber surveillance system (*AFP*, 2019; Marks, 2019; Putsch, 2019). It has also secured training, funded and provided by the European Union, for the country's police, who learned "how to use fake accounts to gather information on social media (*Reuters*, 2020). SIM card registration, of the capture-and-share type,[1] is mandatory in Algeria (GSMA, 2021, Roberts et al., 2023, p. 16; Privacy International, 2019a).

In addition to these instances of actual surveillance, in the mid-2010s Algeria appeared to be in the process—the outcome of which is unknown—of acquiring Hacking Team's RCS Galileo (Finnan, 2015). The Moroccan intelligence services, rather than Algeria's government,

---

[1] The models of SIM card registration vary. Most African governments mandate telephony providers to collect and store user data, which state agencies access on a case-by-case basis. In Algeria, Burundi, the Gambia, Nigeria, Sierra Leone, Tunisia, and Zimbabwe, telecoms transmit full or partial data of all users to governments. Egyptian, Kenyan, Liberian, Senegalese, Tanzanian, Ugandan, and Zambian authorities also require that providers validate user identification credentials against central government databases (GSMA, 2021, p. 16).

appear to have been responsible for the Pegasus infections in the country (Allison, 2018; Marczak et al., 2018).

Angola

Capture-and-store SIM card registration is mandatory in Angola (GSMA, 2021, p. 16; Privacy International, 2019a). Media have reported the government's use of social network information collection and the existence of a Verint contract in the country; these reports may or may not refer to the deployment of Cognyte's social media surveillance technology (Lee, 2014; Shezaf, 2018). Angolan authorities first deployed digital surveillance technologies to target political opponents in the 1990s, when they acquired telecommunications surveillance equipment from an unknown French company; this "equipment enabled Luanda's intelligence agency to listen to GSM cell phones and track down the coordinates of satellite telephones" (*M2 Presswire*, 2015; Verde, 2021, p. 3). A separate telecommunications surveillance system was set up in the 2010s (Verde, 2021, p. 4). Rafael Marques, a prominent Angolan journalist, has had his computer equipment infected; the vector of this attack is unknown (Lee, 2014). In addition, BlackOasis has used FinSpy in Angola (*Business Wire*, 2017).

Benin

The government of Benin has introduced biometric national identity cards—necessary for access to some government services (Macdonald, 2023a; Mascellino, 2023)—created a biometric civil registration system (Macdonald, 2024w), purchased a biometric voter registration system from Gemalto (*ENP Newswire*, 2010), and instituted compulsory SIM card registration that involves the collection of biometrics (fingerprints; *NF News*, 2021c; GSMA, 2021, p. 16; Privacy International, 2019a).

Botswana

The Botswana Telecommunications Authority introduced mandatory capture-and-store SIM card registration in 2008 (GSMA, 2021, p. 16; Motlogelwa, 2008; Privacy International, 2019a). Batswana civil society activists have linked this initiative, "a monster especially to civil society leaders and other opinion leaders," to "a lot of cases of trade unionists and some ruling party politicians whose cell phone conversations were being tapped" (Motlogelwa, 2008). The country's government issues biometrics-backed national identity cards and passports (Macdonald, 2024l). In the early 2020s, it also deployed CCTV surveillance of unknown origin (Mutisi, 2022).

Botswana's Directorate of Intelligence and Security Services procured spyware from Elbit Systems and Circles as early as in 2014 and 2015, respectively (Dadoo, 2021; Marczak et al., 2017b; *Sunday Standard*, 2018). The surveillance and jamming technology obtained from Elbit was reportedly used to conduct "electronic warfare" against the media (Marczak et al., 2017b; *Sunday Standard*, 2014, 2018).

Although the government has contracted with Verint, Cognyte tools were apparently used "in a campaign against poaching" (Shezaf, 2018). In addition, by 2020 Botswana was "building in safeguards and a strong oversight and transparency mechanism with its criminal procedures and evidence (controlled investigations) bill, which seeks to prohibit state surveillance abuse" (*The Namibian*, 2022).

Burkina Faso

Burkina Faso introduced mandatory SIM card registration, of the capture-and-store type, in 2008 (GSMA, 2021, p. 16; Privacy International, 2019a). The country's government has also

made plans to introduce a biometrics-based digital identity register, using tools purchased from BioEnable Technologies (Burt, 2023e), and biometric visas (Macdonald, 2023e). In 2021, "Huawei was negotiating a USD 80 million contract involving 800 km of optical fibre and 900 surveillance cameras for the 'Smart Burkina'" (Van Der Made, 2021); the outcome of these negotiations is unknown.

Burundi

SIM card registration, of the capture-and-share type, has been mandatory in Burundi since 2014 (CIPESA, 2022; GSMA, 2021, p. 16; Privacy International, 2019a). The country has introduced biometric passports and biometric driver's licenses (CIPESA, 2022, p. 19). A government has used NSO's Pegasus to infect devices in Burundi, but it may not have been the country's own (Dahir, 2021).

Cameroon

The government of Cameroon has introduced a mandatory biometrics-based national identity system, but many of those who provided their data have received no identity cards (produced by Thales), with adverse consequences. Interviewed registrants have described their experiences thusly: "The risk of traveling without an ID card especially in the crisis-hit North West and South West Regions is enormous. Even with this application receipt, security forces will still disturb you and force you to pay money" (Macdonald, 2022d). Without a card, "one cannot register for a public exam, conveniently travel from one town to the other, carry out financial and banking transactions such as receiving international money transfers, buy and register a SIM card, apply for a passport, open a bank account, register a business, or get a driver's license" (Macdonald, 2022d). Cameroonian visa applications require submission of biometric data, al-

though the enrollment portal has been down for long stretches of time (Macdonald, 2023e). The government started collecting biometric data for the country's voter register in 2024 (Macdonald, 2024a); enrollment reached 8.1 million people later that year (Macdonald, 2024ab). The Ministry of Public Service and Administrative Reforms has deployed a biometric payroll system to manage payments to civil servants (Macdonald, 2024x).

Cameroon also has mandatory SIM card registration, of the capture-and-store type (GSMA, 2021, p. 16; Privacy International, 2019a). China Shenyang International Economic & Technical Cooperation Corporation has built a Huawei data centre for Cameroon's government (*NF News*, 2019). The centre may be part of a Huawei 'safe city' project that involves the installation of 5,000 facial recognition-equipped CCTV cameras across the country (Macdonald, 2024b).

Central African Republic

The government of the Central African Republic mandated capture-and-store SIM card registration in 2014 (GSMA, 2021, p. 16; Privacy International, 2019a). Registration in the country's biometric voter register began in 2024 (Macdonald, 2024z).

Chad

SIM card registration—of the capture-and-store type—is mandatory in Chad (GSMA, 2021, p. 16; Privacy International, 2019a).

Democratic Republic of the Congo

The Democratic Republic of the Congo introduced mandatory capture-and-store SIM card registration in 2012 (GSMA, 2021, p. 16; Privacy International, 2019a). The country's government also started issuing biometric identity cards in 2023 (McCurdy, 2023); the cards are re-

quired for voter registration but proved difficult to obtain ahead of the 2023 presidential elections, preventing many Congolese from casting ballot (Macdonald, 2023ab). The government has additionally procured unspecified technology from Gemalto (Macdonald, 2023h). In 2016 it installed a CCTV system in Kinshasa (Tungali, 2021).

Republic of the Congo

The government of the Republic of the Congo has instituted mandatory capture-and-store SIM card registration (GSMA 2021, 16; Privacy International 2019a). It has also intercepted phone communications of the opposition presidential candidate and alleged coup plotter General Jean-Marie Michel Mokoko (*Africa News*, 2021).

Côte d'Ivoire

In Côte d'Ivoire, the government has introduced a biometrics-based national identity system, which includes the Carte nationale d'identité produced by Semlex, also responsible for data collection. By 2022 over four million Ivorians had provided their data (Hersey, 2020a, 2022a). The national health insurance scheme has a separate, and compulsory, biometrics-based digital register, in place since 2019 and handled by Abidjan-based Snedai (CIPESA, 2022, p. 32; Hersey, 2022a). Ivorian authorities have also mandated capture-and-store SIM card registration (GSMA, 2021, p. 16; Privacy International, 2019a), procured Gemalto's biometric voter registration system (*ENP Newswire*, 2010), installed CCTV surveillance technology (Mutisi, 2022), and obtained funding from the European Union for "a biometric identification system in Ivory Coast that would accelerate the repatriation of migrants from Europe" (*Reuters*, 2010).

The two instances of targeted digital surveillance in the country, involving NSO's Pegasus CI4 and Intellexa's Predator CI5, may or may not be the work of the Ivorian government (Allison, 2018; Marczak et al., 2018; *NF News*, 2022b).

Egypt

Successive Egyptian administrations' use of digital surveillance has been extensive. Activists in the country have been "arrested for starting Facebook pages or writing critical Facebook posts," while journalists live "in constant fear" because "everything is monitored" (*News Press*, 2017).

Prior to the Arab Spring, the Hosni Mubarak regime used Gamma's FinFisher/FinSpy, which it had purchased for some USD 560,000, to intercept dissidents' Skype calls (Matsiko, 2015; Perlroth, 2013; Valentino-DeVries et al., 2011). It also required internet cafe operators to collect and share with the Ministry of the Interior personal data of internet users (Privacy International, 2019c).

Shortly after Abdel Fattah al-Sisi came to power in 2014, his government published a tender for a "social networks security hazard monitoring system" to be used to surveil Egyptians' use of Facebook, Twitter, Viber, and WhatsApp (Loveluck, 2014). In subsequent years, the al-Sisi regime also contracted with Blue Coat, Hacking Team, and Nokia Siemens Networks (Gibbs, 2015; Loveluck, 2014; Marczak et al., 2014; Ouma, 2015; *Sputnik News*, 2016); Blue Coat's DPI system appears to have been used "to interfere with platforms including Tor browser, which allows anonymous browsing; the encrypted messaging app Signal; and Secure Shell, a protocol to provide secure communication channels" (*News Press*, 2017). Starting in 2016, the NilePhish attack targeted over 110 activists and journalists (*News Press*, 2017); it appears to have

originated in Egypt's Ministry of Communications and Information Technology and the General Intelligence Service (Malsin & El-Fekki, 2019; Scott-Railton et al., 2017). The government has also procured spyware from Nexa Technologies (*AFP*, 2021; Privacy International, 2019c) and, possibly, Intellexa and NSO Group; among those infected with Pegasus has been Egypt's prime minister Nostafa Madbouly (Allison, 2018; Marczak et al., 2018; *NF News*, 2022b).

Egyptian authorities have complemented these targeted attacks with an extensive apparatus of mass digital surveillance. Capture-and-validate SIM card registration has been mandatory in the country since 2014 (GSMA, 2021, p. 16; Privacy International, 2019a). Also in 2014, the government contracted OT-Morpho (later Idemia) to produce national biometric identity cards (Privacy International, 2019c). It has also deployed CCTV surveillance systems procured from Huawei and Honeywell; the latter has built a system of "more than 6,000 surveillance cameras [that] keep watch over" (*Reuters*, 2023) residents of the country's New Administrative Capital. According to Access Now's policy manager, Maria Fatafta, "[t]he Egyptian government is selling its New Administrative Capital as a smart city where people can have a better life quality—but in reality, they are building a surveillance city" (*Reuters*, 2023). "Planting surveillance cameras across the city gives authorities an unparalleled ability to police public spaces and crack down on citizens who wish to protest or exercise their right to peaceful assembly," she observes (*Reuters*, 2023). France's Orange was awarded a contract worth USD 135 million dollars to build a data centre needed to process data from the New Administrative Capital's surveillance system (Swinhoe, 2023). Hurghada and Sharm El-Sheikh airports have deployed a biometric identity system "to better monitor the activities of employees, and automate their entrance and exit of the airport" (Privacy International, 2019c). The use of these digital tools is bolstered by "random

searches of phones and laptops on the street, as part of a campaign to thwart online dissent" (Malsin & El-Fekki, 2019).

Eswatini

The Swaziland Communications Commission introduced mandatory capture-and-store SIM card registration in 2018 (*All Africa*, 2018; GSMA, 2021, p. 16). Allegations of government surveillance of public figures followed; the House of Assembly Speaker Themba Msibi expressed "concerns as at times calls sound hollow, making one suspect that a third party could be listening in" (*All Africa*, 2018). The Swazi government has also had a contract with Verint (Shezaf, 2018).

Equatorial Guinea

In Equatorial Guinea, the government has used Circles to target opponents since 2013 (Dadoo, 2021; Marczak et al., 2017b). It has also instituted mandatory capture-and-store SIM card registration (GSMA, 2021, p. 16) and a biometric register of public servants (Macdonald, 2023f).

Eritrea

Eritrea also has mandatory capture-and-store SIM card registration (GSMA, 2021, p. 16). The country's government has additionally implemented unspecified "monitoring and checks on Internet use inside the country" (Stevis, 2015).

Ethiopia

The government of Ethiopia has launched the Fayda biometric national identity system, which provides both "a legal identity and a functional identity" and "will be layered onto the functional ID systems that are used for various purposes, including the residence credential

which has typically been used in day-to-day life by Ethiopians to identify themselves" (Burt, 2022a). As of 2023, the use of Fayda is mandatory for all transactions with financial institutions (Macdonald, 2023g; McConvey, 2023). The Ministry of Education has replaced student IDs with Fayda (McConvey, 2023), while the Ministry of Health has made plans for a separate Digital ID for Health system, a national patient registry, which it intends to integrate with Fayda (Burt, 2023a). However, only eight million Ethiopians had registered as of 2024 (Macdonald, 2024ac). Ethiopian authorities have also contracted with IrisGuard to collect iris biometrics from recipients of government benefits (Macdonald, 2023n).

Capture-and-store SIM card registration is mandatory in the country (GSMA, 2021, p. 16). According to the Human Rights Watch, "[I]nformation gleaned from telecom and Internet sources is regularly used against Ethiopians arrested for alleged anti-government activities" (HRW, 2014, p. 3). Thanks to ZTE-provided ZSmart, "Ethiopian security officials can access the records of all phone calls made inside Ethiopia with few restrictions" (HRW, 2014, p. 36). The same applies to subscriber information and text messages. Ethio-Telecom has also installed a DPI system used to block Tor connections in the country (*African Press Organization*, 2021).

