Government Digital Surveillance in Africa[1]

Karol Czuba

[1] This is an Accepted Manuscript of an article published by Wiley in *Governance*, available online at https://doi.org/10.1111/gove.70049.

Abstract

Deployment of digital surveillance technologies has enabled governments to acquire detailed, precise, synoptic, and—in settings where capacity and resource constraints had historically impeded state information-gathering efforts—previously inaccessible knowledge about populations. This article introduces a new typology of government digital surveillance and multiple sets of data that provide extensive evidence—the most comprehensive and systematic to date—of the deployment of digital surveillance technologies by African governments. I identify and classify 372 distinct instances of government digital surveillance in Africa, detailing which governments have deployed it; where, when, and whom they have surveilled; the purposes and manner of deployment; and the technological solutions procured to this end as well as their suppliers. The article illuminates the scale and breadth of government use of digital surveillance technologies, advancing our understanding of the political ramifications of digitalization and informing investigation of consequent changes in government performance and state-society relations.

Keywords: surveillance, digital surveillance, government digital surveillance, digitalization, Africa

Government Digital Surveillance in Africa

Technological innovations brought about by digitalization have substantially reduced the difficulty and cost of surveillance—that is, "the gathering of information through the identification, tracking, monitoring, and analysis of individuals, data, organizations, or systems" (Feldstein, 2021, p. 27)—facilitating the expansion of governments' knowledge about populations, a development especially momentous in settings where capacity and resource constraints had historically hindered efforts to increase the legibility of society to the state. In this article, I document the deployment of digital surveillance technologies by African governments, which have taken advantage of the opportunities offered by digitalization to acquire detailed, precise, synoptic—and hitherto unobtainable—knowledge about the continent's inhabitants. While a growing scholarly literature has examined government digital surveillance elsewhere (e.g. Büchi et al., 2022; Feldstein, 2021; Gohdes, 2024), in the African context, where only a few contributions (e.g. Nyabola, 2018; Roberts et al., 2023)—most of them also limited in geographic and topical scope—have addressed this phenomenon, key questions remain unanswered: Which African governments have adopted digital surveillance technologies? When did they do so? What are the targets and purposes of government deployment of such technologies? What forms has government digital surveillance taken? What surveillance tools have governments obtained, and from what suppliers?

To answer these questions, I have reviewed news media reports catalogued in the Factiva repository and other media databases as well as relevant non-media publications, collated multiple datasets that supplement the article, and developed a new typology of government digital surveillance. The typology distinguishes the locations, implementation statuses and timeframes, targets, purposes—both stated by governments and imputed by observers—types, and modalities of government digital surveillance as well as the technological solutions, and developers thereof, that make it possible. I use the typology to categorize the data collected for the article, which provides the most extensive, detailed, and systematic evidence of government digital surveillance in Africa to date.

My analysis reveals 372 distinct instances of digital surveillance technology deployment for political purposes, began primarily in the 2010s and 2020s and generally fully implemented by the time of reporting, by the governments of 49 African countries. Responsible authorities have typically surveilled entire populations or, less frequently, discrete segments of society such as ethnic or sexual minorities; individual government adversaries—civil society activists, journalists, and political opponents—are the targets of surveillance in less than a quarter of the reported instances. Most instances involve mass and oftentimes continuous surveillance through mandatory registration of persons and their electronic devices, capture of telephony data and metadata, filtering and monitoring of internet traffic, and deployment of closed-circuit television (CCTV) systems. To surveil specific targets, governments repurpose passively collected mass surveillance data or deploy dedicated technological solutions such as data extraction spyware, although reports of such mass-to-targeted and targeted surveillance are comparatively rare. While official statements attribute government digital surveillance to efforts to improve security condi-

tions, administrative quality, and service provision, critics suggest that it serves to expand state control over society, restrict civil rights, and suppress civil society, media reporting, and political opposition.

In documenting government deployment of digital surveillance technologies in Africa the article makes both conceptual and empirical contributions. Development of the typology introduced in the article has required conceptualization of important aspects of government digital surveillance—such as surveillance modalities and the distinction between stated and imputed purposes—that have till now escaped scholarly scrutiny. By sorting these and other aspects of government digital surveillance into discrete categories, the typology also enables more accurate, detailed, and precise description of deployments of digital surveillance technologies in different settings. In the African context, I employ the typology to draw inferences from the extensive data I have collected to reveal the large scale and wide spatial diffusion of government digital surveillance on the continent, the rapidity of government adoption of digital surveillance technologies, the multiplicity of the purposes of deployment—as well as the scope of contention about them—the vast number and variety of surveillance targets, and the expansive range of means used to monitor those targets. Accordingly, the article advances the literature on government digital surveillance—and on the political ramifications of digitalization more broadly—by substantially expanding the base of empirical evidence on this increasingly important political phenomenon. The implications of government adoption of digital surveillance technologies bear out this importance, as increased visibility, and legibility, of society to the state has the potential to enhance the capacity to perform government functions and alter the balance of power between the state and society.

Digital Technologies and Government Surveillance

The "administrative power generated by the nation-state could not exist without the information base" (Giddens, 1985, p. 180) derived largely from surveillance activities. Historically, large-scale surveillance needed to build such a base required the allocation of considerable resources, a level of capacity few states attained, and a strong imperative to increase societal legibility (Scott, 1998, p. 513–514). These conditions rarely obtained in Africa, where the generally low-capacity and resource-strapped states—unable "track the individual body or understand the dynamics of the social body" (Cooper, 1996, p. 335)—"were built in an informational void" (Breckenridge, 2014, p. 5). Digitalization has made it possible to fill this void. It "has expanded the precision, resolution, and nature of information" (Gohdes, 2024, p. 44), enabling continuous collection, storage, manipulation—including through combination with other information—retrieval, analysis, and utilization, often without meaningful consent, of vast amounts of personal data at a much greater "speed, scale, and ubiquity" than ever before (Danaher et al., 2017, p. 2).

African governments have jumped at the information-gathering opportunities created by digitalization; collectively, they spend as much as USD 1 billion per year on digital surveillance (Roberts et al. 2023, p. 5). However, only a small number of scholarly works have investigated government digital surveillance on the continent (Roberts et al. 2023, p. 11). Existing contributions have emphasized the extensiveness of surveillance powers granted to government agencies (Matsiko & Kersting, 2023; Nyabola, 2018; Roberts et al., 2021) and used to build "a vast panopticon" (Nyabola, 2018, p. 71) that "replicates patterns of uneven development inherited from the colonial era" (Bernards, 2022, p. 708), when authorities also relied on population registers, some of which included fingerprint biometrics, to identify, track, and discipline Black

Africans (Breckenridge, 2014; Weitzberg, 2017). These pre-digital identity systems—such as Kenya's *kipande*, an "emblem of African subjugation" (Weitzberg, 2020, p. 26) and South Africa's Dompas, "metonymic for white supremacy" (Breckenridge, 2014, p. 139)—have been linked to exploitation of labor, reinforcement of racial hierarchies (Breckenridge, 2014; Weitzberg, 2020), ossification of ethnic identities, and intergroup conflict (Longman, 2001). They have also influenced the development of contemporary, typically biometrics-based, digital population registers—the first of them built in the 1970s and 1980s by the apartheid regime in South Africa—across the continent and elsewhere in the Global South (Breckenridge, 2014). Reliance on technology procured from foreign suppliers (Munoriyarwa & Chiumbu, 2023), which leaves Africans "effectively (dis)empowered" (Calzati, 2022, p. 270), further highlights the colonial undertones of government digital surveillance on the continent. Scholars have noted widespread collection of biometric and other sensitive personal data—their submission increasingly a condition of access to public (Iazzolino, 2021) and private services, such as banking and mobile telephony (Iwuoha & Doevenspeck, 2023)—which African governments have used to populate digital identity registers (Iwuoha & Doevenspeck, 2023; Jentzsch, 2012; Nyabola, 2018; Roberts, 2021), control migration, and monitor social media (Nyabola, 2018). The continent has also seen government installation of CCTV surveillance systems, some equipped with facial recognition technology (Dauvergne, 2022; Nyabola, 2018; Roberts et al., 2023), and interception of internet and telephony traffic (Roberts et al., 2023).

The evidentiary basis on which these findings rest is quite weak; existing work has documented a small number of instances of government digital surveillance and only in 12 African

countries.[2] Roberts et al. (2023), who have compiled the most comprehensive set of data on digital surveillance on the continent, list 70 instances, only some of them of government surveillance undertaken for political purposes, and focus on just five countries. Likewise, Feldstein and Kot's (2023) spyware dataset is important and valuable but small and necessarily far from comprehensive; it only lists 27 instances of spyware deployment in Africa. At the same time, circumstantial evidence is indicative of widespread government use of digital surveillance tools on the continent. For example, 12 of the 45 countries where the University of Toronto's Citizen Lab has detected infections with NSO Group's Pegasus spyware are in Africa (Marczak et al., 2021). The continent is also home to seven of the 25 clients of Circles, another spyware provider, identified by Citizen Lab (Marczak et al., 2017). This paucity of data precludes thorough examination of government digital surveillance in Africa, much needed especially in light of the phenomenon's far-reaching consequences identified by scholars drawing on evidence from a variety of settings.

The broader literature on government uses of digital technologies has emphasized their oppressive applications. It shows that government digital surveillance—also referred to as 'covert repression' (Earl et al., 2022), 'dataveillance' (Büchi et al., 2022), and 'fear-based censorship' (Roberts, 2018)—has led to large-scale repression (Earl et al., 2022; Gohdes, 2020, 2024), other human rights violations (CHRGJ, 2022), reduced public goods provision (Xu, 2020), and self-censorship, stifling freedom of expression, including where it is formally guaranteed (Büchi et al., 2022; Roberts et al., 2021). Digital surveillance technologies have also helped rulers to manipulate information and retain power (Gunitsky, 2015; Guriev & Treisman, 2019). Scholars have been particularly attuned to the repressive potential of state access to biometrics

[2] Egypt, Kenya, Ghana, Malawi, Morocco, Nigeria, Senegal, South Africa, Sudan, Uganda, Zambia, and Zimbabwe.

(Dauvergne, 2022) and artificial intelligence (Dauvergne, 2022; Feldstein, 2021). The danger that government digital surveillance poses to civil society "rises exponentially in states with despotic leaders, a politicised judiciary, inconsistent rule of law, weak political and privacy rights, and histories of human rights abuses" (Dauvergne, 2022, p. 2333). Such abuses of state power contrast with the improvements in government service delivery documented by the scholarship on digital population registers and other identity systems. The ease of internet-enabled collection and validation of the biometric data has facilitated registration and identification of claimants and, thereby, the provision of public goods and services (Mukhopadhyay et al., 2019; Weitzberg et al., 2021; Ziaja et al., 2024). "[I]nclusion in systems of registration and accounting" also serves as "a valued token of recognized membership" that helps to address legacies of discrimination and exclusion (Ferguson, 2015, p. 85–86).

The apparent inconsistency of these findings notwithstanding, they suggest that government use of digital technologies can increase the power of the state in relation to society, facilitate oppression, and enhance the performance of government functions. Such inferences require a solid empirical foundation and, therefore, collection—and analysis—of data more extensive than those available to date.

Data

My article provides such data and, thereby, expands the limited existing evidence of government digital surveillance in Africa. Collection of these data, in the form of thoroughgoing review of news media reporting complemented with examination of relevant non-media publications, proceeded in two phases.

In the first phase, a team of research assistants (RAs) and I conducted 7,796 English-language keyword searches in the Factiva repository of news media articles. The keywords, listed in Supplement 4 (which can be found in Supplementary Material), relate to government digital surveillance, its types and modalities, relevant technologies and tools, their purveyors in Africa, and all 54 countries on the continent. The pan-continental scope of my investigation follows the example of existing work on the subject (Roberts et al., 2021, 2023) and helps to rectify the "disjunction of North and Sub-Saharan Africa" in Africanist scholarship that belies "the long-standing connections between the peoples on both sides of and through the Sahara desert" (Bentahar, 2011, p. 1) as well as the similarities in government use of digital surveillance technologies across the continent. I catalogue the searches, which took place between October 2021 and June 2023, in Supplement 5. They yielded 1,356,589 media articles, which my RAs manually coded. The RAs assessed the presence of mentions of government digital surveillance in Africa undertaken for political purposes and recorded identification variables corresponding to components of the typology introduced in the article. To ensure inter-coder reliability and data quality, I read each included article and checked classification assignments. The RAs identified 3,736 articles that report instances of government digital surveillance, undertaken for political purposes in 1,722 cases.[3] Duplicates account for 1,397 of the 1,722 articles that satisfy the inclusion criteria. We used the content of the remaining 325 articles to collate a dataset, in Supplement 6, that reports mentions of government deployment of digital surveillance technologies for political purposes in Africa identified by the Factiva searches. I discuss the repository dataset's content in

[3] Included publications report political purposes acknowledged by government officials, imputed by observers, or inferable from the context. We excluded government digital surveillance intended to address health and other emergencies.

Supplement 1. The dataset represents the first systematic effort to catalogue media reporting on government digital surveillance in Africa. Its usefulness is nonetheless limited by the relatively small size, Factiva's unrepresentativeness—the repository mostly contains articles published by large media outlets, many of them based in the Global North—and linguistic scope.

The second phase of data collection, intended to address the gaps in the Factiva-indexed outlets' coverage, involved threefold review of additional relevant media—as well as non-media—publications not identified by the repository searches. First, in August 2023 I replicated the Factiva keyword searches on the websites of *All Africa*, a news aggregator, and *Biometric Update*, a media outlet that provides extensive coverage of the surveillance industry. Second, I set up web feeds that notified me of additional relevant articles published on both websites through January 2025. Third, I reviewed reports published by civil society and industry organizations such as Access Now, the African Digital Rights Network, Citizen Lab, the Collaboration on International ICT Policy for East and Southern Africa, the GSM Association, and Privacy International. This work yielded another 264 non-duplicate publications (135, 93, and 36, respectively, per each of the three categories identified above) that satisfy the inclusion criteria, increasing the sample of included sources, listed in Supplement 8, to 589. Figure 1 shows the sources' publication dates.

Included sources report 372 distinct instances of digital surveillance undertaken for political purposes by the governments of 49 African countries. A separate dataset, manually coded following the process outlined above and presented in Supplement 7, lists all these instances and identifies, where known, the countries (and their key characteristics), subnational locations, and United Nations regions where reported government digital surveillance has taken place, its types

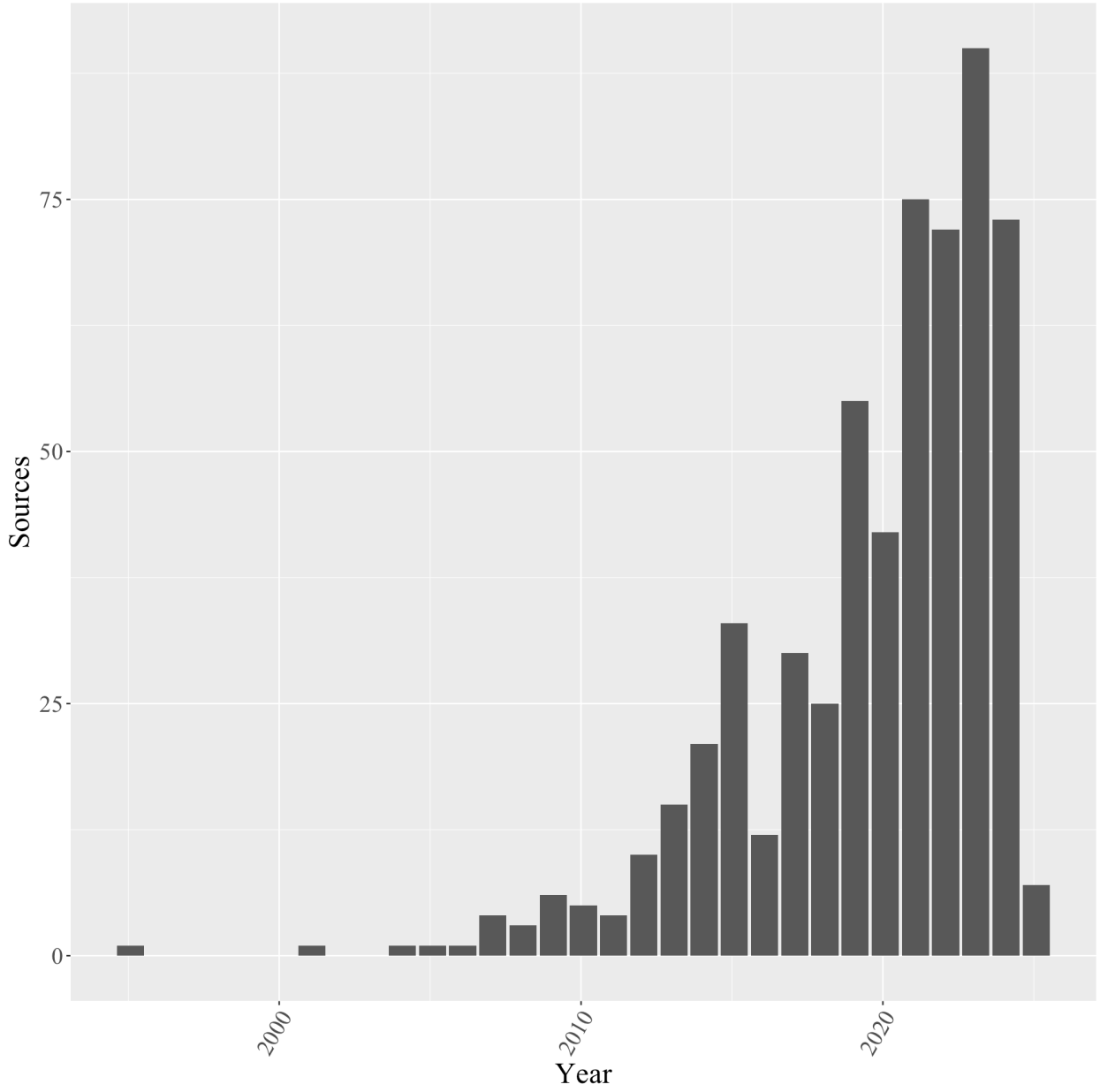
and modalities, tools used and their developers, responsible government agencies, status and start and end dates of implementation, purposes of surveillance stated by government officials and/or imputed by—also listed—other actors, and the types and numbers of surveillance targets in addition to information about data sources. I used variation across these variables and the content of included sources to distinguish specific instances. Each instance has a unique variable combination except for two digital identity registers in Madagascar and another two in South Africa; sources identify differences between these four instances that establish their distinctiveness. I summarize the content of the instances dataset in the article and describe it in detail in supplements 2 and 3. Supplement 9 contains the R script used to generate figures and obtain descriptive statistics.

Figure 1

Source publication dates

Data Quality

Media reporting is a valuable, but imperfect, source of data on government digital surveillance.



Government reluctance to disclose details of surveillance operations limits the availability of data on the use of digital technologies for this purpose. Journalistic tenacity helps to overcome this constraint. Thanks to their contacts in state agencies and other organizations, expertise in accessing government records, on-the-ground presence during many investigations, and incentives they face to doggedly pursue newsworthy stories, investigative reporters in particular are

well positioned to uncover digital surveillance activities that authorities seek to conceal from the public. Governments also share some information about instances of surveillance they wish to publicize with journalists, who often follow up on such leads. Crucially, media reporting has broad coverage: a variety of outlets report on, and oftentimes from, all African countries. Especially complemented, and triangulated, with non-media publications, media reporting enables collation of extensive, detailed, and otherwise unavailable—if necessarily incomplete—data about government digital surveillance on the continent.

At the same time, reliance on media reporting presents the risk of both selection and description bias (Earl et al., 2004, p. 67). The linguistic scope of the data collection process I followed has almost certainly resulted in overrepresentation of instances occurring in countries prioritized by English-language media due to size, prominence, or availability of informants conversant in English as well as of English-language government documents.[4] Journalistic focus on countries with fewer restrictions on reporting might similarly produce such selection bias.[5] Information about instances that governments openly disclose or even promote, including because implementation requires public participation—as is the case with digital population and SIM card registers—is also likely to be more readily available to journalists, contributing to potential overrepresentation.[6] Among instances that governments seek to conceal from the public journalists may prioritize reporting on those considered newsworthy, notably spyware infection of prominent targets' electronic devices, over more mundane surveillance, such as the use of data

---

[4] The large number of instances in countries such as Egypt and Nigeria and in countries where English is an official language, discussed below, indicates that this concern is warranted.

[5] However, collected data are not indicative of such a relationship.