The Ethiopian government has deployed spyware provided by Gamma, Hacking Team, and Cyberbit against its opponents. Gamma's FinFisher/FinSpy was used against members of the opposition movement Ginbot 7 located in Norway, the United Kingdom, and the United States (*AFP*, 2014; Tekle, 2013; HRW, 2014, pp. 73–74). The targets of Hacking Team's RCS worked for the US-based Ethiopian Satellite Television; Hacking Team considered the Ethiopian authorities, which it charged USD 1 million for its services, too "reckless and clumsy" to use the surveillance tools it provided (*All Africa*, 2015; Amahazion, 2015; Marczak et al., 2014, 2015; Pe-

terson, 2015). The PC Surveillance System (or PC 360) obtained from Cyberbit was used to infiltrate the devices of no fewer than 43 different people, including Oromo activists and scholars, in 20 countries (*Al Jazeera*, 2017a; *All Africa*, 2017a; Marczak et al., 2017a; Shezaf, 2018). The government has also apparently purchased unspecified communications surveillance equipment from Trovicor (Roberts et al., 2023, p. 148).

During the conflict in Tigray, federal troops used "high-tech surveillance drones bought from China […] to track and destroy targets across the region" (Bariyo, 2020). Ethiopian police have also deployed drones to patrol in major cities (*Addis Standard*, 2025). In addition, the Ethiopian government and the US National Security Agency have jointly built "a network of clandestine eavesdropping outposts designed to listen in on the communications of Ethiopians and their neighbors across the Horn of Africa in the name of counterterrorism" (Nurse, 2017).

Gabon

The government of Gabon has purchased a Gemalto biometric registration system (or, possibly, two of them), variably described as intended for the creation of a national identity register or a voter register (*ENP Newswire*, 2010; Macdonald, 2023h, 2023i). As of 2023, the national identity register had not been implemented, although "plans [were] advancing in terms of setting up the equipment and training of operational personnel," undertaken by Thales (which had taken over Gemalto; Macdonald, 2023i). Registration began in 2025 (Macdonald, 2025a). The National Social Security Fund of Gabon initiated a biometric enrollment process for retirees in 2018 (CIPESA, 2022, p. 28). Capture-and-store SIM card registration is mandatory in the country (GSMA, 2021, p. 16).

Gabon has also seen deployment of Gamma's FinFisher/FinSpy (Marczak et al., 2015).

The Gambia

The Gambian government has also introduced mandatory SIM card registration, of the capture-and-share type, despite civil society concerns. “I do not have any trust in the current government and therefore I consider it unsafe for me to register my SIM card. They can do anything; they can go to any extent just to implicate people,” a Gambian interviewed by the *Agence France-Presse* at the time of registration in 2012 noted (*AFP*, 2012; also GSMA, 2021, p. 16). The government has also launched a biometric civil registry and national health insurance scheme (Macdonald, 2022p; Mascellino, 2023). By 2024, it had collected biometric data from 1.17 people out of the population of 2.71 million (Macdonald, 2024p).

Ghana

SIM card registration, of the capture-and-store type, is mandatory in Ghana (GSMA 2021, 16). Following the introduction of Ghana Card, issued as part of the country’s biometrics-based national identity register and printed by Margins Group, the government further mandated that Ghanaians re-register their phone subscriptions and link them to their identity cards (Hersey, 2022h; Macdonald, 2022f, 2023j), although as of 2022 5.7 SIM cards in operation, a quarter of the total number, had not been registered (Hersey, 2022f). 1.9 million of those cards had service disconnected that year before their holders completed registration (Macdonald, 2023j). Ghanaians with the means to do so can pay a fee to submit their fingerprints through a self-service mobile app (Macdonald, 2022e). 17.9 million Ghanaians had completed registration by 2024; the same year, authorities began issuing the Ghana Card numbers at birth (Macdonald, 2024g). The Ghana Card registry has been used to audit the civil service and identify ‘ghost workers’ (Macdonald, 2022a). Presentation of the card “has become mandatory for many transactions [as] a

trustworthy ID credential which is used as the single source of truth for identity proofing" (Macdonald, 2023k). The country's Electoral Commission has also made plans to stop accepting identity documentation other than Ghana Card during voter registration, making provision of biometrics a prerequisite to voting despite the inaccuracy of the system, which incorrectly identified some voters during the 2022 district elections (Macdonald, 2023c, 2023j, 2023l). The National Health Insurance system has meanwhile started collecting biometric data from registrants (Macdonald, 2023m). It has also proposed the introduction of Ghana Cards for children (Macdonald, 2024g). Ghanaian authorities have also installed CCTV surveillance, which includes a Huawei-powered 'smart city' project being implemented in multiple locations across the country, used Cellebrite's UFED, and deployed unspecified network monitoring technology provided by Decision Group (Roberts et al., 2023, pp. 72, 74). In 2024, the government installed biometric entry gates at Kotoka International Airport (*Ghana Today*, 2024). Ghana has received EU funding for a border surveillance project (Roberts et al., p. 148).

In 2015, the government paid NSO EUR 8 million to infect 25 targets with Pegasus (*NF News*, 2022c). It also appears to have acquired Intellexa's Predator and unspecified telecommunications interception technology provided by Tactical Devices (Roberts et al., 2023, p. 21). Citizen Lab has detected QuaDream's Reign in Ghana, although it is not clear if the spyware has been deployed by the country's government (Marczak et al., 2023).

Guinea

Guinea has launched a national identity register, which includes face, fingerprint, and iris biometric data collected using technology provided by Tech5 (Hersey, 2022b). The country's government has also used Idemia equipment to capture biometric data of the recipients of a cash

transfer program (Hersey, 2020b). A separate system contains the biometrics of government scholarship recipients (Macdonald, 2024c). Capture-and-store SIM card registration is mandatory in Guinea (GSMA, 2021, p. 16). Cybercafe operators are also required to identify users (CIPESA, 2022, p. 28). The government's future plans include a land management project, undertaken as part of a profit-sharing agreement with Datasonic Group Berhad, and a criminal identification system to be supplied by Innovatrics, both of which involve biometric data collection (Hersey, 2022b).

Guinea-Bissau

Guinea-Bissau has introduced biometric identity cards (Mascellino, 2023). The country uses the capture-and-store model of SIM card registration (GSMA, 2021, p. 16).

Kenya

In 2018, the Kenyan government announced the creation of Huduma Namba, a national population register including "GPS coordinates for home addresses, fingerprints, hand and earlobe geometry, retina and iris scans, and voice samples" (Mayhew, 2019b). By 2019, biometric data had been collected, using equipment from Idemia, from 8 million people (Burt, 2019a). Kenya's High Court stopped Huduma Namba data collection, which it ruled violated the Data Protection Act, two years later (Burt, 2021). Kenyan civil society organizations subsequently launched legal action against Idemia in France, claiming that Huduma Namba "continues exclusion against marginalized communities who face barriers to enroll," while its "centralized database lacks sufficient checks and balances and is at risk of exploitation, such as for surveillance" (Hersey, 2022e). Although Huduma Namba was originally promoted as a public service delivery tool, in 2022 the Kenya Revenue Authority asked asked parliament for permission to access

Huduma Namba data (Macdonald, 2022h), a move followed by the introduction of fees for compulsory identification documents described as "exorbitant and unaffordable" (Macdonald, 2023q) and reduction of document validity period that according to the government "has nothing to do with revenue generation as some citizens have claimed" (Macdonald, 2024d). A year later, the new William Ruto administration replaced Huduma Namba with Maisha Namba, which will also take the place of birth certificates and "be used for death registration […] identify verification in mobile transactions [and] access to both public and private sector services to cut fraud" (Macdonald, 2023p). The new "population register will integrate Kenya's existing databases of citizens and refugees" and include the Maisha Card, the replacement for existing national identity cards. Maisha Namba enrollment is, in contrast to Hudumba Namba, optional (Macdonald, 2023p). However, unlike previous identity cards, issued free of charge, Maisha Card will command a fee of KES 1,000 (Mbuthia, 2023). The Ruto administration has stated its intention to retain data collected for Huduma Namba: "We will not go back to Kenyans for biometrics because we will use the existing database," a government minister has said (Burt, 2023c). Civil society groups have warned "of the possibility of discrimination and the erosion of privacy given what they consider to be a lack of the steps needed to reform and upgrade the national identification system" (Burt, 2023d). By 2024, the government had issued a million Maisha cards (Macdonalrd, 2024e). Legal challenges led to repeated suspensions of Maisha Card issuance (Burt, 2023b, 2024a; Muriuki, 2024).

A separate biometric voter register, built on technology provided by Idemia (at that time called OT-Morpho), was first used in the 2017 elections (Privacy International, 2019d). The National Hospital Insurance Fund (NHIF) has introduced another biometrics-based register of those

who access health services in the country; in 2021, several hundred hospitals sued NHIF "in a dispute over the requirement to install equipment to biometrically register and verify patients and submit e-claims for payments [because] the sudden introduction of the system [was] preventing people from accessing healthcare" (Macdonald, 2021a). The National Police Service Information Management System contains biometric and other data of Kenyan officers collected starting in 2019 (Mayhew, 2019b). The Ministry of Education has its own digital register, of students, the National Education Management Information System, or NEMIS (Privacy International, 2019d). Some Kenyan schools have reportedly used iris-scanning technology provided by BioSIM to track student attendance (Privacy International, 2019d). The Kenyan government also issues biometric passports; as of 2022, Kenyans need the "new East African Community (EAC) biometric passports if they want to be able to leave the country" (Macdonald, 2022g). In 2022, the government introduced microchip-equipped digital vehicle license plates that "allow law enforcement agencies to track vehicles and enable the Kenya Revenue Authority to track tax evaders" (Wanjala, 2022).

Huawei CCTV surveillance 'safe city' systems were installed in Mombasa and Nairobi in 2016 (*ENP Newswire*, 2016). The incidence of crime, which the systems were claimed to reduce, increased following their construction (Muriuki Kithinji et al., 2023; Wangari, 2023). Huawei has since expanded its operations in the country to include a data centre. Its services have cost the Kenyan government some USD 150 million (Van Der Made, 2021). The government used Dataminr social media monitoring technology during the 2017 elections (Roberts et al., 2023, p. 157).

Capture-and-validate SIM card registration is compulsory in Kenya, with 97 percent of SIM cards registered by 2023 (*Capital FM*, 2023; GSMA, 2021, p. 16; Hersey, 2022h), although biometric data collection undertaken by Safaricom—the country's largest telecom—had not, despite its claims, been authorized by the government (Macdonald, 2022i). A Privacy International report (2017b) has documented Kenyan National Intelligence Service (NIS) and Directorate of Criminal Investigations' direct access to telecom records, including BTS data, which they complement with the use of IMSI catchers and/or similar location tracking devices. Between 2012 and 2014, with the assistance of NIS, the Communications Commission of Kenya set up the Network Early Warning System (NEWS) to monitor international data traffic. The Commission's successor agency, the Communications Authority, subsequently complemented NEWS with the National Intrusion Detection and Prevention System, which includes a "media monitoring and management" system provided by Israel's WebintPro, and made plans to introduce a government-controlled device management system intended to capture and analyze internet traffic (Privacy International, 2017a, 2017b). The Communications Authority introduced a separate device register, set to record the IMEI numbers of all mobile phones entering Kenya, in 2024, although implementation was stopped by a court order (Resian, 2024; Rotich, 2024).

Citizen Lab has also detected the use of Blue Coat's DPI system (*BBC*, 2013) and both Circles and NSO spyware in Kenya (Dadoo, 2021; Marczak et al. 2015, 2017b, 2018). The Kenyan government has additionally deployed Verint's Engage GI2 cellular network monitoring system, which allows operatives to identify, intercept, track, manipulate, and locate targets' mobile phones (Kapiyo et al., 2024, p. 31). Its attempt to acquire Hacking Team's RCS in order to "deface or bring down" the opposition-leaning Kahawa Tungu blog has been unsuccessful.

Hacking Team declined to provide the system: "the [URL] they asked us to tear down is a news website that is highlighting corruption and other wrongdoings in the Kenya government. I don't think we want to be involved with this," wrote the company's representative (Finnan, 2015; also Ouma, 2015). An unknown actor has deployed Gamma's FinFisher/FinSpy in the country (Marczak et al., 2015).

Kenya has received considerable assistance from foreign governments—in particular a grant from the US Trade and Development Agency for Technical Assistance—to fund its digital initiatives. The US government contractor Booz Allen developed the country's National Cybersecurity Strategy (Privacy International, 2017a).

Lesotho

Regulations specifying mandatory SIM card registration, which includes collection of fingerprint data, were introduced in Lesotho in 2021 (CIPESA, 2022, p. 34). The country's government also plans to issue biometric identity cards (CIPESA, 2022, p. 33).

It has additionally installed a biometric access control scanner in the offices of Prime Minister Thomas Thabane; since a limited number of people presumably visited the location, this instance can be classified as one of targeted surveillance. Wiretapping devices were detected at the prime ministerial offices; it is unclear if they had been installed by agents of the Basotho state (*AFP*, 2017).

Liberia

Liberia has introduced a biometric-based national identity register. Enrollment "entails capturing the biometric data of those concerned for the issuance of highly secured biometric national ID cards with a unique number which will be used as a social security number" (Macdon-

ald, 2023r). Liberians have been reportedly reluctant to enroll (Macdonald, 2023r). The country also has a biometric voter register, with high level of mistrust in the system reported (Macdonald, 2023s, 2023ad, 2024f). Capture-and-validate SIM card registration became mandatory in Liberia in 2021 (CIPESA, 2022, p. 36).

Libya

Amesys, VASTech, and ZTE provided Libya's Gaddafi regime with communications monitoring systems also used to monitor regime opponents (*Al Jazeera*, 2017a; Lee, 2021; Coker & Sonne, 2011; Valentino-DeVries et al., 2011). The regime also obtained Hacking Team's RCS (Gibbs, 2015). Some of these tools appear to have been reintroduced by post-Gaddafi authorities (Coker & Sonne, 2012), which may or may not be responsible for the deployment of Pegasus in Libya (Marczak et al., 2018). SIM card registration—of the capture-and-store type—is mandatory in the country (GSMA, 2021, p. 16).

Madagascar

The Madagascan government has increasingly taken "measures to monitor and control its civil servants and citizens" (Hersey, 2020a). It has instituted mandatory capture-and-store SIM card registration (CIPESA, 2022, p. 37; GSMA, 2021, p. 16) and contracted with Huawei to install over 1,000 CCTV cameras in major cites and with Pangea IT to build an e-payment system for government employees and students intended "to monitor their spending habits" (Hersey, 2020a). The government also issues biometric passports and biometric driver's licenses (CIPESA, 2022, p. 37) and has made plans to create a biometric digital identity register (Opiah, 2024a).

Citizen Lab and Meta have detected Intellexa's Predator in Madagascar (*NF News*, 2022b). President Andry Rajoelina did not deny his administration's involvement in Predator's acquisition when asked about it in an interview (*Radio France International* 2023).

Malawi

Malawian authorities have introduced a digital identity register based on biometric data collected—as of 2017 from 9 million Malawians—using United Nations Development Program-funded registration kits from Laxton Group. As of 2017, they had enrolled 9 million Malawians; in 2022, the registration rate reached 94% of the adult population (Hersey, 2022c; Mayhew, 2017). Malawians need to enroll in the system to open bank accounts (Burt, 2019b). Enrollment is also a prerequisite for participation in the 2025 elections (Macdonald, 2024v). In 2018, the country's telecom regulator initiated mandatory capture-and-store SIM card registration (*Business Wire* 2018); touted as a crime prevention measure, it preceded an increase in mobile money fraud (Roberts et al., 2023, p. 109). In 2010, the Malawi Communications Regulatory Authority made plans to deploy a device management system that "could be used to eavesdrop on people's communication" and "surveil mobile money transactions"; due to court challenges and vendor changes, the plan remained unimplemented as of 2022 (Roberts et al., 2023, p. 110). The government has also deployed CCTV surveillance (Mutisi, 2022). In 2020, in partnership with Huawei it opened a data centre to manage the collected information (Roberts et al., 2023, p. 105).

Mali

Mali requires that mobile phone users register their SIM cards with telecom companies. The country uses the capture-and-store model of SIM card registration (GSMA, 2021, p. 16).

Mauritania

The government of Mauritania has mandated capture-and-store biometric SIM card registration (GSMA, 2021, p. 16; Macdonald, 2023o). It has also made plans to introduce a digital identity register (Opiah, 2024b).

Mauritius

Mauritius has launched a biometrics-backed digital identity register, based on legislation which the United Nations Human Rights Committee has found "does not provide sufficient guarantees for securely protecting the biometrics of cardholders and therefore violates citizens' privacy rights" (Hersey, 2021c). Capture-and-store SIM card registration became mandatory in 2008 (GSMA, 2021, p. 16). In 2020, the Mauritian government was planning to "institute a widespread surveillance apparatus. The Safe City project funded by Huawei [would] install a system of hundreds of CCTV cameras in the Port-Louis area purportedly intended to fight crime" (Robertson, 2020); it is not clear if the system has been installed. The National Security Service has been linked to surveillance of government opponents' communications undertaken by a team of Israeli operatives from ECI Telecom (Khan, 2019).

Morocco

SIM card registration—of the capture-and-store type—is mandatory in Morocco (GSMA, 2021, p. 16). In 2018, the Moroccan government introduced a mandatory digital identity card, based on software from Thales, that contains fingerprint biometrics (Borak, 2023a; Burt, 2020a; Privacy International, 2019e). It has also deployed Gemalto's biometric voter registration system, biometric driver's licenses, and biometric passports (Lee, 2017a; Privacy International, 2019e) and made plans for the use of facial recognition to identify social welfare program recipients

(Pascu, 2020). In 2019, Morocco's Direction Générale de la Sûreté Nationale contracted with Idemia to "provide the cards for use with online services and transactions, along with a platform for secured digital identity online services" (Burt, 2019d). The government has also deployed Amesys's Eagle DPI tool (Privacy International, 2015b). By 2016, Casablanca had 500 CCTV cameras (Privacy International, 2019e); Moroccan authorities' stated intention to expand this system and create 'smart cities' in the country (*ENP Newswire*, 2016; *PR Newswire*, 2020). Morocco has received EU funding for a border surveillance project (Roberts et al., 2023, p. 148).

The government procured Hacking Team's Da Vinci or Galileo RCS, used to surveil the citizen media and journalism project Mamfakinch, no later than in 2012; the unidentified spyware it deployed in mid- and late-2010s to surveil journalists might have been the Hacking Team RCS or another tool, such as FinFisher, which Moroccan authorities are known to have used (Gibbs, 2015; Hajjaj, 2019; Marczak et al., 2014; Marquis-Boire, 2012; Privacy International, 2015b). The Moroccan Ministry of the Interior has been a Circles client since 2018 (Dadoo, 2021; Marczak et al., 2017b), while the country's intelligence services appear to have used Pegasus to infect the devices of multiple opposition figures and journalists as well as Sahrawi irredentists and Algerian and French politicians and government officials (Chown ,2020; *M2 Presswire*, 2022; Marczak et al., 2018; Neugeboren, 2020; *NF News*, 2021b). Moroccan authorities have also acquired a mass surveillance system from ETI A/S (Privacy International, 2019e). Total Secure Defense has provided them with an IMSI catcher (Roberts et al., 2023, p. 91). During the 2015 elections, the government reportedly tapped 30,000 mobile phone lines across the country (Privacy International, 2019e).

Mozambique

The Mozambican government has introduced mandatory capture-and-store SIM card registration that in 2016 resulted in the deactivation of five million unregistered mobile connections (*Business Wire*, 2020; GSMA, 2021, p. 16). New regulations adopted in 2023 require that phone users "provide their fingerprint and face biometrics in addition to other identity credentials such a national ID card, passport or driver's licence" to (re-)register their SIM cards (Macdonald, 2023b). Biometric data collection began the following year (Burt, 2024b). The government has also instituted two biometrics-backed digital identity systems, used to issue identity cards to citizens and refugees (Macdonald, 2024r). In 2018, the Mozambican electoral commission purchased a biometric voter registration system from Laxton (Mayhew, 2018). Three years later, a biometric identification layer provided by Simprints was added to land ownership registries (Hersey, 2021b). The country's government has also contracted with Verint, but Cognyte software has apparently only been used to stop abduction (Shezaf, 2018).

Namibia

Namibia's mandatory SIM card registration process includes optional biometric data collection (Hersey, 2022d; Links, 2022; *The Namibian*, 2022). Introduction of this requirement in 2023 met with resistance "from locals against setting up registration points in certain communities, lack of interest by mobile phone users or the submission of inaccurate information" (Macdonald, 2023o). Civil society figures expressed concerns that "[t]he SIM card registration and data-retention measures collectively mean confidentiality and anonymity in telecommunications are effectively eradicated. […] Telecommunication service providers will track, gather and store all the communications data of everyone talking, posting or typing on their services. Every active Namibia-registered mobile number or internet connection will be permanently visible to and data

retrievable by national intelligence or law enforcement" (*The Namibian*, 2022). After the registration deadline passed in 202, operators suspended 22 percent of SIM cards in the country (*Namibia Economist*, 2024). The Namibian government started issuing biometrics-based identity cards to refugees and asylum seekers in 2024 (Macdonald, 2024h).

In 2014 the Namibian government was in talks to obtain Hacking Team's RCS. Their outcome is unknown (Links, 2018).

Niger

Niger has introduced a biometric voter register, despite donor concerns; by inserting biometrics into the electoral code, Nigerien authorities "blackmailed their partners: now if we want to support democracy, we need to fund indirectly a biometric system" (Privacy International, 2019b). Enrollment began in 2020 (CIPESA, 2022, p. 46). The unspecified technology purchased from Gemalto may be the voter register (Macdonald, 2023h). SIM card registration—of the capture-and-store type—is mandatory in the country (GSMA, 2021, p. 16).

Nigerien authorities have used EUR 11.5 million provided by the EU to purchase "surveillance drones, cameras and software to bolster migration controls" in addition to an IMSI catcher. The European Ombudsman has found that the EU had not properly assessed the human rights impact of the transfer, noting that it "came in the context of a crackdown on activists in Niger" (European Ombudsman, 2022). At that time, Niger had "no laws that regulate[d] the use of this kind of intrusive equipment" and "there was little to deter authorities from using the equipment for purposes other than border surveillance" (*Reuters*, 2010). Such a legal framework came into being in 2020: "Niger adopted an interception of communications law that legalizes intercepting electronic communications 'in the interest of national security.' Opposition politi-

cians boycotted the vote in the National Assembly, arguing that the law allows for widespread monitoring of communications 'under false pretences other than those related to security and the fight against terrorism'" (*All Africa*, 2020a). Indeed, a government minister admitted that intelligence services had placed opposition politicians under surveillance: "Are you afraid of being tapped? You have been and still are. It is just going to be organised now," he said in parliament (CIPESA, 2022, p. 46).

Nigeria

"Nigeria is Africa's largest user of surveillance technologies" (Roberts et al., 2023, p. 18). Between 2013 and 2022 the country's governments—which, uniquely, include subnational state authorities—spent no less than USD 2.7 billion on digital surveillance (Roberts et al., 2023, p. 18).

The first documented instance of government digital surveillance technology in Nigeria dates back to the 1990s, although details are scarce (*M2 Presswire*, 1995). The Nigerian Communications Commission (NCC) implemented a capture-and-share SIM card registration system in 2011 and in 2015 fined the telecom giant MTN USD 5.2 billion for failing to deactivate some five million unregistered mobile connections (Privacy International, 2019i; Wexler & Akingbule, 2015). In 2021, President Muhammadu Buhari decided that the government would start recording IMEI numbers of all phones in the country, "raising suspicion about the real intent of the move, and whether stronger digital ID systems are enabling indiscriminate surveillance" (Macdonald, 2021g). This move may be related to the NCC's plans to implement a device management system intended to "serve as a repository for keeping records of all registered mobile phones' International Mobile Equipment Identity and owners of such devices." Critics fear "that

since the IMEI of a phone enables it to track down its owner, the government might abuse it and use it to arrest critics and opposition members" (Alagbe, 2021). In 2020, the NCC issued a directive mandating that subscribers link their SIM card registrations to valid National Identification Numbers (NINs; *Regulatory News Service*, 2020); "intended to erect a major barrier against an epidemic of kidnappings plaguing the country," this requirement proved ineffectual due to "lack of utilisation" (Burt, 2024b). Nonetheless, some 40 million SIM cards were disconnected in 2024 (Burt, 2024c). By 2024, 57 billion Naira (USD 35 million) had been spent on SIM card registration (Macdonald, 2024j). Nigerian authorities have obtained data from telephony operators to surveil the communications of journalists on at least one occasion (*Daily Trust*, 2020).

NINs are issued to Nigerians enrolled in the country's biometrics-based digital identity register, maintained by the National Identity Management Commission (NIMC). By 2021, 66 million people had provided their data (Macdonald, 2021e), by 2023—102 million (Macdonald, 2023x), and by 2024—105 million (Macdonald, 2024j). As of 2023, only 43 percent of enrollees were women, a number indicative of gender-based exclusion (Burt, 2023f). To expedite registration, some have paid bribes to NIMC staff (Burt, 2023h). According to a lawsuit filed by a civil society organization, the government allegedly allowed security agencies to access the biometric data collected by NIMC (Macdonald, 2022o). At least one state government has made access to public services conditional on having a NIN, which many residents did not at the time this requirement was imposed (Macdonald, 2021f). As of 2024 sensitive personal data collected by NIMC were available for purchase on several websites (Macdonald, 2024k).

A separate Bimodal Voter Accreditation System, maintained by the Independent National Electoral Commission (INEC), also based on biometrics, records Nigerian voters; registration is

a precondition to voting, despite the "failure of biometric kits across many polling stations, presumably threatening citizens' ability to exercise their right to vote" (Macdonald, 202b) and amid "complaints of disenfranchisement due to the limited timeframe and staff incompetence, as well as failures of some of the biometric kits supplied by Laxton" (Macdonald, 2023ad). The system has been used to identify "many multiple and ineligible registrations to the country's voter rolls" (Burt, 2022b). "Digital rights activists have raised concerns over the safety and security of biometric data collected from millions of Nigerians who registered and voted in the country's general elections" held in 2023, expressing "worries that the biometric and biographic data in the keeping of INEC could potentially be used by the state for surveillance or other unorthodox purposes," especially since "the absence of a personal data protection bill in Nigeria also makes the problem worse as citizens who feel their data privacy rights are violated cannot seek redress from government" (Macdonald, 2023d).

To open bank accounts, Nigerians need Bank Verification Numbers (BVNs), with biometric enrollments made with Dermalog equipment, of which 55 million had been issued by 2022; 79 million previously opened bank accounts remained unregistered at that time (Macdonald, 2022k, 2022m). In 2023, the government ordered banks to close accounts not linked to BVNs; a Central Bank of Nigeria official said at the time: "Once a customer's biometrics have been captured and enrolled in the database of NIBSS [Nigeria Inter-Bank Settlement System], the BVN remains for life" (Burt, 2023g). Starting in 2018, the Nigerian government began collecting biometrics for the Correction Information Management System used to keep tabs on convicts (Macdonald, 2021c). It also issues biometrics-based driver's licenses (Macdonald, 2021b). As of 2021, the government had taken delivery of mobile biometric enrollment kits ahead of planned

registration for the National Health Insurance Scheme's patient register (Macdonald, 2023a) and was planning to collect biometric data of 6 million students to facilitate enrollment in the National Social Home Grown School Feeding Program (Macdonald, 2021d). Nigerian authorities subsequently made plans to collect biometric data while administering the 2023 census (Macdonald, 2021l). A cash transfer program launched in the same year, expected to benefit 12 million households (and 60 million individuals), involves mandatory identification using both NINs and BVNs (Macdonald, 2023t). 25 million people received the first payments in 2024 (Opiah, 2024c). A year later, the government introduced biometric scanners to the airports in Abuja, Enugu, Kano, Lagos, and Port Harcourt (Gonzalez, 2024). The scanners are part of a larger "advanced e-border surveillance system" deployed to 80 border crossings (Salako, 2025).