[6] Indeed, such registers make up much of the sample.

routinely collected by and obtained from financial institutions or telephony operators.[7] Comparison with other sources and, in particular, with non-media data—"the current state of the art" in media research (Dietrich & Eck, 2020, p. 5)—helps to address, but does not eliminate, potential selection bias. The risk of description bias is likely smaller; factual statements made by journalists such as those used to collate the supplementary datasets tend to be accurate (Earl et al., 2004, p. 72), especially in the wake of improved access to digital communication tools (Croicu & Kreutz, 2017, p. 27). Nevertheless, many claims made in included sources cannot be verified; qualifiers such as "allegedly" or "according to media reports"—omitted for brevity—are implied throughout.

Some information about instances is also missing from included sources. Each instance is linked to a country and a region. Of the typology categories I discuss in the article, implementation status is not available in 17 instances, the start date of implementation—235 instances, target type—63 instances, stated purpose—200 instances, imputed purpose—238 instances, disapprover type—241 instances, surveillance type—12 instances, and surveillance modality—19 instances. The names of the developers of surveillance tools obtained by African governments, the locations of these businesses' headquarters, and specific surveillance tools are not available in 196, 197, and 297 instances, respectively. Included sources also do not report the end date of implementation in 345 instances, while the number of targets is not specified in 337 instances (including sources that identify entire populations as targets but do not contain specific target numbers); given the number of missing values, I do not address these two categories in the article. In

[7] The small number of instances of mass-to-targeted surveillance could be the result of such uneven media interest.

addition, four instances (in Angola, Gabon, Morocco, and Rwanda, discussed in Supplement 3) might be duplicates.

While the data collected for the article provide the most complete record of government digital surveillance in Africa to date, in light of the aforementioned limitations they cannot be presumed to account for all of its instances. Accordingly, my discussion of these data relates the characteristics of the sample of instances reported in included sources, rather than of the universe of all such instances.

A Typology of Government Digital Surveillance

Contemporary governments have access to a profusion of digital surveillance technologies that they can procure from a wide range of suppliers and deploy in multiple ways, to numerous ends, and against a variety of targets. The typology (Table 1) I introduce in the article helps to make sense of the variegated landscape of government digital surveillance in Africa.

Governments—and different *state agencies*—have deployed digital surveillance technologies in multiple countries and geographic *regions*. Instances of government digital surveillance also vary by the *date* as well as *status of implementation*—some deployments have been completed, while others are in progress or planned for the future—and specific technological solutions used in surveillance operations, the suppliers of these tools, and the jurisdictions where they operate; for example, the NSO Group, which develops the Pegasus spyware, is based in Israel.

Table 1

Typology of government digital surveillance

Region
Country
Responsible government agency
Implementation status
Implementation start date
Implementation end date
Target type
Number of targets
Stated purpose
Imputed purpose
Disapprover type
Surveillance type
Surveillance modality
Technology provider
Technology provider country
Tool

Government digital surveillance can *target* entire populations or specific individuals or segments of society: civil society activists and groups; journalists; political opponents; government employees; ethnic, sexual, or other minorities; migrants; or populations of delimited geographic areas, such as specific cities. Authorities monitor such targets for a variety of purposes, which include provision of protection—in the form of crime prevention and prosecution, counterterrorism operations, national defense, and other security improvements—better public service delivery; development of the quality and effectiveness of the administrative apparatuses of the state; enhancement of voting processes as well as prevention of electoral fraud; control over populations and specific groups, such as migrants and members of sexual and other minorities; restriction of civil rights; suppression of civil society activity, media reporting, and political opposition; and extension of the power of the state in general and of particular governments cur-

rently in power. Official acknowledgement of some of such objectives of government digital surveillance is rare; accordingly, I distinguish *stated purposes*—articulated by government officials—from those *imputed* by *observers* such as civil society activists and groups, journalists, and political opponents, whom the typology also identifies.

Depending on the objectives of government digital surveillance, it takes three primary forms, to which I refer as *types*: mass, mass-to-targeted, and targeted. Governments routinely deploy digital surveillance technologies to continuously, passively collect troves of data on people's lives,[8] without much active involvement of state officials. Such mass (Gohdes, 2024) surveillance (also referred to as passive surveillance; Feldstein, 2021) increases governments' knowledge about populations at relatively low—or, where data can be obtained from private businesses, no—cost. At times, governments use mass surveillance data to target specific individuals or groups. For this reason, I distinguish mass and mass-to-targeted types of government digital surveillance. Both types are distinct from targeted surveillance (Feldstein, 2021; Gohdes 2024),[9] which requires the deployment of specialized tools capable of obtaining otherwise unavailable data to surveil particular targets.

To monitor society and its individual members, the state deploys a variety of technologies. I distinguish 24 such *modalities* of government digital surveillance. Biometric digital population registers, "the *bête noire* of scholarly and popular fears of the overweening surveillance state" (Breckenridge, 2014, p. 16), have attracted particular attention. Governments also com-

---

[8] The comprehensiveness of these data may account for the rare instances of surveillance retrenchment. Notably, governments dismantled the Covid-19 contact tracing systems once the pandemic's emergency phase ended. However, existing surveillance apparatuses already provide detailed location and social network data, which pandemic-era systems duplicated.

[9] I adopt the distinction between mass and targeted surveillance from existing scholarship. Other components of the typology are novel.

monly introduce other mandatory digital identification systems, which connect legal identities derived from enrollment in population registers to different aspects of targets' lives, including internet and telephony network usage, monitored through the registration of electronic devices such as mobile phones in device management systems or of the users of Subscriber Identity Module (SIM) cards. Compulsory identity verification enables the deployment of several other surveillance modalities. It links individuals to data collected by governments, which install deep packet inspection (DPI) equipment—used to inspect, store, and filter internet traffic—and other internet surveillance tools as well as automated license plate readers and similar vehicle location tracking systems, and by private companies: mobile telephony operators routinely record device location data from Base Transceiver Stations (BTS) as well as Short Messaging System (SMS) message content and both phone call and SMS message metadata, internet service providers filter and monitor internet traffic, digital platforms have access to user data stored on their servers, and financial institutions retain financial transaction data. Photograph biometrics typically stored in digital identity registers also help authorities to identify people recorded by CCTV surveillance cameras, either manually or with the assistance of facial recognition software, which is increasingly integrated into CCTV systems, especially in the so-called 'safe' or 'smart' cities, "extraordinary apparatuses of surveillance" designed to track residents' activities at all times (Galič, 2022, p. 206). Such mass—and, in specific instances, mass-to-targeted—surveillance "is mundane. Quotidian. Banal" (Brayne, 2022, p. 372). The modalities of targeted surveillance at government disposal are, in contrast, anything but. Remote infection of electronic devices with dedicated spyware not only enables extraction of their contents but also surveillance of targets' activities, including their physical movements and communications, from anywhere in the world.

Where government operatives have physical access to devices, they can also either compel owners to unlock them or use forensics extraction tools to the same end. The interception of phone calls—that is, wiretapping—involves the use of similar dedicated tools. International mobile subscriber identity (IMSI) catchers, sometimes referred to as Stingrays (a genericized trademark), which imitate carrier BTS to intercept mobile phone traffic and location data, and aerial drones can be used to either passively monitor large populations or target specific individuals or groups. Digital surveillance requires the use of technological *tools*, such as Stingrays or biometric data capture kits, which governments procure from a variety of *providers* based in different *countries*.

These categories describe digital surveillance technologies at the disposal of African governments. In the remainder of the article, I turn my attention to actual deployments of these technologies reported in the included sources.

Geographic Distribution, Implementation, Targets, and Purposes of Government Digital Surveillance in Africa

Analysis of the instances dataset is indicative of considerable variation in the geographic distribution of government digital surveillance in Africa, the identity of its targets, the purpose of its deployment, and the implementation status of individual instances. This multiplicity of the forms of government digital surveillance illuminates the range of objectives it helps to realize.

While reported throughout Africa, government digital surveillance is geographically concentrated. Eastern Africa (as defined by the United Nations geoscheme) accounts for a plurality of reported instances of such surveillance (37.1%). Western (28.5%), Northern (16.7%), South-

ern (11.6%), and Middle Africa (6.2%) follow (Figure 2). Except for Central Africa,[10] these proportions approximate regional shares of the continent's countries and population. Despite the appearance of cross-regional balance, just 11 governments are responsible for the majority of instances. Reports of government digital surveillance in Nigeria are particularly numerous. The dataset reports 44 distinct instances in the country, 11.8% of the continental total. The other 10 large deployers of digital surveillance technologies are the governments of Egypt (17 instances, or 4.6%), Ethiopia (12, 3.2%), Ghana (12, 3.2%), Kenya (22, 5.9%), Morocco (18, 4.8%), South Africa (19, 5.1%), Tunisia (12, 3.2%), Uganda (16, 4.3%), Zambia (12, 3.2%), and Zimbabwe (18, 4.8%). In contrast, Mali only accounts for one reported instance. Instances number two in Eritrea, Guinea-Bissau, Mauritania, and Sierra Leone and three in Eswatini, the Gambia, Liberia, Namibia, and Somalia (Figures 3 and 4). The geographic distribution of instances suggests that some African governments have pursued the opportunities offered by government digital surveillance technologies more actively than others. Explanation of such variation is outside the scope of the article, but I briefly discuss some key country characteristics for illustrative purposes. Reported instances are plentiful across regime types (identified by the Polity 5 regime score; Marshall, 2020), but concentrations among authoritarian-leaning anocracies, notably Egypt and Morocco (score of -4 each), and democracies such as Ghana, Malawi, Mauritius, and South Africa (scores from 6 to 10) are intriguing (Figure 5). Deployment of digital surveillance technologies does not require a high level of economic development (proxied by gross domestic product per capita; World Bank Group, n.d.-a), underscoring their accessibility to African governments (Figure 6). The relationship between population size and the number of reported in-

[10] The region's share of instances may be low due to resource constraints faced by most Central African governments or the paucity of English-language media reporting.

stances is positive but weak (Figure 7; World Bank, n.d.-b). Most instances have been reported in countries where English is an official language (Figure 8). Reported instances are slightly less numerous on average in countries with higher media freedom scores (assigned by Reporters Without Borders, 2024; Figure 9).