In 2022, the Lagos State government announced the introduction of its own biometric registration system, to be used for access to public services (Macdonald, 2022b). Similarly, Borno State has collected biometric data from former Boko Haram members (Macdonald, 2023y), while authorities in Anambra have mandated that public transit providers submit their biometrics using technology supplied by OneID, an Appmart subsidiary (Macdonald, 2022n). Another Nigerian company, eGate Technology, has sold the national government biometric 'smart' payment cards that "will be integrated with existing payment facilities to facilitate payments for citizens" (Macdonald, 2023w),

Indeed, the use of biometrics has become widespread in Nigeria: "From the National Population Commission (NPC) to the Nigeria Immigration Service (NIS), Federal Road Safety Corps (FRSC), Independent National Electoral Commission (INEC), Central Bank of Nigeria (CBN) and several other federal agencies, Nigerians are being asked for their biometric data for

almost every service" (*This Day*, 2022). Until the adoption of the Data Protection Bill in 2023, following the establishment of the Nigeria Data Protection Bureau a year earlier, no legal restrictions on the use or retention of these data existed in the country (Macdonald, 2022k; 2023v).

The Nigerian federal government has also installed a ZTE-provided 'smart city' system in Abuja and Lagos (Mutisi, 2022; Roberts et al., 2023, p. 53). The Kaduna, Kano, Kogi, Lagos, and Niger state authorities have invested in analogous systems (Roberts et al., 2023, pp. 553–554). Federal authorities have also made plans to install surveillance cameras alongside Nigeria's borders (Roberts et al., 2023, p. 54). In addition, the country has seen the deployment of Blue Coat's DPI system (*BBC*, 2013). On at least two occasions, in 2018 and 2021, the federal government made provisions to acquire social media monitoring systems (Roberts et al., 2023, p. 52). It also seems to have used the social media monitoring tools provided by Dataminr (Roberts et al., 2023, p. 157).

The construction of this extensive apparatus of mass surveillance has gone hand in hand with the use of spyware. Faced with the Boko Haram insurgency, Goodluck Jonathan's federal administration subsequently awarded a USD 40 million contract intended to "strengthen intelligence gathering […] and the movement of funds" to Elbit Systems (*BBC*, 2013; Roberts et al., 2023, p. 49; Shezaf 2018). Several Nigerian state governors also procured digital surveillance tools to surveil political opponents. The Bayelsa governor Seriake Dickson "distributed compromised Blackberry phones as gifts to his targets to gain access to their private lives"; the phones had been infected with Hacking Team's RCS (*BBC*, 2015; Marczak et al., 2014; Ogala, 2014, 2015a, 2015b, 2016). His colleagues Akwa Ibom of Rivers and Rotimi Amaechi, Godswill Akpabio, and Emmanuel Uduaghan of Delta made use of Circles' spyware (Ogala, 2015a, 2016;

Shezaf, 2018). The Nigerian Defence Intelligence Agency and the Nigerian Police Force also deployed Circles spyware (Dadoo, 2021; Marczak et al., 2017b; Roberts et al., 2023, p. 51). In 2010, the Israeli-owned Abuja-based V&V Nigeria won a contract, worth 6 billion Nigerian naira, to build a location tracking system for the Nigeria Police Force and expand and upgrade an existing system operates by the State Security Service; one of those systems appears to have been a Circles installation (Ogala, 2015b; Roberts et al., 2023, p. 51). That same year, the Ministry of Police Affairs awarded a contract to Gamma International; a FinFisher/FinSpy control server appears to have been subsequently installed in Abuja (Roberts et al., 2023, pp. 50–51). An unknown federal body contracted with MPD Systems, and the Office of the National Security Adviser with Verint, presumably following the election of Muhammadu Buhari, who had been surveilled as a candidate for presidential office (Ogala, 2016; Shezaf, 2018; *Sputnik News*, 2018); the latter incident might have been connected to the hacking of opposition politicians' phones ahead of the 2015 elections (Roberts et al., 2023, p. 149). In 2017, "almost 70 percent of mobile phones in Abuja [were] bugged by a covert security unit" (Uwerunonye, 2017). Mi Marathon Resources, previously also involved in Nigeria's Verint contract, has also provided the Office of the National Security Adviser with Fiber Optic Landing Solution, intended to enable backend access to all fibre-optic cables connecting the country to the rest of the world (Roberts et al., 2023, p. 50). The National Intelligence Agency has obtained tools that enable it to "track, intercept and monitor calls and messages on mobile devices, including Thuraya, as well as social networking platforms like WhatsApp" (Alagbe, 2021). The Economic and Financial Crimes Commission has obtained at least one UFED, used to target Nigerian journalists, from Cellebrite (Roberts et al., 2023, pp. 50–51).

Rwanda

The government of Rwanda reportedly first deployed unspecified digital surveillance technology shortly after the 1994 genocide (*M2 Presswire*, 1995). In 1997, it launched a 'smart city' project in Kigali (*M2 Presswire*, 2017), which may or may not be the instance of CCTV surveillance reported elsewhere (Mutisi, 2022). As of 2016, the Rwandan government was planning to introduce a national identity register, although it was not yet in place in 2023, when the announcement of plans to start issuing biometric identity cards prompted concerns of exclusion (King, 2016). In 2024, it created a separate social register to help implement a poverty alleviation scheme (Macdonald, 2024i). Capture-and-store SIM card registration is mandatory in Rwanda (GSMA, 2021, pp. 16). The government has made plans to start collecting biometric data during SIM card registration (Macdonald, 2024aa).

The Paul Kagame regime has also deployed spyware to monitor the activities of individual targets. The exiled former Rwandan intelligence chief Patrick Karegeya thought that Apollo Kiririsi Gafaranga used a recording device disguised as a BlackBerry during a meeting in South Africa; Gafaranga murdered Karegeya on a later visit to the country (Wrong, 2021). The Rwandan government has also been a client of NSO and used Pegasus the devices of Rwandan activists, journalists, and opposition party members in addition to those used by Cyril Ramaphosa and Ugandan government officials (*Deutsche Presse-Agentur*, 2021; Kirchgaessner & Taylor, 2022; Marczak et al., 2018).

Senegal

Senegalese authorities have launched a national digital identity register, which includes biometric data (Macdonald, 2022j; Mascellino, 2023). Capture-and-validate SIM card registra-

tion became mandatory in 2006 (GSMA, 2021, p. 16; Privacy International, 2019a). European Union funding has enabled the government to obtain "invasive surveillance technologies" that include aerial drones and Cellebrite's UFED (Popoviciu, 2023). Huawei has opened in Senegal a data centre similar to the ones in Cameroon and Kenya, but no evidence of its use for government surveillance is available (*NF News*, 2021a). The Senegalese government has also contracted with Gemalto to obtain unspecified technology (Macdonald, 2023h).

Seychelles

Capture-and-store SIM card registration is mandatory in Seychelles (GSMA, 2021, p. 16). Seychellois authorities have also introduced biometric passports (Karapetyan, 2021b) and biometric entry gates at the Seychelles International Airport (Karapetyan, 2021a).

Sierra Leone

The government of Sierra Leone has introduced biometric national identity cards. It subsequently increased the fees it charges for these compulsory documents—required for travel within the country—tenfold (Macdonald, 2023aa, 2024n; Mascellino, 2023). By 2024, 90 percent of the population had registered (Mascellino, 2024m). Capture-and-share SIM card registration became mandatory in 2020 (CIPESA, 2022, p. 52; GSMA, 2021, p. 16).

Somalia

Capture-and-store SIM card registration is mandatory in Somalia (GSMA, 2021, p. 16). Somalian authorities have also introduced a biometric digital identity register (Borak, 2023a; Borak, 2023b; Macdonald, 2025b). Voters in the 2024 elections in Somaliland needed to enroll in a biometric digital identity register to cast a vote (Macdonald, 2024y).

South Africa

South Africa's apartheid regime began work on the world's first universal, biometric, and digital population register, built using IBM computers, in the early 1970s (Breckenridge, 2014, pp. 170–181). Much later, in the 2000s, the government procured Gemalto's biometric voter registration system (*ENP Newswire*, 2010). It subsequently made plans to require submission of biometrics from driver's license applicants (Macdonald, 2024o) and to collect photographs of the eyes, hands, feet, and ears as well as fingerprints of every newborn for a digital identity verification register; the system's rollout was delayed by corruption (Burt, 2022c; *NF News*, 2019). South African authorities used Dataminr's social media monitoring tools to keep tabs on student demonstrations in Cape Town (Roberts et al., 2023, p. 157). They have also tapped fibre-optic undersea cables for the purpose of bulk interception of internet traffic (Privacy International, 2019j).

South Africa's government began the rollout of CCTV surveillance systems with their installation on the Gautrain and Johannesburg Bus Rapid Transport in the late 2000s (*Canada Stockwatch*, 2009). By 2022, Johannesburg had 574 cameras (Hao & Swart, 2022; Mutisi, 2022). Huawei has been involved in the creation of a 'smart city' project in South Africa (Roberts et al., 2023, p. 135). In addition, police regularly access CCTV feeds from "South Africa's private surveillance machine" (Hao & Swart, 2022).

Capture-and-store SIM card registration is mandatory in South Africa (*Business Wire*, 2010; GSMA, 2021, p. 16). The South African State Security Agency used data obtained from telecom companies to surveil the country's residents en masse, a practice that the constitutional court declared unlawful and invalid in 2021 (*The Namibian*, 2022). Between 2008 and 2011 alone South African authorities used the emergency provisions in the Regulation of Interception

of Communications and Provision of Communication-Related Information Act of 2002, which regulates communications surveillance in the country, over 3,200 times to trace the locations of individual mobile phones, presumably using BTS data from telecoms (Hunter, 2014). By the second half of the 2010s, the number of requests for sensitive communications information submitted to telecoms had grown to at least 70,000 per year and possibly as many as 200,000 per year (*All Africa*, 2017). Civil society organizations have collected substantial evidence of "unlawful surveillance of journalists, political activists, and human rights defenders" (*All Africa*, 2017) as well as the "rivals and love interests" of government functionaries (Hunter, 2014). The South African Revenue Service seems to have been responsible for the use of FinFisher in the country (Privacy International, 2019f). South African police have deployed aerial drones and IMSI catchers (Privacy International, 2019f; Magcaba, 2023). President Jacob Zuma's administration has intercepted the communications of his political opponents, including his predecessor Thabo Mbeki, apparently without court approval (Cohen, 2009). Some of this interception involved the deployment of an IMSI catcher sourced from China (Erasmus, 2021). It is the government of Rwanda that seems to have used Pegasus in South Africa (Marczak et al., 2018).

South Sudan

In 2017, the government of South Sudan started a USD 1 million 'smart city' project, which has involved the deployment of surveillance drones and cameras, apparently provided and partly operated by an unnamed Israeli company, throughout Juba. It has also introduced biometric verification to the public service payroll in order to "to mitigate the risk and unethical payroll activities, particularly the control of potential ghost workers" (Macdonald, 2024q). The government collects fingerprints of holders of national identity cards (CIPESA, 2022, p. 53). Since

2012, to purchase a SIM card South Sudanese need to show a government-issued identity document and provide personal information including home address and place of birth (*All Africa*, 2020b; CIPESA, 2022, p. 53; GSMA, 2021, p. 16). South Sudanese authorities have used these data, captured and stored by telecoms, to target individuals, compelling telecom operators "to provide phone numbers, metadata, and call logs belonging to their customers," including for the purpose of wiretapping and arrest. Similarly to Ethiopia and Kenya, National Security Service (NSS) "officers assigned to telcos have access to the company databases and can monitor specific phone numbers and even make voice audio recordings of conversations" (*All Africa*, 2020b).

In addition, the NSS has obtained surveillance equipment acquired to "intercept and monitor" telephone and internet networks as well as IMSI catchers (*All Africa*, 2020b). Providers of this equipment have included Hacking Team and Verint; Hacking Team's RCS was used to surveil the former minister and detainee Pa'gan Amum (*All Africa*, 2020b; Shezaf 2018). Beyond remote infiltration, government officials have seized devices from individuals and coerced them to reveal passwords in order to access personal data (*All Africa* 2020b).

Sudan

In the early 2010s, Sudan's Ministry of Interior launched an electronic civil registry that includes fingerprint data (*All Africa,* 2011). Mandatory SIM card registration—of the capture-and-store type—was introduced in 2008 (GSMA, 2021, *All Africa*, 2020b16; Privacy International, 2019a). The Sudanese National Intelligence and Security Services has deployed Blue Coat's DPI system in the country (Roberts, 2021, p. 113).

The Sudanese government has also procured Hacking Team's RCS (Gibbs, 2015; Marczak et al., 2014). More recently, Intellexa sold its Predator spyware to the Rapid Support Forces

(Black, 2022); since at that time they formed part of the Sudanese army, I categorize this purchase as one of government surveillance.

Tanzania

Tanzania's digital population register, built by KT Corp, "includes the digital national identification data centre in Kibaha, a backup centre, 13 regional resident registration offices, a fingerprint identification and management system, a network control system and a resident registration website" (*PR Newswire*, 2018). By 2020 the National Identification Authority had registered over 22 million people (Burt, 2020b). In 2023, the government announced that the existing register will be replaced by a new system (Macdonald, 2023ac). The collection of biometrics extends to mandatory capture-and-validate SIM card registration (Msemo, 2022; *NF News*, 2021e). Biometric SIM card registration has not curbed fraud, one of the justifications for its introduction, as "people ignorantly allow their ID cards for the registration of SIM cards which are not theirs. Fraudsters then use such SIM cards and commit crimes" (Macdonald, 2023ai). In 2018 the government instituted mandatory—and, at USD 930 per year, prohibitively expensive—registration for bloggers (Dahir, 2018). Five years later it mandated registration of virtual private network users (Dawa, 2024). CCTV surveillance is present in many locations (Mutisi, 2022), including in internet cafés, whose operators are required to install surveillance cameras to monitor customers' online activity (Wright, 2019). This technology has been used "to round up opposition," although information is limited (*NF News*, 2022a). In addition, the government has monitored social media to "hunt down and round up" LGBTQ people (Charity, 2018). Tanzania adopted a Personal Data Protection Act in 2022, but as of 2023 the government was yet to establish a data protection authority as required by the Act (Macdonald, 2023z).