Figure 2

Regions

Figure 3

Countries

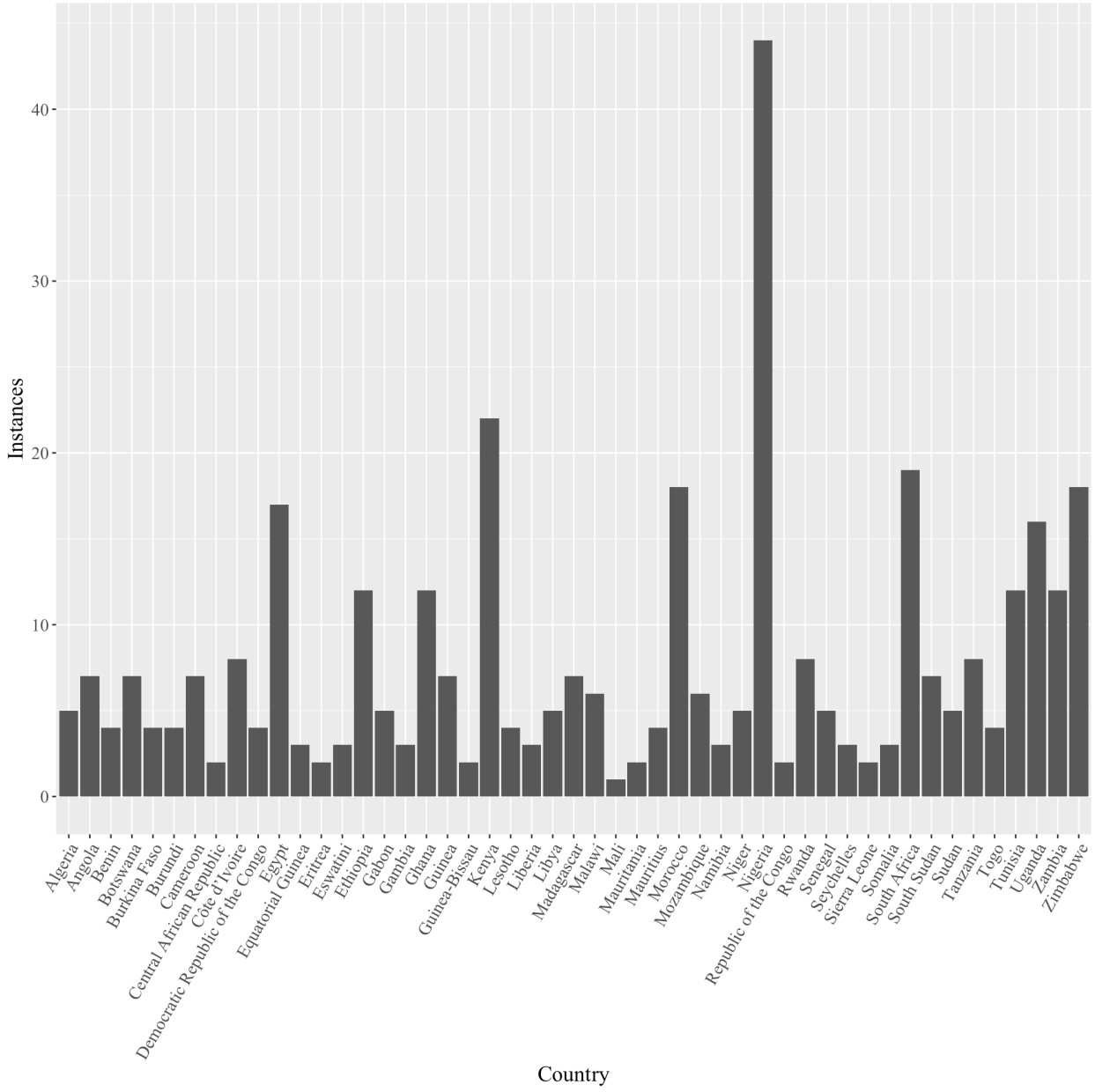


Figure 4

Countries: map

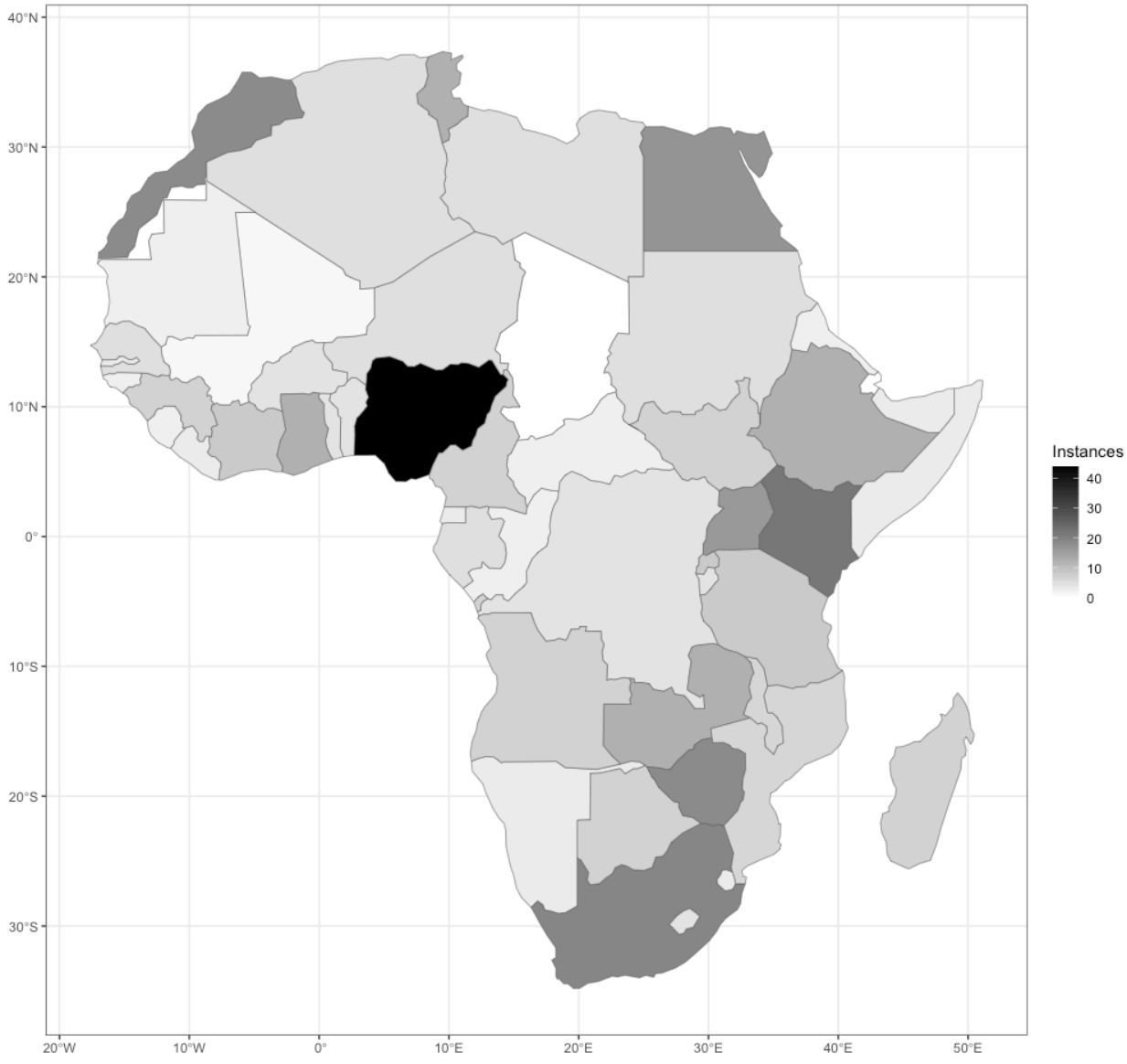


Figure 5

Countries: regime type

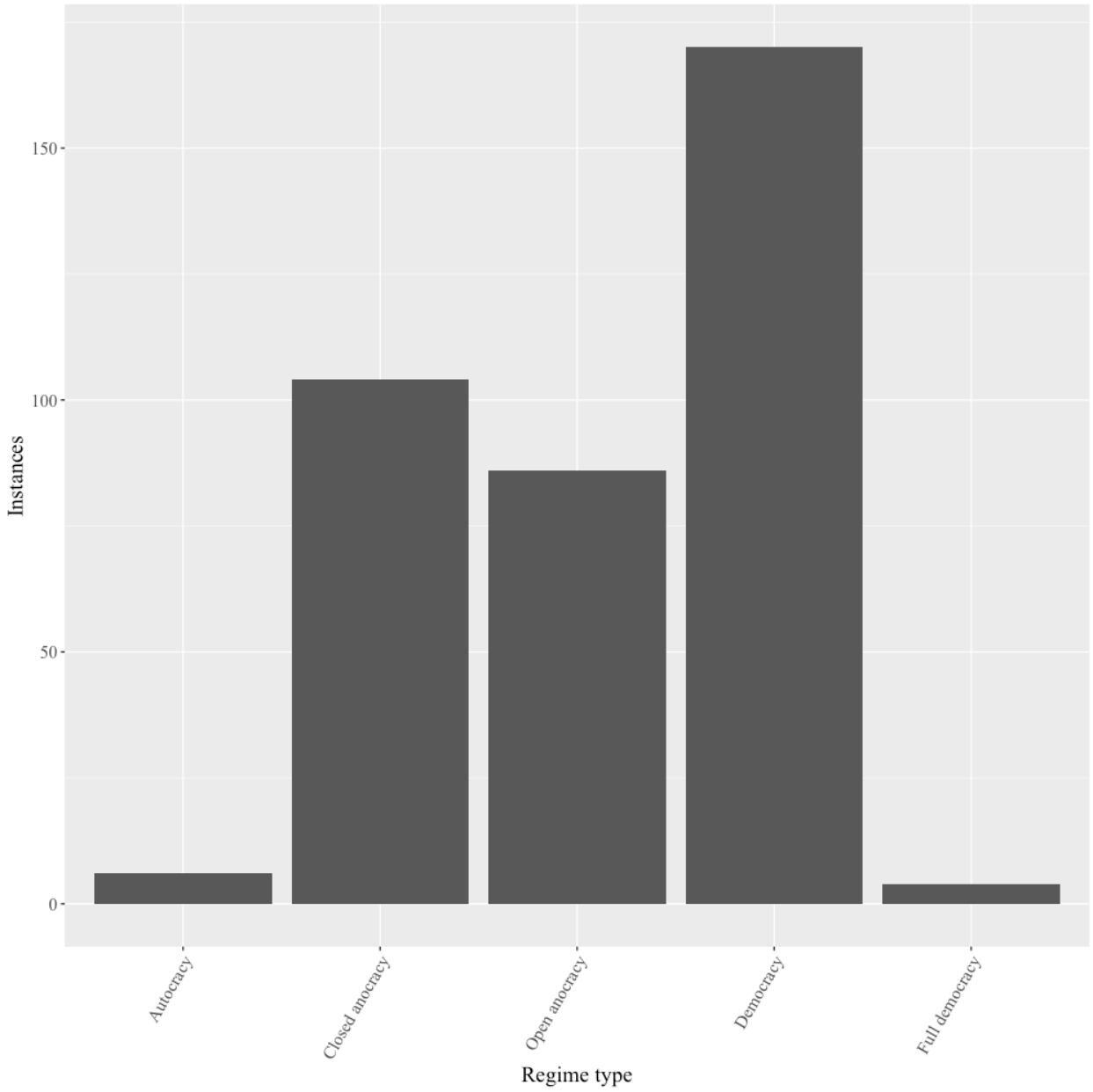


Figure 6

Countries: GDP per capita

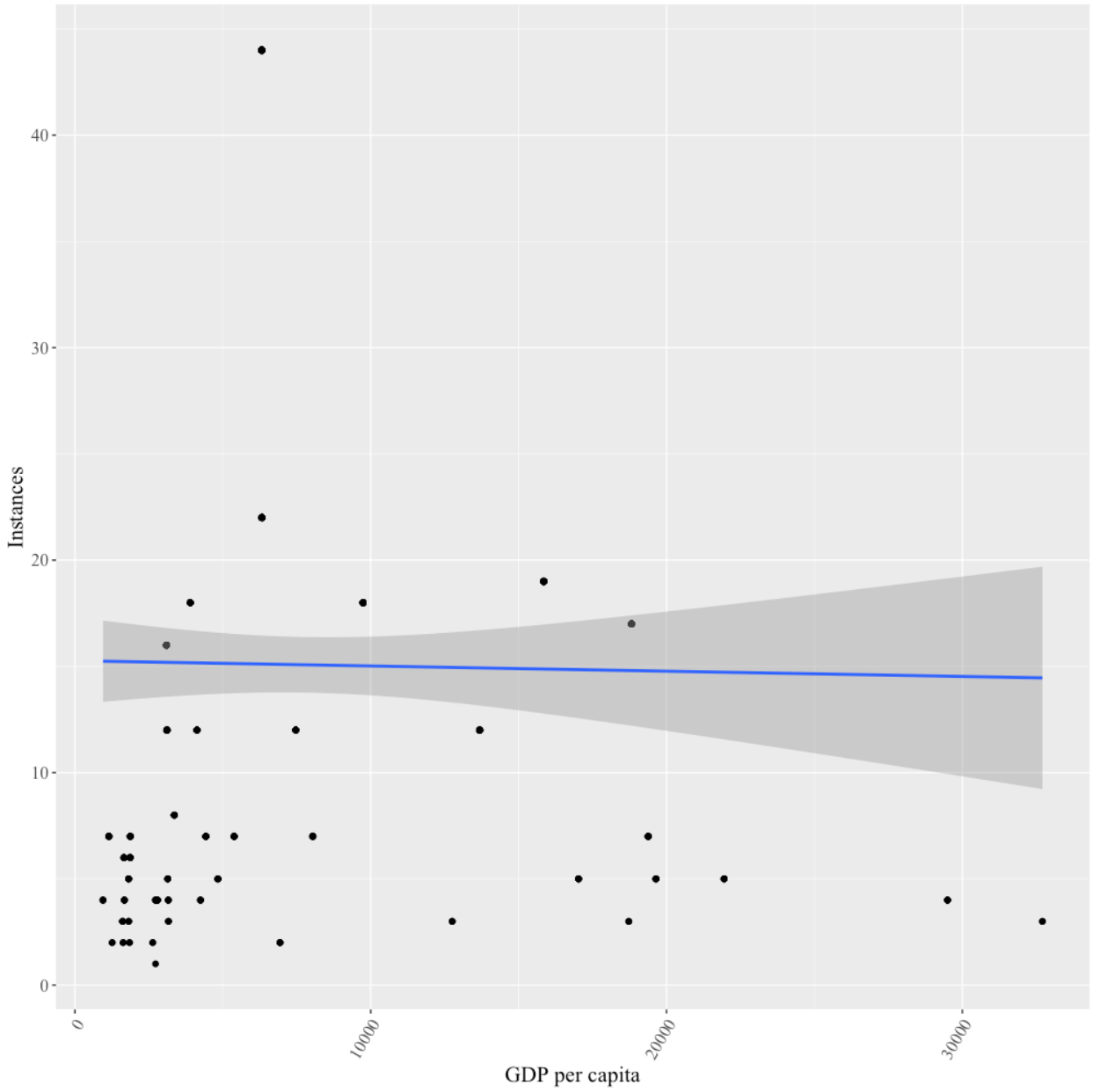


Figure 7

Countries: population

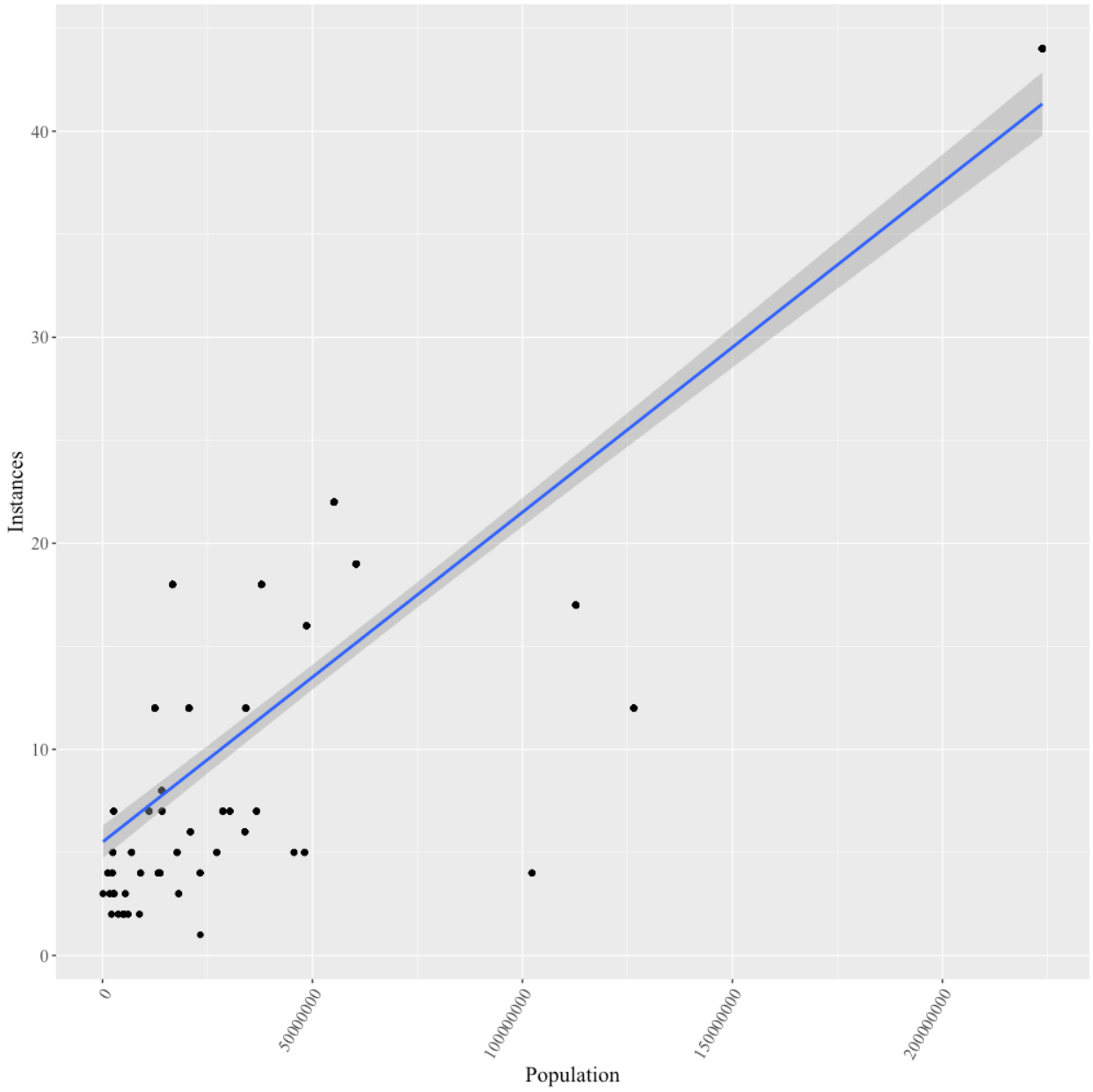


Figure 8

Countries: official languages

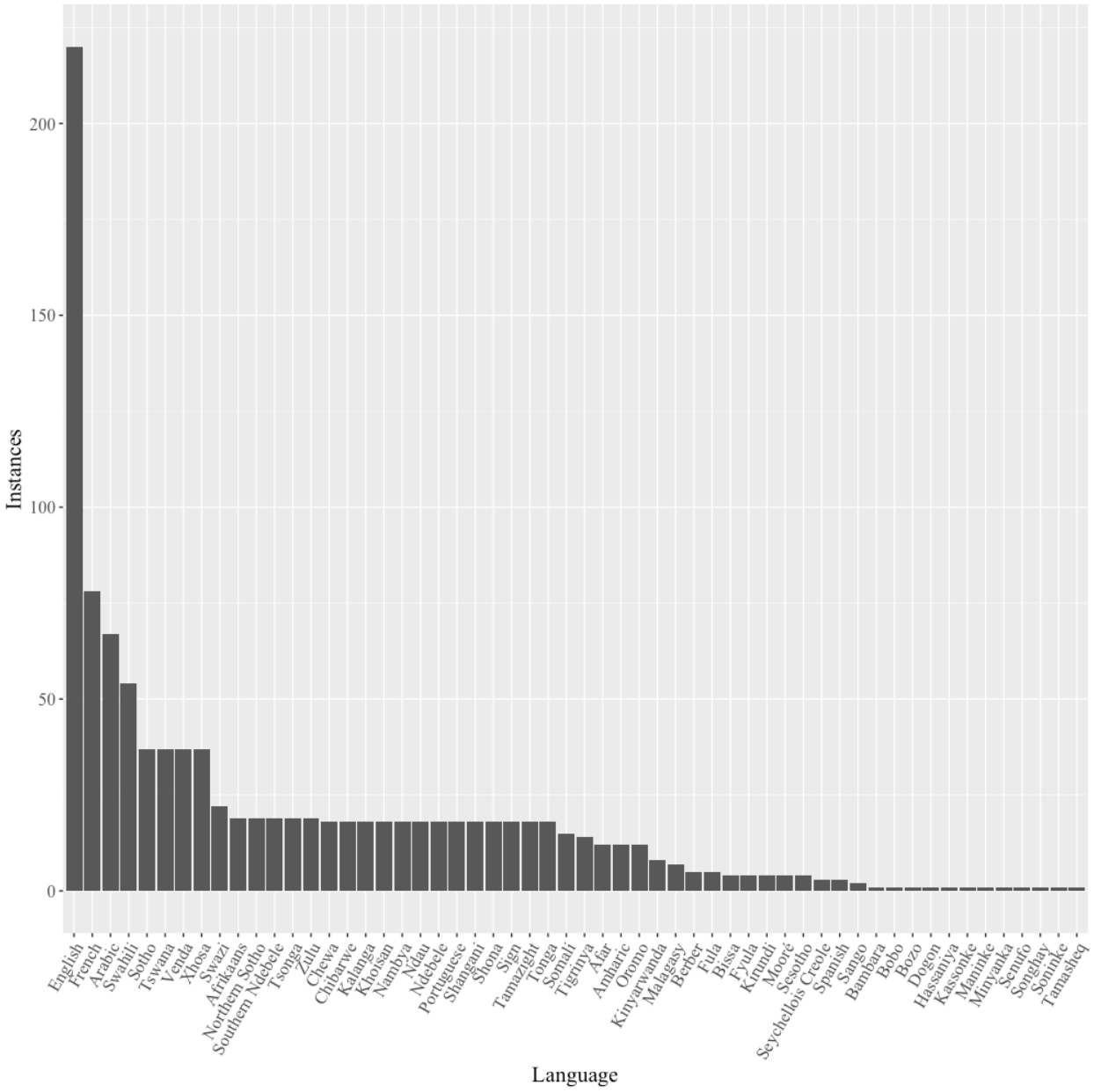
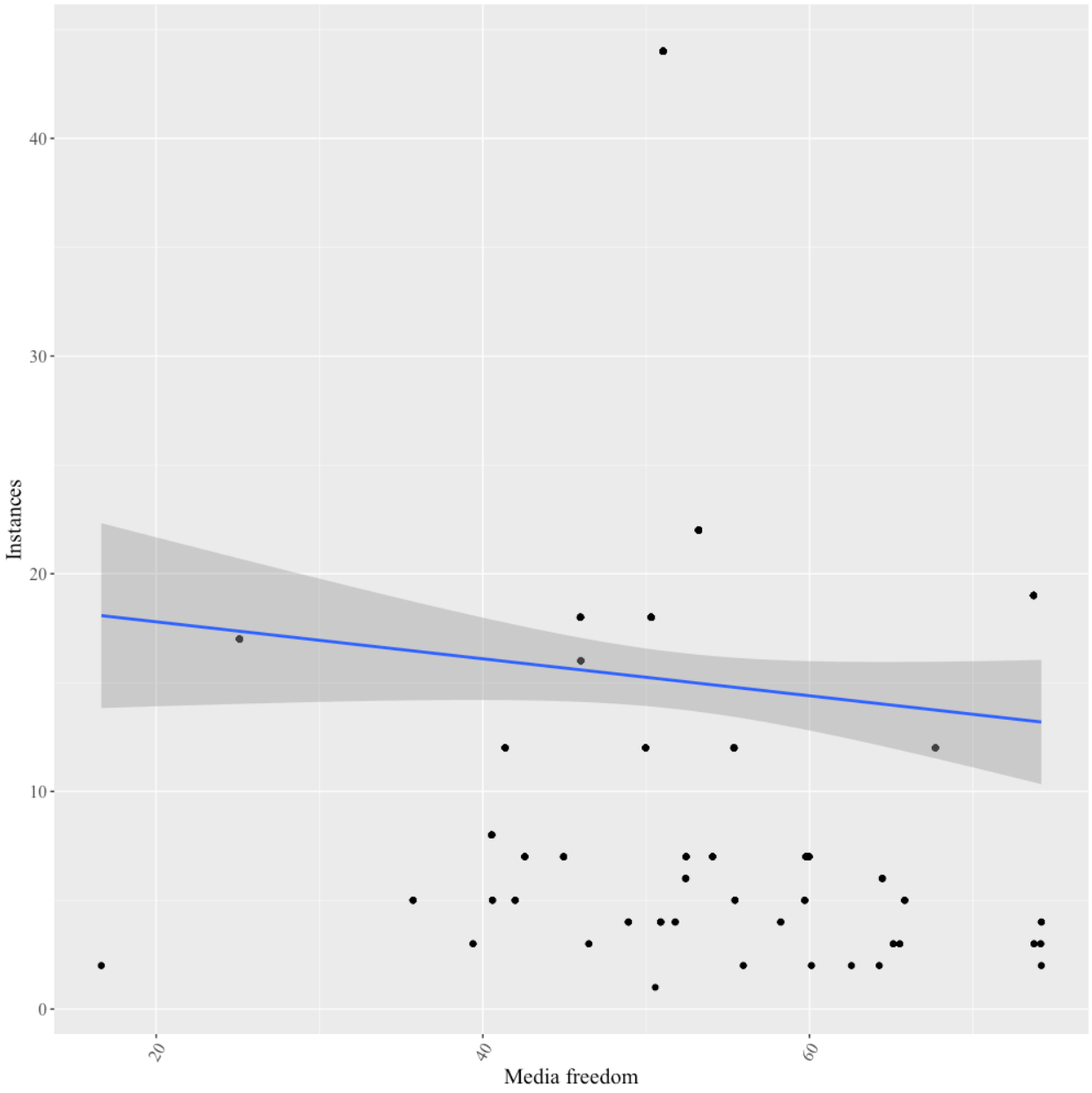

Instances
200
150
100
50
0
English
French
Arabic
Swahili
Sotho
Tswana
Venda
Xhosa
Swazi
Afrikaans
Northern Sotho
Southern Ndebele