Togo

SIM card registration—of the capture-and-store type—is mandatory in Togo (GSMA, 2021, p. 16). The country's government has also made plans to issue biometrics-based identity cards "to every citizen in order to facilitate their access to different public and social services" (Macdonald, 2023ae). Togolese authorities have used NSO's Pegasus to target a Catholic bishop, a priest, and other members of civil society as well as opposition politicians (Allison 2018; Marczak et al., 2018; Scott-Railton et al., 2020) and obtained spyware from Donot Group to surveil a human rights defender (*M2 Presswire*, 2021).

Tunisia

Prior to the Arab Spring, Tunisia's Ben Ali regime purchased Gemalto's biometric voter registration system (*ENP Newswire*, 2010). It also filtered internet access in the country using DPI systems provided by Blue Coat, NetApp, and Utimaco as well as ETI A/S's browsing and email logger (*All Africa*, 2008; Privacy International, 2019g). Trovicor provided voice and data interception technologies to the government, which also used ATIS Huer's 100 Klarios system for "satellite monitoring, data retention and traffic monitoring" (Privacy International. 2019g). A contemporary report detailed the measures taken by the regime:

> Under a post and telecommunications law adopted in 1998, the authorities can check the content of email messages at any time. The law authorises the interception of any message that could "jeopardize public order and national security." The communications ministry keeps information exchanged online under very close surveillance. […] In the provinces, internet users must often show ID in order to be able to sit down at a computer. (*Canada NewsWire*, 2007)

In 2016, Ben Ali's successors announced the installation of over 1,000 surveillance cameras in 300 'electronic checkpoints' in Tunis and the Kasserine, Kef, Jendouba, and Sidi Bouzid governorates (Privacy International, 2019g). The following year, with American and European support, the government started building a border surveillance system to "to prevent extremists and migrants from slipping across into the country and to halt the flow of migrants across the Mediterranean from Africa" (Privacy International, 2019g). More recently, the Kais Saled administration has initiated the construction of 'smart cities' in Tunisia (*Reuters*, 2023). Capture-and-share SIM card registration is mandatory (GSMA, 2021, p. 16).

Mobile phones located in the country have been among those infected with NSO's Pegasus, but there is no evidence of the Tunisian government's involvement (Allison, 2018; Marczak et al., 2018). The same is true of BlackOasis use of FinFisher/FinSpy in Tunisia (*Business Wire*, 2017).

Uganda

The Ugandan government began building its mass surveillance apparatus with mandatory SIM card registration, of the capture-and-validate type. In the absence of data protection legislation, the data collected during the registration drive, launched in 2012, lacked any legal protections, especially in light of the Regulation of Interception of Communications Act 2007, which authorized the government to monitor and intercept telephone and other communications for 'security purposes' (*All Africa*, 2012; *BBC*, 2014; GSMA, 2021, p. 16; Privacy International, 2019a). The Human Rights Network for Journalists-Uganda called upon the government to halt the process, a demand that went unheeded despite concerns that registration violated the country's constitution, which states that "no person shall be subjected to interference within the priva-

cy of their home, correspondence, communication, or other property" (*All Africa*, 2012). Telecoms began collecting biometric data during SIM card registration in 2018 (*NF News*, 2021c; Privacy International, 2019a). Two years later, the Uganda Communication Commission ordered telecoms to disconnect 1.4 million SIM cards that had not been biometrically registered (Macdonald, 2023ah).

The government has also contracted Mühlbauer to build Ndaga Muntu, the country's biometric national ID register, which as of 2019 contained the fingerprints—in addition to non-biometric data—of 30 million Ugandans (Burt, 2019c; CHRGJ, 2022, p. 64). The database is reportedly "rife with spelling errors, incorrect birth dates and wrong residence addresses" (Choi, 2022; also CHRGJ 2022, p. 10). "Initially designed to serve national security objectives that have dominated its operation ever since, Ndaga Muntu has never made good on its other promise to foster social inclusion" (CHRGJ, 2022, p. 8). During the Covid-10 pandemic, the system, described at the time as "so exclusionary that a third of the adult population, including vulnerable groups, are prevented from registering," was used to distribute welfare (Hersey, 2021a); human rights organizations successfully sued the government after it had attempted to restrict access to Covid-19 vaccines to those who could present national identity cards (Hersey, 2022g). As of 2024, financial transactions of 1 million Ugandan shillings or more require presentation of the cards (Macdonald, 2024u). Ugandan authorities have used Ndaga Muntu to target political adversaries, including the prominent human rights lawyer Nicholas Opiyo (Solon, 2024). By 2021, Ndaga Muntu had cost some USD 200 million (CHRGJ, 2022, p. 15). In 2022, the government announced plans to start collecting DNA biometrics for an updated version of the system, with enrollment set to begin in 2024 (Choi, 2022).

The Uganda Police Force has acquired Gemalto's Cogent Automated Biometric Identification System and LiveScan technology "to facilitate better crime-solving through the electronic collection, storage and processing of fingerprints, palm prints and facial captures" (Mayhew, 2019c), while the Directorate of Citizenship and Immigration Control has deployed fingerprint and facial recognition technology provided by the same company at Entebbe International Airport, followed by plans to introduce facial recognition systems at land border crossings (Macdonald, 2023af; Mayhew, 2019a). Ugandan authorities have also used Cellebrite's UFED (*All Africa*, 2024). In the census scheduled for 2024, "all the data, including fingerprints that will be collected by enumerators during the census, will be processed digitally" (Macdonald, 2023ag).

In 2018, the Yoweri Museveni regime signed a USD 126 million deal with Huawei for a 'safe cities' project made up of CCTV cameras equipped with facial recognition software that transfers collected data to 83 police stations in Kampala and, eventually, another 271 stations across the country. The system was in use by 2019 (Marks, 2019; Mutisi, 2022; Woodhams, 2019). The government subsequently contracted with Joint-Stock Global Systems of Russia to install digital trackers in all vehicles in Uganda. The plan drew widespread opposition. According to Dorothy Mukasa of Unwanted Witness, a Ugandan digital rights organization, "[t]his is an expansion of the state's plan of surveilling on everybody, they want to use this GPS data collection to track opposition politicians, activists and journalists" (*Reuters*, 2021). The Ugandan parliament approved compulsory installation of vehicle trackers in 2023 (*New Vision*, 2023). 2014 saw the creation of a social media monitoring centre intended "to weed out those who use [social media] to damage the government and people's reputations" (Privacy International, 2019h).

Extensive use of spyware to target the regime's opponents accompanies these mass surveillance systems. In 2011, the government paid Gamma 200 billion Ugandan shillings for the use of FinFisher/FinSpy, deployed in hotels and government offices, including the country's parliament, as part of operation Fungua Macho ('Open Your Eyes'; *BBC*, 2014; Marks, 2019; Oluka, 2015; Privacy International, 2015a, 2015c). According to an internal government briefing, the purpose of Fungua Macho was "to manage and control the media houses and opposition politicians, which in the worst case scenario, may involve blackmailing them especially after personal information is in our hands" (*Canadian Press*, 2015). In 2012, the Chieftaincy of Military Intelligence's Director of Technical Intelligence Michael Bbosa wrote to President Museveni: "People deemed dangerous to state security like government officials and opposition politicians are being surveilled. […] Given the caliber of our negative-minded politicians, we stand a very high chance of easily crushing them by being a step ahead" (Matsiko, 2015). According to Simon Mulongo, a ruling party parliamentarian, "the state has to watch all of us all the time […] it has to have capabilities to do so all the time" (Matsiko, 2015). At the same time, "[despite procuring advanced hacking technology, the Ugandan police and intelligence agencies' forensic skills remain rudimentary, according to industry insiders" interviewed by the Privacy International team that investigated Fungua Macho (Privacy International, 2015a). In 2014, members of Uganda's LGBTQ community were targeted with Zeus keystroke-logging spyware (Privacy International, 2019h).

Later in the decade, the regime obtained spyware from both NSO and Verint (Marks, 2019; Shezaf, 2018). It also appears to have used NSO's Pegasus to infect the devices of the journalists Raymond Mujuni and Canary Mugume, the opposition politician Norbert Mao, and

American diplomats (Dahir, 2021; *NF News*, 2021d). When the mobile phone of Robert Kyagulanyi, or Bobi Wine, proved resistant to Pegasus infection, intelligence officers sought help from Huawei. According to one of them, "[t]he Huawei technicians worked for two days and helped us puncture through," leading to multiple arrests. They "teach us to use spyware against security threats and political enemies," added another officer (Marks, 2019). Bobi Wine has attributed the physical abuse he suffered at the hands of regime operatives to his experience of digital surveillance: "I even learned that day when I was arrested and brutalized in Arua, it was because of that technology that they got that they could listen to my phones, and they were tracking me" (Solomon, 2019). Another arrestee, Unwanted Witness's Dorothy Mukasa, was located by the police who tracked her mobile phone (Latham, 2020); it is not clear if they used an IMSI catcher, BTS, or another technology. It is also unknown if the Ugandan government successfully acquired spyware from Hacking Team; in 2015, it was in talks to purchase Hacking Team's RCS for 10 billion Ugandan shillings, but the outcome of these negotiations has not been reported (Katusiime, 2021).

Zambia

The creation of Zambia's digital population register, the Integrated National Registration Information System, set to cost some USD 12.6 million, involves the collection of biometric data in the form of "a photograph for facial recognition and 10 plain and rolled fingerprints for now. Later, iris images will be taken for persons whose fingerprints are not readable or may not have fully developed" (Zulu, 2020). By 2022, data had been collected from over 15,000 Zambians (Macdonald, 2022c). The Electoral Commission of Zambia has implemented a separate biometric voter register built using Smartmatic equipment (Roberts et al., 2023, p. 128). In 2011, the

government mandated capture-and-validate SIM card registration that includes biometric data collection (GSMA, 2021, p. 16; *NF News*, 2021e; Privacy International, 2019a). It has also required farmers enrolled in a subsidy program to provide fingerprints (Burt, 2018). Zambia appears to have acquired unspecified DPI technology by 2013 (Roberts et al., 2021, p. 73). At the cost USD 210 million, ZTE has built a 'smart city' project for the government (Roberts et al., 2021, p. 73), which complements earlier CCTV surveillance deployment (Mutisi, 2022). Also involved in the project is Huawei, which the government paid USD 75 million to build a data centre commissioned in 2022 (Roberts et al., 2021, p. 127).

Much like its Ugandan counterpart, Zambia's government has leveraged the relationship with Huawei to target opponents (Latham, 2020): "Huawei technicians helped the government access the phones and Facebook pages of a team of opposition bloggers running a pro-opposition news site, which had repeatedly criticized President Edgar Lungu" (Marks, 2019). Zambian authorities have also used spyware provided by Circles (Dadoo, 2021; Marczak et al., 2017b), Cyberbit (Shezaf, 2018), and, possibly, Pegasus (Allison, 2018; Marczak et al., 2018).

Zimbabwe

In 2017, the Zimbabwe Electoral Commission awarded Laxton Group a USD 3.9 million contract to supply biometric voter registration kits for the 2018 elections (Lee, 2017b). The country's government has also introduced biometric-backed land title deeds and biometric passports (Macdonald, 2022q).

Capture-and-share SIM card registration became mandatory in Zimbabwe in 2013; in 2015 the country's largest mobile service provider disconnected at least one million SIM cards because they were unregistered (GSMA, 2021, p. 16; Privacy International, 2019a). Zimbabwean

internet service providers and telecom operators "have to provide the government with equipment to sort and intercept communications" (*Associated Press*, 2017; Ndlela, 2020b). In addition, in 2015 the government acquired the communication services provider Portnet Software in order "to consolidate its grip on cyberspace as well as its capacity to spy on citizens' communication devices" (Zhangazha, 2015). Having received unsolicited text messages from ZANU-PF, the ruling party, ahead of the 2022 elections, "[s]ome Zimbabwean voters doubt the political line that their biometric and demographic data is safely stored in a server" (Nash, 2022).

Zimbabwean authorities have also deployed a CCTV system equipped with facial recognition software provided by CloudWalk (Chimhangwa, 2022; Gross et al., 2019). The new capital at Mount Hampden is being built as a 'smart city' (Ndlela, 2020a). Bulawayo has seen installation of a vehicle tracking system (Munhende, 2021). Zimbabwean authorities have also deployed aerial drones to patrol borders and made plans to introduce biometric entry gates at border crossings (Freddy, 2023). Data obtained through these mass surveillance systems are to be stored in the National Data Centre constructed with the support of CloudWalk, Huawei, and Hikvision (Ndlela, 2020b).

In 2007, government operatives installed a hidden camera in the ceiling of the Roman Catholic archbishop Pius Ncube's bedroom and used resulting footage to silence his criticism of the government; a cabinet minister subsequently warned opponents that the government could "visit your bedrooms and expose what you will be doing" (Ndlela, 2020a). In the last years of the Robert Mugabe regime, it deployed a "custom-built app [that] allows local police departments to access a database of political activists managed and compiled by the country's central intelligence agency" (*PressWire*, 2016). According to President Mugabe, the deployment represented

"a great step in the democratic process of Zimbabwe. All my enemies will be liquidated. I am just waiting for police to pick up Morgan Tsvangirai and look him up on the app. Then they can shoot him. That will be a great day for Zimbabwe indeed" (*PressWire*, 2016) The Mnangagwa government continued the use of spyware to target its opponents. In particular, it appears to have installed a GPS tracker in the parliamentary vehicle of the opposition leader Charlton Hwende in addition to monitoring his communications. "I've heard spies telling me things I said to my family on the phone organising my own household," Hwende has said (Ndlela, 2020b). According to another opposition politician, Prosper Mutseyami, "[a]lmost the majority of our MPs are being tracked. […] That's the sad reality of the situation we live in because that's how the regime thrives" (Ndlela, 2020b). Some of this tracking has involved the use of IMSI catchers, "widely seen as part of government's current plans to enhance state control over national cyberspace by actively using surveillance and data mining as means to confuse and entrap actual and perceived opponents such as protesters" (Gwagwa & Hove, n.d.), apparently of Chinese make—although the first devices of this type to arrive in Zimbabwe were a gift from Iran—and Circles spyware (Gwagwa & Hove, n.d.; Marczak et al. 2017b).

Part II: Data

This part of supplemental material contains the data on which the article is based. Supplement 4, below, lists the keywords used to search the Factiva repository. The other supplements can be found in separate files that accompany this one. Supplement 5 details all the repository searches. The two repository and instances datasets make up supplements 6 and 7, respectively. Supplement 8 lists the sources used to collate the datasets. The R script used to generate the figures and

other information derived from the datasets and shared in the article and supplements 1, 2, and 3 can be found in Supplement 9.

Supplement 4: Repository search keywords

- Internet surveillance
- Internet whistleblower surveillance
- Internet opposition surveillance
- Internet dissident surveillance
- Internet journalist surveillance
- Internet civil society surveillance
- Internet NGO (non-governmental organization) surveillance
- SIM registration
- Biometrics
- SMS interception
- SMS tracking
- Phone call interception
- Phone call tracking
- Voice logging
- Social media monitoring
- Facial recognition
- CCTV
- Location tracking

- GPS (Global Positioning System) tracking
- Deep packet inspection
- Base Transceiver Station/BTS
- Device management system
- IMSI catcher
- Stingray
- Man-in-the-middle
- Smart city
- Safe city
- Smart policing
- Digital ID
- Emotion recognition
- Gamma
- FinFisher
- FinSpy
- PC 360
- Cyberbit
- NSO
- Pegasus
- CloudWalk Technology
- Circles
- Hacking Team

- Elbit
- Blue Coat
- Hikvision
- ZTE
- Huawei
- MPD Systems
- Verint
- Dark Basin

For example, the searched keyword combinations included "internet *and* surveillance *and* Africa" and "FinFisher *and* Angola."

References

Addis Standard. (2025, January 17). Ethiopian Federal Police Launch Drone Simulation Training Center.
Africa News. (2021, October 2). Congo drags ill former army chief Mokoko back to prison.
African Press Organization. (2012, July 7). Ethiopia: Government steps up control of news and information.
Agence France-Presse. (2012, May 18). In oppressive Gambia, citizens fear SIM card registration.
Agence France-Presse. (2014, March 25). Ethiopia spies on citizens with foreign technology.
Agence France-Presse. (2017, July 29). Lesotho probes tapping of new PM's office.
Agence France-Presse. (2019, August 16). Uganda, Zambia deny Huawei helped spy on political opponents.
Agence France-Presse. (2021, June 22). French prosecutors charge 4 executives over Libya, Egypt cyber-spying.
Al Jazeera. (2017, April 10). How we revealed the surveillance world's illegal trades.
Al Jazeera. (2017, April 10). Spy merchants: Spying on dissent through illegal means.
Alagbe, J. (2021, July 25). Disquiet over govt's unusual surveillance on citizens. *The Punch*.
All Africa. (2008, October 27). Country continues to be one of region's most authoritarian.
All Africa. (2011, May 10). Govt to launch advanced, nationwide civil registry in mid-May.

All Africa. (2012, September 26). Law requiring registration of SIM cards in Uganda a threat to privacy.
All Africa. (2015, March 9). Letter to Hacking Team re—Update on sale and use of Hacking Team solutions in Ethiopia.
All Africa. (2017, December 8). New spate of abusive surveillance.
All Africa. (2017, October 27). Statement—Stats reveal that cops are spying on 70,000+ mobile phones every year.
All Africa. (2018, February 6). True Life of Swazi Prime Minister.
All Africa. (2020, December 14). Summary of report—Inaction on dire security agency abuse.
All Africa. (2020, September 1). Niger passes new law on interception of communications.
All Africa. (2024, August 14). Uganda's Digital Number Plate System, Which Is Aimed At Facilitating the Ability of Authorities to Improve Services, Will Also Have the Detrimental Impact of Expanding the Country's Surveillance Capabilities.
Allen, N. (2019, November 10). Huawei under fire for helping African rulers spy on rivals. *The Daily Telegraph*.
Allison, S. (2018, October 2). South African phones targeted by notorious 'governments only' spyware. *The Mail & Guardian*.
Amahazion, F. (2015, July 14). Ethiopia's Hacking Revelations. *Pambazuka News*.
Associated Press. (2017, August 4). Zimbabwean president approves surveillance law allowing state monitoring of internet, phones.
Bariyo, N. (2020, November 26). Ethiopian forces begin decisive battle in Tigray's capital. *The Wall Street Journal*.
Black, C. (2022, November 30). Flight of the Predator: Jet linked to israeli spyware tycoon brings surveillance tech from eu to notorious sudanese militia. *Haaretz*.
Borak, M. (2023a, June 22). Morocco will introduce digital IDs into health services. *Biometric Update*.
Borak, M. (2023b, September 18). Somalia begins issuing new biometric digital ID developed with NADRA's help. *Biometric Update*.
Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.
Brewster, T. (2020, December 11). Israeli surveillance companies are siphoning masses of location data from smartphone apps. *Forbes*.
British Broadcasting Corporation (BBC). (2013, October 25). Nigeria reportedly awards 40m-dollar security contract to Israeli firm.
BBC. (2014, December 13). Uganda to spend 73m dollars on phone-tapping equipment.
BBC. (2015, November 10). Nigeria's Bayelsa state paid Italian firm 500,000 dollars to hack computers.
Burt, C. (2018, June 5). Biometrics solution by Ingenico and Paycode helps Zambia distribute millions in agricultural subsidies. *Biometric Update*.
Burt, C. (2019a, April 16). Kenya national biometric enrollment project reaches 8 million people. *Biometric Update*.
Burt, C. (2019b, June 13). Malawi bank integrates biometric National ID system for KYC checks. *Biometric Update*.

Burt, C. (2019c, October 10). Mühlbauer helps Uganda reach 30M biometric registrations, details Mozambique and Fiji projects. *Biometric Update*.
Burt, C. (2019d, November 29). Idemia to supply biometric ID cards to Morocco for online services and transactions. *Biometric Update*.
Burt, C. (2020a, August 17). Cyprus and Morocco launching biometric identity cards, India to launch national health cards. *Biometric Update*.
Burt, C. (2020b, November 16). PPPs and social media influencers for biometrics registration and national ID. *Biometric Update*.
Burt, C. (2021, October 15). Kenya's digital ID ruled illegal until data protection impact assessment completed. *Biometric Update*.
Burt, C. (2022a, October 3). Ethiopia's national digital ID prepares foundation ahead of scale-up. *Biometric Update*.
Burt, C. (2022b, September 14). Nigeria finds more ineligible registries in latest biometric deduplication round. *Biometric Update*.
Burt, C. (2022c, July 25). South Africa still waiting for biometric system upgrade after spending whole budgeted amount. *Biometric Update*.
Burt, C. (2023a, September 11). Ethiopian government agencies partner on digital ID for health sector. *Biometric Update*.
Burt, C. (2023b, December 5). History repeats with Kenyan High Court blocking Maisha Namba for lack of DPIA. *Biometric Update*.
Burt, C. (2023c, September 13). Kenya approves Maisha Namba, plans launch this month with $6.8M budget. *Biometric Update*.
Burt, C. (2023d, September 15). Kenyan rights groups warn digital ID program repeating past mistakes. *Biometric Update*.
Burt, C. (2023e, August 23). MOSIP implementation pilot with BioEnable biometrics nears successful completion. *Biometric Update*.
Burt, C. (2023f, May 3). Nigeria closes in on 100M digital IDs issued as enrollment pace declines. *Biometric Update*.
Burt, C. (2023g, May 19). Nigerian banks given deadline to close accounts not linked to ID. *Biometric Update*.
Burt, C. (2023h, September 14). Nigerian digital ID system wrestles with persistent corruption and delays. *Biometric Update*.
Burt, C. (2024a, July 25). Kenyan high court pauses national digital ID for third time in 4 years. *Biometric Update*.
Burt, C. (2024b, January 19). Nigeria struggles to utilize biometric SIM registration to ID criminals. *Biometric Update*.
Burt, C. (2024c, March 5). SIMs not registered, verified with digital IDs in Nigeria blocked. *Biometric Update*.
Business Wire. (2001, February 27). Government of Uganda selects Viisage for new electoral system; Face-recognition technology to be used to reduce potential voter registrations fraud.
Business Wire. (2010, August 12). Research and markets: The Q3 2010 telecommunications report on Nigeria contains forecasts that anticipate the development of the fixed-line, internet, broadband and mobile sectors.

Business Wire. (2017, October 16). Kaspersky Lab discovers Adobe Flash zero day used in the wild by a threat actor to deliver spyware.
Business Wire. (2018, October 11). Malawi's network operators adjust to SIM card registration deadline.
Business Wire. (2020, May 14). Analysis of Mozambique's telecoms, mobile & broadband markets, 2020—Includes an impact assessment of COVID-19 on the global telecoms sector.
Canada NewsWire. (2007, November 5). Tunisia—A textbook case in press censorship for the past 20 years.
Canada Stockwatch. (2009, June 8). MN March Networks to provide VideoSphere to South Africa.
Canadian Press. (2015, October 15). Report: Poorer, smaller nations investing in cyberespionage tools despite leaks, lawsuits.
Capital FM. (2023, July 31). Communications Authority of Kenya Boss Chiloba Says SIM Card Registration Compliance at 97%.
Center for Human Rights & Global Justice (CHRGJ). (2022). *Paving a digital road to hell: A primer on the role of the World Bank and global networks in promoting digital ID*. New York University.
Charity, N. (2018, November 1). Tanzania taskforce to start 'witch hunt' to round up and imprison LGBT community. *London Evening Standard*.
Chimhangwa, K. (2022, June 13). How Artificial Intelligence could influence Zimbabwe's 2023 elections. *Global Voices*.
Cohen, T. (2009, March 26). "Illicit" Phone Taps of Mbeki Part of Zuma's Plea to NPA. *All Africa*.
Choi, T. (2022, May 17). Concerns raised as Uganda plans DNA upgrade for biometric ID cards. *Biometric Update*.
Chown, M. (2020, June 22). Moroccan authorities suspected of using 'invisible' technique to hack journalist's phone. *Toronto Star*.
Coker, M., & Sonne, P. (2011, December 14). Censorship Inc.: Life under the gaze of Gadhafi's spies. *The Wall Street Journal*.
Coker, M., & Sonne, P. (2012, July 3). Gadhafi-era spy tactics quietly restarted in Libya. *The Wall Street Journal*.
Collaboration on International ICT Policy for East and Southern Africa (CIPESA). (2022). *Privacy imperilled: Analysis of surveillance, encryption, and data localization laws in Africa*. CIPESA.
Dadoo, S. (2021, March 2). Botswana uses Israeli cyberespionage tools. *All Africa*.
Daily Trust. (2020, February 17). How Nigeria's Police Used Telecom Surveillance to Lure, Arrest Journalists.
Dahir, A. L. (2018, April 10). You now have to pay the government over $900 a year to be a blogger in Tanzania. *Quartz*.
Dahir, A. L. (2021, December 5). Spyware hacks in Uganda expand to journalists and opposition figure. *The New York Times*.
Dawa, M. (2024, May 7). Tanzania's new VPN policy leaves LGBTQ+ individuals exposed. *Global Voices*.

Deutsche Presse-Agentur. (2021, October 16). Anger and accusations worldwide as Pegasus spy scandal deepens.
ENP Newswire. (2016, October 18). Huawei hosts safe city summit in Africa to showcase industry best practices.
Erasmus, C. (2021, October 1). Questions as rogue elements in South African agency spy on 'everyone.' *The Nation*.
European Ombudsman. (2022). *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)*. European Ombudsman.
Finnan, D. (2015, July 20). Kenyan government asked Hacking Team to attack dissident website. *Radio France Internationale*.
Freddy, T. (2023, December 19). Unmanned Border Posts By Next Year. *The Herald*.
Gemalto delivers enrolment solution for Benin's upcoming presidential elections. (2010, October 5). *ENP Newswire*.
Ghana Today. (2024, December 4). Vice President Bawumia Launches Digital Border Control System, E-Gates At Kotoka Airport.
Gibbs, S. (2015, July 13). Hacking Team boss: We sold to Ethiopia but 'we're the good guys.' *The Guardian*.
Gonzalez, B. (2024, February 20). Airport face biometrics systems arrive in Philippines, Nigeria and Spain. *Biometric Update*.
Gross, A., Murgia, M., & Yang, Y. (2019, October 26). Chinese tech shapes UN standards. *Financial Times*.
GSM Association (GSMA). (2021). *Access to mobile services and proof of identity 2021: Revisiting SIM registration and Know Your Customer (KYC) contexts during COVID-19*. GSMA.
Gwagwa, A. E., & Hove, K. (n.d.). *Use of IMSI catchers in Zimbabwe's domestic law enforcement*.
Hajjaj, D. (2019, July 3). Moroccan Independent Journalists Describe Climate of Pervasive Surveillance, Harassment. *All Africa*.
Hao, K., & Swart, H. (2022, April 19). South Africa's private surveillance machine is fueling a digital apartheid. *MIT Technology Review*.
Hersey, F. (2020a, March 8). Biometrics and digital ID in Africa this week: Increasing CCTV surveillance, new ID document contracts. *Biometric Update*.
Hersey, F. (2020b, August 31). Idemia biometrics secures Africa's largest welfare transfer system as Nigeria unites identity-handling agencies. *Biometric Update*.
Hersey, F. (2021a, June 17). Simprints adds facial recognition to Mozambique land ownership records. *Biometric Update*.
Hersey, F. (2021b, July 16). Millions excluded as Uganda uses national digital ID system for emergency COVID welfare. *Biometric Update*.
Hersey, F. (2021c, July 23). UN finds storing biometric data on Mauritius ID cards violates privacy. *Biometric Update*.
Hersey, F. (2022a, March 11). Côte d'Ivoire final push for biometric registration as third national ID extension deadline approaches. *Biometric Update*.