Tsonga
Zulu
Chewa
Chibarwe
Kalanga
Khoisan
Namibya
Ndau
Ndebele
Portuguese
Shangani
Shona
Sign
Tamazight
Tonga
Somali
Tigrinya
Afar
Amharic
Oromo
Kinyarwanda
Malagasy
Berber
Fula
Bissa
Fyula
Kirundi
Mooré
Sesotho
Seychellois Creole
Spanish
Sango
Bambara
Bobo
Bozo
Dogon
Hassaniya
Kassonke
Maninke
Minyanka
Senufo
Songhay
Soninke
Tamasheq
Language

Figure 9

Countries: media freedom



The first African government to take advantage of the surveillance opportunities offered by digitalization was South Africa's apartheid regime, which implemented its pioneering biometric digital population register in 1981. Implementation of few instances of government digital surveillance identified in the included sources began, however, before 2011. The number of reported instances introduced each year increases in subsequent years, reaching 14 in 2023 (Figure 10). In over two-thirds of instances (258, 69.4%) the primary objectives of government digital surveillance—such as SIM card registration or spyware device infection—have been fully accomplished (even if some activities, such as enrollment of new mobile phones, continues). Implementation was in progress or planned at the time of reporting in 39 (10.5%) and 58 (15.6%) instances, respectively (Figure 11).

Figure 10

Implementation start date

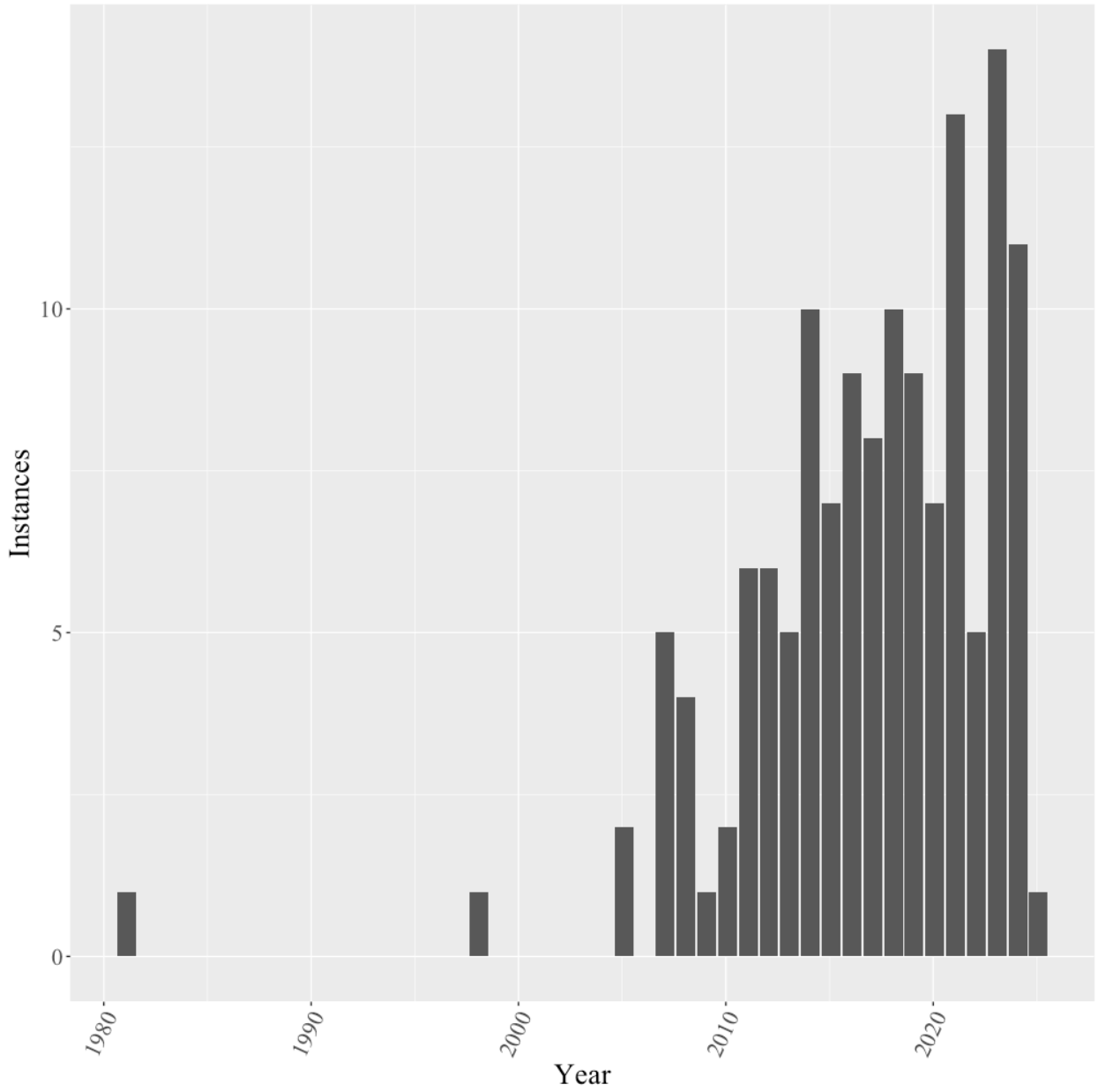
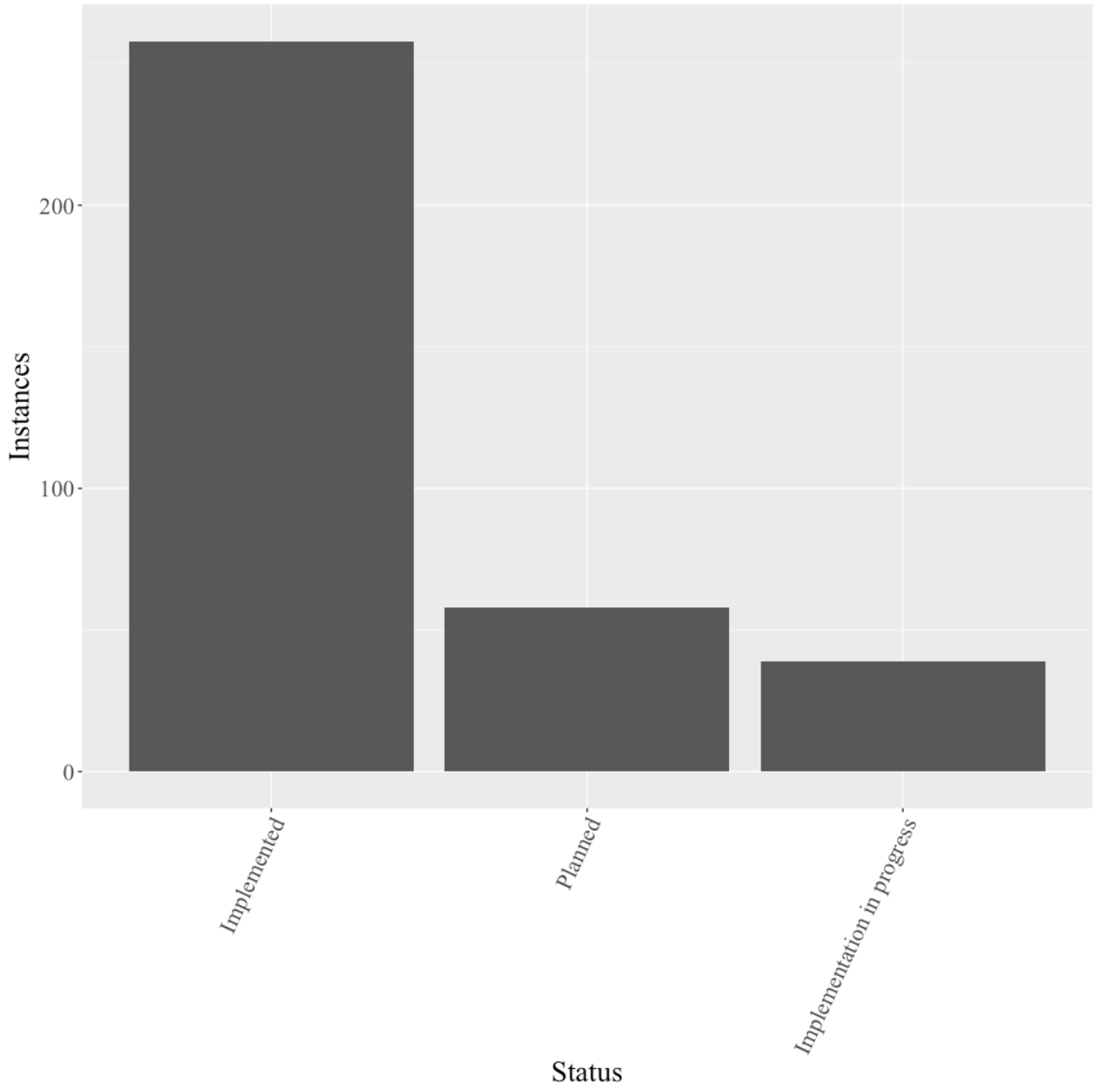


Figure 11

Implementation status



Included sources indicate that African governments tend to deploy digital surveillance technologies at scale. Half (194, 50.3%) of all reported instances involve the surveillance of entire populations, most commonly in the form of mandatory registration of people and their electronic devices. Another 21 instances (5.4%) affect populations of delimited geographic areas, usually specific cities that see installation of CCTV cameras or 'safe' and 'smart' city surveillance systems. Ethnic, sexual, or other minorities are the targets of government digital surveillance in 17 reported instances (4.4%). For example, the Tanzanian government has monitored social media to "hunt down and round up" LGBTQ+ people (Charity, 2018), also targeted with spyware in Uganda.[11] Included sources document 13 instances (3.4%) of migrant surveillance. Ghanaian, Nigerian, and Ugandan authorities have deployed fingerprint and facial recognition technology at airports, while the Tunisian government has 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, 2019a).

Governments have also on occasion subjected their own employees—required to enroll in public service registers or monitored with facial recognition-equipped CCTV cameras—to surveillance (eight instances, or 2.1%). Surveillance of real or perceived political adversaries appears to be, however, more common. Political opponents are the targets in 40 instances of reported government digital surveillance (10.4%). In Zimbabwe, the Robert Mugabe regime deployed

[11] Except for direct quotations, I identify the sources of data about individual instances in supplements 2, 3, and 7.

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). President Mugabe said at the time:

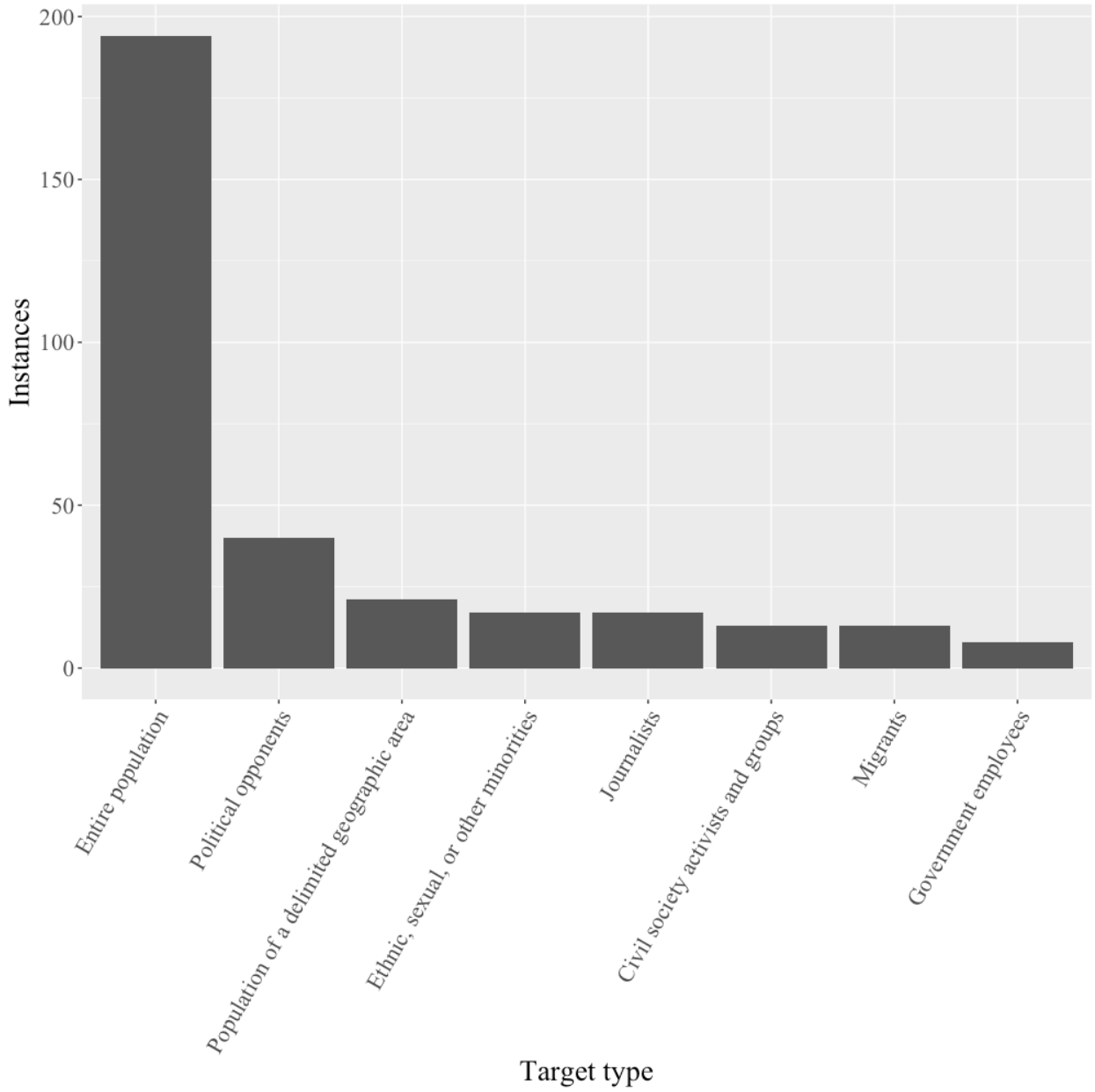
> This is a great step in the democratic process of Zimbabwe. All my enemies will be liquidated. I am just waiting for police to pick up [the opposition leader] Morgan Tsvangirai and look him up on the app. Then they can shoot him. That will be a great day for Zimbabwe indeed. (*PressWire*, 2016)

The Emerson Mnangagwa government has continued the use of spyware to target its opponents. In particular, its operatives have reportedly installed a GPS tracker in the parliamentary vehicle of Tsvangirai's co-partisan 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 claimed (Ndlela, 2020b). Ugandan security forces have infected the devices used by the opposition politicians Robert Kyagulanyi, or Bobi Wine, and Norbert Mao. The former has linked his subjection to government digital surveillance to the physical abuse he suffered at the hands of regime operatives: "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). In Nigeria, the future president Muhammadu Buhari was surveilled as a candidate for office. Ethiopian authorities have monitored online behavior of members of the opposition movement Ginbot 7. Another 17 instances involve surveillance of journalists (4.4%). The Ethiopian and Moroccan governments have installed Hacking Team spyware on the devices of journalists working for the (United States-based) Ethiopian Satellite Television and the citizen media project Mamfakinch, respectively. Ugandan journalists Raymond

Mujuni and Canary Mugume have had their devices infected with NSO Group's Pegasus. In Zambia, "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). Included sources describe government digital surveillance targeted at civil society activists and groups in 13 reported instances (3.4%; Figure 12). Togolese authorities have deployed Pegasus against a Catholic bishop, a priest, and other members of civil society as well as opposition politicians, while their Zimbabwean counterparts have 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 Mugabe regime; a cabinet minister subsequently warned opponents that the government could "visit your bedrooms and expose what you will be doing" (Ndlela, 2020a).