Hersey, F. (2022b, December 12). Guinea to introduce biometric land management with Datasonic. *Biometric Update*.
Hersey, F. (2022c, December 9). Malawi's biometric ID approaches total coverage, huge cost savings. *Biometric Update*.
Hersey, F. (2022d, December 8). Mandatory SIM-ID link fever spreads as Namibia unveils registration dates. *Biometric Update*.
Hersey, F. (2022e, July 29). NGOs sue Idemia for failing to consider human rights risks in Kenyan digital ID. *Biometric Update*.
Hersey, F. (2022f, December 21). Tanzanians urged to check biometrically registered SIMs, tidy links before January cut off. *Biometric Update*.
Hersey, F. (2022g, October 6). Ugandan digital ID on trial: High court requests expert witness while AG denies exclusion. *Biometric Update*.
Hersey, F. (2022h, October 19). Unregistered SIM blocking: Kenyans get another 60 days, Ghanaians have till end of October. *Biometric Update*.
How surveillance, trolls, and fear of arrest affect Egypt's journalists. (2017, June 14). *News Press*.
Human Rights Watch (HRW). (2014). *They know everything we do: Telecom and internet surveillance in Ethiopia*. HRW.
Hunter, M. (2014, November 11). Rica in South Africa—How big is Big Brother? *All Africa*.
Kapiyo, V., Oyier, C., & Monyango, F. (2024). *Surveillance laws and technologies used in countering terrorism and their potential impact on civic space*. Kenya ICT Action Network (KICTANet).
Karapetyan, S. (2021a, December 9). Biometric entryway at Seychelles' airport heralds era of "your face as a passport." *Seychelles News Agency*.
Karapetyan, S. (2021b, December 28). Seychelles signs contract for biometric passports, expected end of 2022. *Seychelles News Agency*.
Khan, I. A. (2019, October 15). Snooping on citizens—How an Israeli company might come to determine our politics. *L'Express*.
Katusiime, I. (2021, October 16). Uganda's next war. *All Africa*.
King, R. (2016, May 25). Rwanda to introduce new eID card. *Biometric Update*.
Kirchgaessner, S., & Taylor, D. (2022, July 18). Nephew of jailed Hotel Rwanda dissident hacked by NSO Spyware. *The Guardian*.
Latham, D. (2020, October 26). Africa's technological arms race. *All Africa*.
Lee, J. (2017a, June 5). Laxton Group to supply biometric voter registration kits for Zimbabwe elections. *Biometric Update*.
Lee, J. (2017b, July 9). Gemalto biometric passports are being used in over 30 different countries. *Biometric Update*.
Lee, K. (2021, November 5). Spyware for sale: The booming trade in surveillance tech. *Agence France-Presse*.
Lee, R. (2014, February 19). Nation's dire human rights situation. *All Africa*.
Links, F. (2018, March 15). The Rise of the Namibian surveillance state. *The Namibian*.
Links, F. (2022, August 14). Greatly undermining privacy rights – Part 2. *The Namibian*.

Loveluck, L. (2014, June 30). Citing terrorism, Egypt to step up surveillance of social media. *The Christian Science Monitor*.
M2 Presswire. (1995, December 6). PRIVACY INTL: Report uncovers massive intl surveillance trade funded by arms industry & led by UK.
M2 Presswire. (2017, May 10). Smart Africa Alliance and Inmarsat developing blueprint for digital services across the continent.
M2 Presswire. (2021, October 7). Togo: Prominent Activist Targeted with Indian-made Spyware Linked to Notorious Hacker Group.
M2 Presswire. (2022, March 9). Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months—new evidence.
Macdonald, A. (2021a, June 15). Biometric registration drive in Kenya for health insurance scheme. *Biometric Update*.
Macdonald, A. (2021b, January 26). Digital driver's license for Nigerians requires biometrics-backed NIN. *Biometric Update*.
Macdonald, A. (2021c, November 15). Nigeria counts on biometrics to recapture nearly 4K fleeing jail-breakers. *Biometric Update*.
Macdonald, A. (2021d, July 6). Nigeria to add 6M students to biometric database for school meal program. *Biometric Update*.
Macdonald, A. (2021e, November 2). Nigerian digital ID registrations reach 66M, SIM linkage deadline extended. *Biometric Update*.
Macdonald, A. (2021f, March 2). Nigerian State makes digital ID numbers mandatory to access government services. *Biometric Update*.
Macdonald, A. (2021g, May 24). Trust lacking as African digital ID systems expand. *Biometric Update*.
Macdonald, A. (2022a, August 18). Biometric audit finds thousands of 'ghost workers' on Ghana's public service payroll. *Biometric Update*.
Macdonald, A. (2022b, February 22). Biometrics implementations for public uses expanding in Nigeria. *Biometric Update*.
Macdonald, A. (2022c, March 14). Biometrics registration for Zambia's new national ID system underway. *Biometric Update*.
Macdonald, A. (2022d, March 8). Cameroon seeks escape from its biometric national ID card woes. *Biometric Update*.
Macdonald, A. (2022e, August 4). Ghana imposes fee for biometric SIM registration with self-service app. *Biometric Update*.
Macdonald, A. (2022f, February 21). Ghana telcos trying to facilitate biometric SIM registrations as diverse concerns grow. *Biometric Update*.
Macdonald, A. (2022g, September 27). Kenya to comply with regional bloc directive on biometric passports from end November. *Biometric Update*.
Macdonald, A. (2022h, April 21). Kenya wants to use Huduma Namba digital ID system to tackle tax evasion. *Biometric Update*.
Macdonald, A. (2022i, February 3). Kenyan telco requires face biometrics for SIM card re-registration. *Biometric Update*.

Macdonald, A. (2022j, June 27). National digital ID to be launched by Senegal, legislative foundation proposed for Finland. *Biometric Update*.
Macdonald, A. (2022k, April 19). New Nigerian data protection body calls for stronger privacy standards to drive digital ID. *Biometric Update*.
Macdonald, A. (2022l, July 7). Nigeria deploying biometrics to prevent manipulation in upcoming population census. *Biometric Update*.
Macdonald, A. (2022m, July 20). Nigeria issues 700K biometric bank verification numbers between April and July 2022. *Biometric Update*.
Macdonald, A. (2022n, June 8). Nigerian state to begin biometric identification in transport sector to improve security. *Biometric Update*.
Macdonald, A. (2022o, March 15). Security agencies granted access to Nigeria's biometric database; Buhari faces lawsuit. *Biometric Update*.
Macdonald, A. (2022p, August 8). The Gambia launches new biometric CRVS and health insurance scheme. *Biometric Update*.
Macdonald, A. (2022q, April 25). Zimbabwe opts for biometrics to fight fraud in issuance of land title deeds. *Biometric Update*.
Macdonald, A. (2023a, July 27). Benin issues digital IDs to citizens living abroad. *Biometric Update*.
Macdonald, A. (2023b, April 24). Biometric SIM registration soon in Mozambique, Ghana orders block of unlinked lines. *Biometric Update*.
Macdonald, A. (2023c, December 21). Biometric verification system fails to distinguish identical twins in Ghana local elections. *Biometric Update*.
Macdonald, A. (2023d, February 27). Biometrics used at 98% of Nigerian polls; advocates concerned for safety of voters' data. *Biometric Update*.
Macdonald, A. (2023e, August 31). Cameroon biometric visa portal down, Burkina Faso launches own platform. *Biometric Update*.
Macdonald, A. (2023f, September 1). Equatorial Guinea, Ghana want to flush out 'ghost' public workers using biometrics. *Biometric Update*.
Macdonald, A. (2023g, July 12). Ethiopia to make digital ID obligatory for banking operations. *Biometric Update*.
Macdonald, A. (2023h, February 14). France probes Thales subsidiary over past ID deals in Africa. *Biometric Update*.
Macdonald, A. (2023i, May 1). Gabon hopes to deliver on its lingering national ID card promise this year. *Biometric Update*.
Macdonald, A. (2023j, December 14). Ghana plans digital version of national ID card to simplify authentication. *Biometric Update*.
Macdonald, A. (2023k, September 7). Ghana starts follow-up nationwide biometric ID card enrollment drive. *Biometric Update*.
Macdonald, A. (2023l, August 22). Ghana, Zambia plan biometric voter registration drives for September. *Biometric Update*.
Macdonald, A. (2023m, April 25). Healthcare apps, biometric ID cards integrated for service access in Ghana, India, Japan. *Biometric Update*.

Macdonald, A. (2023n, June 28). IrisGuard biometrics to support Ethiopia's G2C payments, financial inclusion. *Biometric Update*.
Macdonald, A. (2023o, October 9). Italy okays digital ID for SIM activation, Namibia and Mauritania race to meet deadlines. *Biometric Update*.
Macdonald, A. (2023p, August 1). Kenya targets Feb. 2024 for new digital ID rollout, sign-up optional. *Biometric Update*.
Macdonald, A. (2023q, November 13). Kenyan court blocks govt move to hike ID card, passport fees. *Biometric Update*.
Macdonald, A. (2023r, August 21). Liberia's low biometric national ID card renewal rate bemoaned by authorities. *Biometric Update*.
Macdonald, A. (2023s, July 25). Mistrust in Liberia's biometric voter registration system is high, survey claims. *Biometric Update*.
Macdonald, A. (2023t, October 19). Nigeria launches cash transfers with biometric ID verification for 15m households. *Biometric Update*.
Macdonald, A. (2023u, November 10). Nigeria launches digital CRVS platform built by private partner. *Biometric Update*.
Macdonald, A. (2023v June 15). Nigeria now has a data protection legislation after years of back and forth. *Biometric Update*.
Macdonald, A. (2023w, August 9). Nigeria signs MOU on biometric cards for payments in healthcare, agriculture. *Biometric Update*.
Macdonald, A. (2023x, September 5). Nigeria to strengthen digital ID enrollment operations to ease access to govt services. *Biometric Update*.
Macdonald, A. (2023y, August 23). Nigeria's Borno State to capture biometrics of nearly 7k ex-Boko Haram fighters. *Biometric Update*.
Macdonald, A. (2023z July 4). Report finds data protection loopholes in Tanzania's biometric SIM registration drive. *Biometric Update*.
Macdonald, A. (2023aa, January 19). Sierra Leone hikes fees for obtaining biometric ID documents. *Biometric Update*.
Macdonald, A. (2023ab, December 15). South Africa fixes date for final round of voter registration ahead of 2024 general polls. *Biometric Update*.
Macdonald, A. (2023ac, July 18). Tanzanian govt underlines importance of new digital ID system in the offing. *Biometric Update*.
Macdonald, A. (2023ad, September 12). Technical report declares Liberia's biometric voter registration exercise a success. *Biometric Update*.
Macdonald, A. (2023ae, May 4). Togo preparing census to issues biometric ID cards for social protection. *Biometric Update*.
Macdonald, A. (2023af, June 6). Uganda plans biometric gates at land borders to control trade fraud. *Biometric Update*.
Macdonald, A. (2023ag, November 16). Uganda procuring biometric devices for 2024 census. *Biometric Update*.
Macdonald, A. (2023ah, November 29). Uganda suspends over 1.4M SIM cards not linked to users' biometrics. *Biometric Update*.

Macdonald, A. (2023ai, December 14). Ghana plans digital version of national ID card to simplify authentication. *Biometric Update*.
Macdonald, A. (2024a, April 18). Cameroon bishops urge massive participation in ongoing biometric voter registration. *Biometric Update*.
Macdonald, A. (2024b, March 25). Cameroon wants €50M to expand facial recognition surveillance project. *Biometric Update*.
Macdonald, A. (2024c, July 22). Coppernic biometric tablets selected for Guinea scholarship program modernization. *Biometric Update*.
Macdonald, A. (2024d, January 29). Govt source says Kenya's biometric national ID card chip expiry protects security. *Biometric Update*.
Macdonald, A. (2024e, July 23). Groups reject expiry date for digital ID cards in Kenya as govt defends move. *Biometric Update*.
Macdonald, A. (2024f, January 4). Liberia lauds Nigeria for support on biometric voter registration. *Biometric Update*.
Macdonald, A. (2024g, March 26). MPs challenge proposal to spend $15M on Ghana Cards for children. *Biometric Update*.
Macdonald, A. (2024h, June 24). Namibia begins issuance of much-anticipated biometric ID cards to refugees. *Biometric Update*.
Macdonald, A. (2024i, March 15). Nigeria, Rwanda use digital ID for social welfare payments. *Biometric Update*.
Macdonald, A. (2024j, April 18). Nigerians decry duplicative biometric capture for SIM registration, ID cards, SIM-NIN linkage... *Biometric Update*.
Macdonald, A. (2024k, June 25). Nigeria's NIMC fights off data breach accusations, flags 5 data harvesting websites. *Biometric Update*.
Macdonald, A. (2024l, July 8). Report points out personal data protection lapses in Botswana. *Biometric Update*.
Macdonald, A. (2024m, April 11). Sierra Leone putting digital ID at the center of its digital transformation agenda. *Biometric Update*.
Macdonald, A. (2024n, January 11). Sierra Leone urges citizens to obtain biometric ID cards for security, services. *Biometric Update*.
Macdonald, A. (2024o, January 11). South Africa to add biometrics to new driving license cards, maintains plan for mDLs. *Biometric Update*.
Macdonald, A. (2024p, April 3). The Gambia reaches 1.17M birth registration milestone with World Bank support. *Biometric Update*.
Macdonald, A. (2024q, February 26). World Bank gives South Sudan $10M for biometrics to ID govt payroll thieves. *Biometric Update*.
Macdonald, A. (2024r, July 8). World Bank supports Mozambique to scale up free issuance of national ID cards. *Biometric Update*.
Macdonald, A. (2024u, April 26). Criticisms as Uganda orders ID verification for digital financial transactions of $260 and above. *Biometric Update*.
Macdonald, A. (2024v, August 6). Malawi insists ID card compulsory for scheduled biometric voter registration. *Biometric Update*.

Macdonald, A. (2024w, October 28). Benin receives 2,050 biometric terminals from World Bank to boost civil registration. *Biometric Update*.
Macdonald, A. (2024x, November 4). Cameroon squares up to its payroll fraud conundrum with biometric verification. *Biometric Update*.
Macdonald, A. (2024y, November 18). 18M Ghanaians on biometric voter register for December 7 elections. *Biometric Update*.
Macdonald, A. (2024z, December 10). Central African Republic enrols citizens for first local elections in 36 years. *Biometric Update*.
Macdonald, A. (2024aa, September 17). Rwanda conducts pilot to implement biometric SIM registration, verification. *Biometric Update*.
Macdonald, A. (2024ab, September 10). Cameroon ends 2024 biometric voter registration drive with 755k new enrollments. *Biometric Update*.
Macdonald, A. (2024ac, September 29). Laxton to accompany Ethiopia on 90M digital ID target by 2030. *Biometric Update*.
Macdonald, A. (2025a, January 15). Biometric voter registration underway in Gabon ahead of presidential vote. *Biometric Update*.
Macdonald, A. (2025b, January 20). Somalia officially launches printing process of new national ID card. *Biometric Update*.
Magcaba, B. (2023, July 16). SAPS introduces drones for enhanced police visibility and suspects tracking. *South African Broadcasting Corporation*.
Malsin, J., & El-Fekki, A. (2019, October 8). Egypt tries to quell online dissent. *The Wall Street Journal*.
Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., & Deibert, R. (2017a). *Champing at the Cyberbit: Ethiopian dissidents targeted with new commercial spyware*. Citizen Lab.
Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014). *Mapping Hacking Team's untraceable spyware.* Citizen Lab.
Marczak, B., Scott-Railton, J., & McKune, S. (2015). *Hacking Team and the targeting of Ethiopian journalists*. Citizen Lab.
Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2018). *Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries*. Citizen Lab.
Marczak, B., Scott-Railton, J., Perry, A., Al-Jizawi, N., Anstis, S., Panday, Z., Lyon, E., Razzak, B. A., & Deibert, R. (2023). *Sweet QuaDreams: A first look at spyware vendor QuaDream's exploits, victims, and customers.* Citizen Lab.
Marczak, B., Scott-Railton, J., Rao, S. P., Anstis, S., & Deibert, R. (2017b). *Running in Circles: Uncovering the clients of cyberespionage firm Circles*. Citizen Lab.
Marczak, B., Scott-Railton, J., Razzak, B. A., Al-Jizawi, N., Anstis, S., Berdan, K., & Deibert, R. (2021). *FORCEDENTRY: NSO Group iMessage zero-click exploit captured in the wild*. Citizen Lab.
Marczak, B., Scott-Railton, J., Senft, A., Poetranto, I., & McKune, S. (2015). *Pay no attention to the server behind the proxy: Mapping FinFisher's continuing proliferation*. Citizen Lab.
Marks, J. (2019, August 15). The Cybersecurity 202: How Huawei helped extend China's repressive view of Internet freedom to African nations. *The Washington Post*.

Marquis-Boire, M. (2012). *Backdoors are forever: Hacking Team and the targeting of dissent.* Citizen Lab.
Marquis-Boire, M., Marczak, B., & Scott-Railton, J. (2013). *You Only Click Twice: FinFisher's Global Proliferation*. Citizen Lab.
Mascellino, A. (2023, May 12). ECOWAS Commission urges remaining 9 member states to issue biometric regional ID card. *Biometric Update*.
Matsiko, H. (2015, October 26). Spying On Wrong 'Enemy.' *All Africa*.
Mayhew, S. (2017, November 15). 9M enrolled in Malawi identity program. *Biometric Update*.
Mayhew, S. (2018, May 28). Mozambique deploys Laxton Group biometric voter registration solution. *Biometric Update*.
Mayhew, S. (2019a, January 14). Gemalto wins contract for biometric border management system in Uganda. *Biometric Update*.
Mayhew, S. (2019b, February 11). Ugandan police deploy Gemalto tech for rapid capture of suspects' biometric data. *Biometric Update*.
Mayhew, S. (2019c, March 24). Kenya completes biometric data collection of police as public registration exercise set to begin. *Biometric Update*.
Mbuthia, B. (2023, November 8). More pain for Kenyans as gov't raises ID, passport application costs by over Ksh.3,000. *Citizen*.
McConvey, J. R. (2023, September 14). Ethiopia rolls out student IDs, integrates biometric data to issue Fayda. *Biometric Update*.
McCurdy, W. (2023, July 7). National ID cards launched in DRC, remain uncollected in Ghana. *Biometric Update*.
Motlogelwa, T. (2008, July 10). Media uneasy over Sim-card registration. *All Africa*.
Msemo, M. (2022, October 25). 'Gone like it was nothing': The irrepressible rise of mobile scams. *African Arguments*.
Munhende, L. (2021, August 13). Government approves massive surveillance for Bulawayo. *New Zimbabwe*.
Muriuki, B. (2024, February 23). Gov't announces issuance of Maisha Cards to resume immediately. *Citizen*.
Muriuki Kithinji, P., Gathecha, V., & Chepkemoi, C. (2023). *Nairobi diagnostic report*. Edgelands Institute.
Mutisi, J. (2022, November 2). Surveillance technology needs a national policy. *The Standard (Harare)*.
Namibia Economist. (2024, April 4). Mandatory SIM Card Registration Deadline Concludes.
Nash, J. (2022, June 14). CloudWalk has Zimbabwean's face biometrics, but trust in voter roll still lacking. *Biometric Update*.
Ndlela, D. (2020a, March 1). Creating a surveillance state: ED govt zooms in for critics with Chinese help. *The Standard*.
Ndlela, D. (2020b, June 22). Privacy violations fears grow as govt sets surveillance cameras in cities. *All Africa*.
Neugeboren, E. (2020, June 29). Pegasus spyware targets journalist. *Voice of America*.
NF News. (2019, December 3). China to scan every mobile user's face.
NF News. (2021, April 15). Mexico to join countries that require biometric registration.

NF News. (2021, August 15). Analysts: China expanding influence in Africa via telecom network deals.
NF News. (2021, December 3). Pegasus developer investigates reports that spyware targeted US diplomats.
NF News. (2021, July 20). Macron, in the crosshairs of the Pegasus spy program hired by Morocco.
NF News. (2021, May 31). Unfeasible, cell phone roll with biometric data: Experts.
NF News. (2022, December 8). How the global spyware industry spun out of control.
NF News. (2022, January 27). China has colonized half the world with its foreign development program.
NF News. (2022, May 6). Pegasus, naked: A silent intruder with self-destruct button.
Nurse, N. (2017, September 13). How the NSA built a secret surveillance network for Ethiopia. *The Intercept*.
Ogala, E. (2014, February 11). U.S. spy program reforms spotlight Nigeria's expanding surveillance program. *All Africa*.
Ogala, E. (2015a, July 9). Bayelsa governor hires world's most ruthless hackers for N100M to hack computers, phones in Nigeria. *Premium Times*.
Ogala, E. (2015b, July 13). Investigation—Bayelsa governor distributes gifts of compromised Blackberry phones, then hacks beneficiaries. *All Africa*.
Ogala, E. (2016, June 9). Investigation—How governors Dickson, Okowa spend billions on high tech spying on opponents, others. *Premium Times*.
Oluka, B. H. (2015, October 19). Govt spends shs 200 billion on spying gadgets. *All Africa*.
Opiah, A. (2024a, July 30). Madagascar's $143M Prodigy initiative to advance digital identity infrastructure. *Biometric Update*.
Opiah, A. (2024b, August 2). Mauritania launches digital ID app to boost access to services and improve governance. *Biometric Update*.
Opiah, A. (2024c, November 4). 25M Nigerian poor get cash payments enabled by digital ID. *Biometric Update*.
Ouma, M. (2015, July 13). Wikileaks—Hacking Team declined Kenya govt's request to bring down Kahawatungu blog. *All Africa*.
Pascu, L. (2020, August 19). Face biometric authentication for social welfare approved by Morocco's data protection authority. *Biometric Update*.
Perlroth, N. (2013, March 15). Evidence of spyware found in 25 countries. *International Herald Tribune*.
Peterson, A. (2015, March 9). Ethiopia spies on journalists based in Va., researchers say. *The Washington Post*.
Popoviciu, A. (2023, July 26). How Europe outsourced border enforcement to Africa. *In These Times*.
PR Newswire. (2018, July 26). KT builds digital system for national identification in Tanzania.
PR Newswire. (2020, August 7). The data center construction industry in Africa, 2020-2025.
PressWire. (2016, March 31). Magora app technology: Helping one despot at a time.
Privacy International. (2015a). For God and my president: State surveillance in Uganda. Privacy International.

Privacy International. (2015b). *Their eyes on me: Stories of surveillance in Morocco*.
Privacy International. (2015c). *Uganda's grand ambitions of secret surveillance*. Privacy International.
Privacy International. (2017a). *New documents reveal Kenya's worrying attempts to monitor the internet.* Privacy International.
Privacy International. (2017b). *Track, capture, kill: Inside communications surveillance and counterterrorism in Kenya*. Privacy International.
Privacy International. (2019a). *Africa: SIM card registration only increases monitoring and exclusion*. Privacy International.
Privacy International. (2019b). *Inside Niger's new biometric voting system.* Privacy International.
Privacy International. (2019c). *State of Privacy Egypt*. Privacy International.
Privacy International. (2019d). *State of Privacy Kenya*. Privacy International.
Privacy International. (2019e). *State of Privacy Morocco*. Privacy International.
Privacy International. (2019f). *State of Privacy South Africa*. Privacy International.
Privacy International. (2019g). *State of Privacy Tunisia*. Privacy International.
Privacy International. (2019h). *State of Privacy Uganda*. Privacy International.
Privacy International. (2019i). *Timeline of SIM Card Registration Laws*. Privacy International.
Privacy International. (2019j). *Two states admit bulk interception practices: Why does it matter?* Privacy International.
Putsch, C. (2019, October 26). Africa, the Huawei Continent. *Die Welt*.
Radio France Internationale. (2023, October 20). Malagasy Leader Rajoelina Says Opposition Is Seeking to Derail Elections.
Regulatory News Service. (2020, December 16). Airtel Africa PLC Nigeria new SIM registration rules.
Reuters. (2010, November 10). EU criticised over surveillance aid in nations where privacy at risk.
Reuters. (2021, July 29). Ugandan opposition, activists denounce digital car tracker plan.
Reuters. (2023, January 4). Feature—CCTV cameras will watch over Egyptians in new high-tech capital.
Resian, S. (2024, December 19). High Court Extends Suspension of KRA, CA Directives On Mobile Device IMEI Declaration. *Capital FM*.
Roberts, T. (Ed.). (2021). *Digital rights in closing civic space: Lessons from ten African countries*. Institute of Development Studies.
Roberts, T., Gitahi, J., Allam, P., Oboh, L., Oladapo, O. A., Appiah-Adjei, G., Galal, A., Kainja, J., Phiri, S., Abraham, K., Klovig Skelton, S., & Sheombar, A. (2023). *Mapping the supply of surveillance technologies to Africa: Case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia*. Institute of Development Studies.
Robertson, T. (2020, December 1). Mauritius's newly introduced tax on online services threatens freedom of expression. *All Africa*.
Rotich, K. (2024, November 5). Passengers Entering Kenya Must Declare Mobile Devices, Says KRA. *Capital FM*.
Sackey, S., & Mahama, A. (2010, June 16). Haruna Iddrisu: No phone tapping. *All Africa*.

Salako, F. (2025, January 12). Securing Nigeria's Borders—The Transformative Impact of E-Surveillance. *Vanguard*.
Scott-Railton, J., Anstis, S., Chan, S., Marczak, B., & Deibert, R. (2020). *Nothing sacred: Religious and secular voices for reform in Togo targeted with NSO spyware*. Citizen Lab.
Scott-Railton, J., Raoof, R., Marczak, B., & Maynier, E. (2017). *Nile Phish: Large-scale phishing campaign targeting Egyptian civil society*. Citizen Lab.
Shezaf, H. (2018, October 19). Revealed: Israel's cyber-spy industry aids world dictators hunt dissidents and gays. *Haaretz*.
Solomon, S. (2019, November 14). In Uganda, Dissidents adapt to evade Huawei assisted government spying. *Voice of America*.
Solon, O. (2024, June 4). Uganda: Yoweri Museveni's critics targeted via biometric id system. *Bloomberg*.
Sputnik News. (2016, February 26). Europe sold surveillance technology to Egypt—Privacy International.
Sputnik News. (2018, March 27). 'Not conducive to democracy'—Cambridge Analytica whistleblower.
Stevis, M. (2015, July 8). Government brutality sparks Eritrean exodus, U.N. report says. *The Wall Street Journal*.
Sunday Standard. (2014, September 15). DISS/MI launch electronic warfare attacks against private media.
Sunday Standard. (2018, October 21). Khama/Kgosi network of shady intelligence security bigshots has DISS over a barrel.
Swinhoe, D. (2023, November 8). Orange to build data center in Egypt's new capital. *Data Center Dynamics*.
Tekle, T.-A. (2013, April 2). Ethiopia using spyware to monitor political activists—Report. *All Africa*.
The Namibian. (2022, November 1). Kavekotora warns of govt phone-spying abuse.
This Day. (2022, February 7). Data collections and citizen protection.
Tungali, A. (2021). *Surveillance of public spaces and communications in the Democratic Republic of the Congo*. Media Policy and Democracy Project.
Uwerunonye, N. (2017, November 8). DSS bugs 70% of mobile phones in Abuja. *The Independent (Nigeria)*.
Valentino-DeVries, J., Angwin, J., & Stecklow, S. (2011, November 19). Censorship Inc.: Document trove exposes surveillance methods. *The Wall Street Journal*.
Van Der Made, J. (2021, July 22). Chinese tech, ignored by the West, is taking over Africa's cyberspace. *Radio France Internationale*.
Verde, R. S. (2021). *Israeli involvement in electronic surveillance in Angola: A step towards transparency or the sophistication of illegal practices?* African Studies Centre, University of Oxford.
Vermeer, A. (2014, February 20). Surveillance follows Ethiopian political refugee to the UK. *All Africa*.
Wangari, N. (2023, November 8). In Africa's first 'safe city,' surveillance reigns. *Coda Story*.
Wanjala, E. (2022, September 1). How to apply for digital number plates. *The Star*.

Wexler, A. E., & Akingbule, G. (2015, November 10). MTN chief resigns after huge fine. *The Wall Street Journal*.
Woodhams, S. (2019, September 13). Huawei, Africa and the global reach of surveillance technology. *Deutsche Welle*.
Wright, O. (2019, August 9). Tanzania condemned after arrest of journalist Erick Kabendera. *The Times*.
Wrong, M. (2021, July 26). Rwandans have long been used to Pegasus-style surveillance. *The Guardian*.
Zhangazha, W. (2015, November 7). Govt intensifies crackdown on dissenting voices. *All Africa*.
Zulu, B. (2020, April 23). Biometric citizen identification to enhance voter registration and identification in Zambia. *Biometric Update*.