Figure 12

Target type



Similarly, a Nigerien minister has admitted that intelligence services had placed opposition politicians under surveillance: “Are you afraid of being tapped? You have been and still are” (CIPESA, 2022, p. 46). Such public acknowledgement of the use of digital surveillance technologies to surveil political adversaries is rare. Suppression of political opposition is the stated purpose of government digital surveillance in four reported instances (1%). Governments have also openly used digital surveillance technologies to identify and monitor members of sexual and other minorities and to restrict civil rights in in two instances (0.5%) each. More commonly, however, official justifications of government deployment of digital surveillance technologies centre on criminality and security threats, even where it affects entire populations. Crime prevention and prosecution, cited in 51 reported instances (13.2%), is the most common purpose identified by government officials. Counterterrorism operations, national security, and unspecified security improvements are the stated purposes cited in 11 (2.8%), 21 (5.4%), and 14 (3.6%) instances, respectively. Governments have also attributed their use of digital surveillance technologies to efforts to improve administrative quality (15 instances, or 3.9%) and service provision (35 instances, or 9%) and to enhance voting processes (16 instances, or 3.8%). Included sources report migration control as the stated purpose in 16 instances (4.1%; Figure 13).

In contrast, observers impute government digital surveillance to efforts to suppress political opposition (62 instances, 14.7%), media reporting (27, 6.4%), or civil society activity (23,

5%); to restrict civil rights (37, or 8.8%); to expand state control over population (27, 6.4%); or to extend the power of either the state (two, 0.5%) or the sitting government (five, 1.2%; Figure 14). Civil society activists and groups have identified such purpose in 48 instances (12.7%), journalists—in 85 instances (22.4%), and political opponents—in four instances (1.1%; Figure 15). In Nigeria, "[d]igital 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 [Independent National Electoral Commission] could potentially be used by the state for surveillance or other unorthodox purposes" (Macdonald, 2023a). Dorothy Mukasa of the Ugandan nongovernmental organization Unwanted Witness, herself a subject of targeted government digital surveillance, has described mandatory installation of location trackers in all motor vehicles in the country as "an expansion of the state's plan of surveilling on everybody" (*Reuters*, 2021). "Ugandans should be worried about this, this is a mechanism to control their lives," the opposition politician Patrick Oboi Amuriat has added (*Reuters*, 2021). Analogously, a journalist has highlighted the measures the Madagascan government has taken "to monitor and control its civil servants and citizens" (Hersey, 2020).

Figure 13

Stated purpose

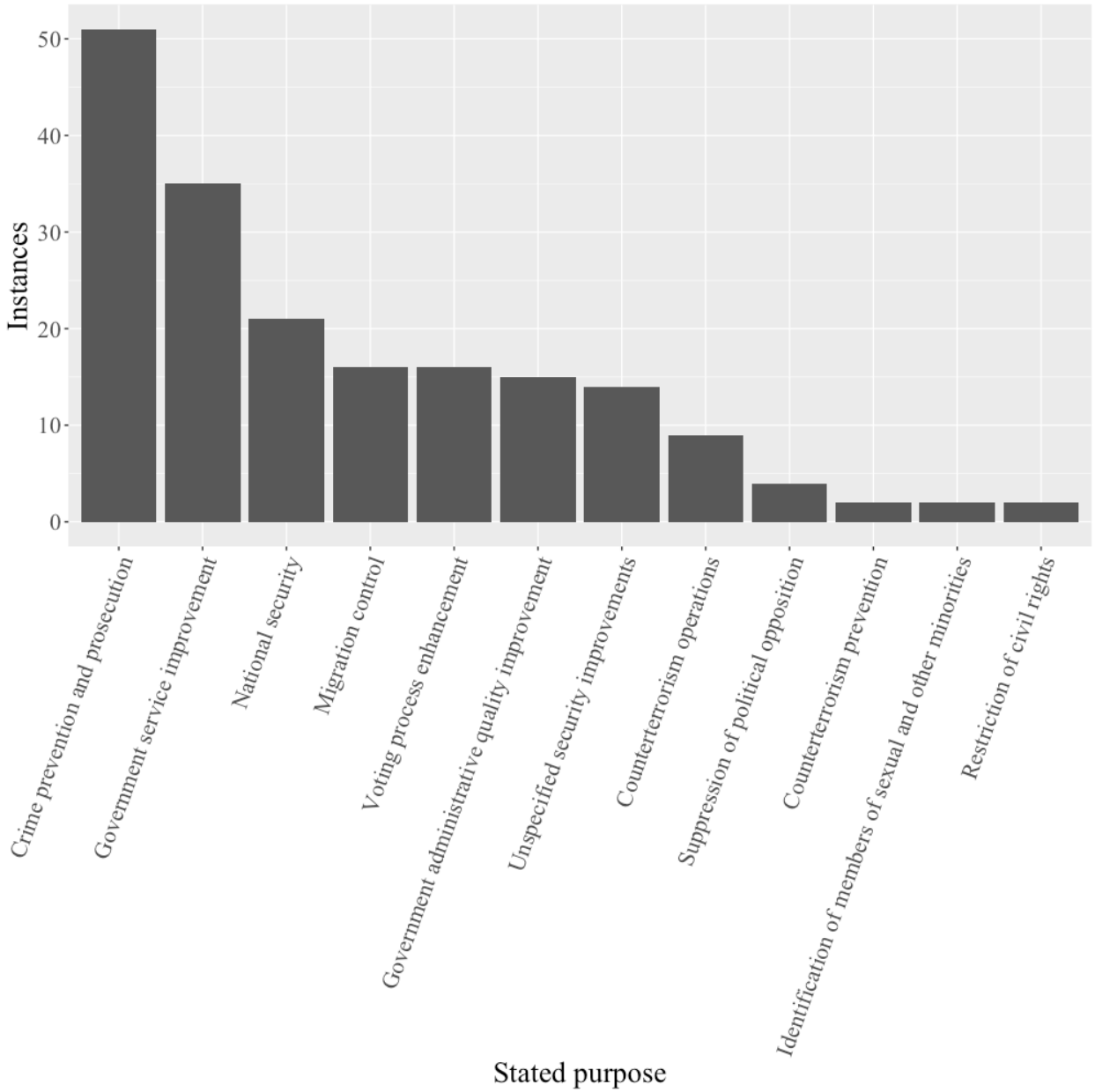


Figure 14

Imputed purpose

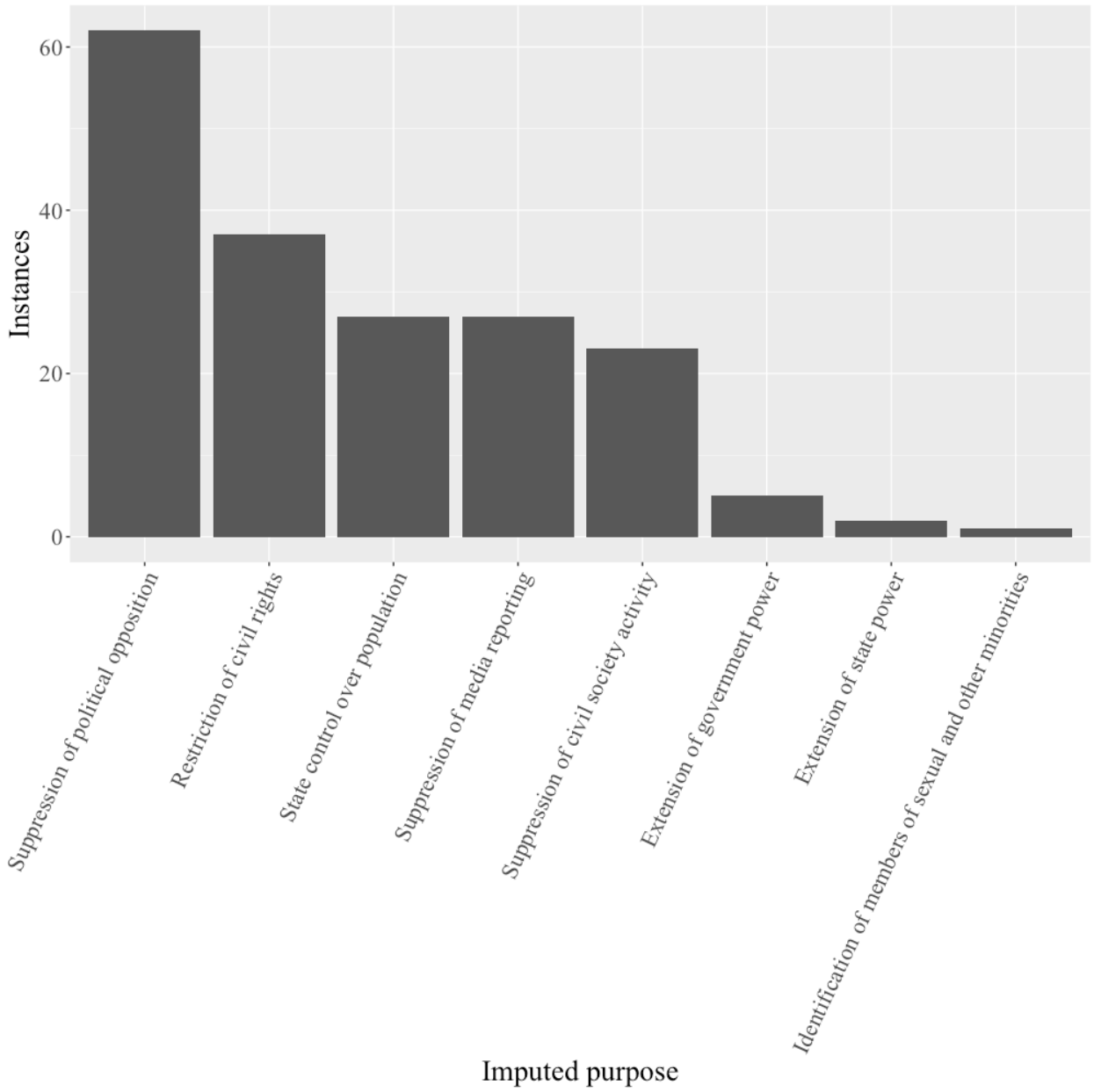
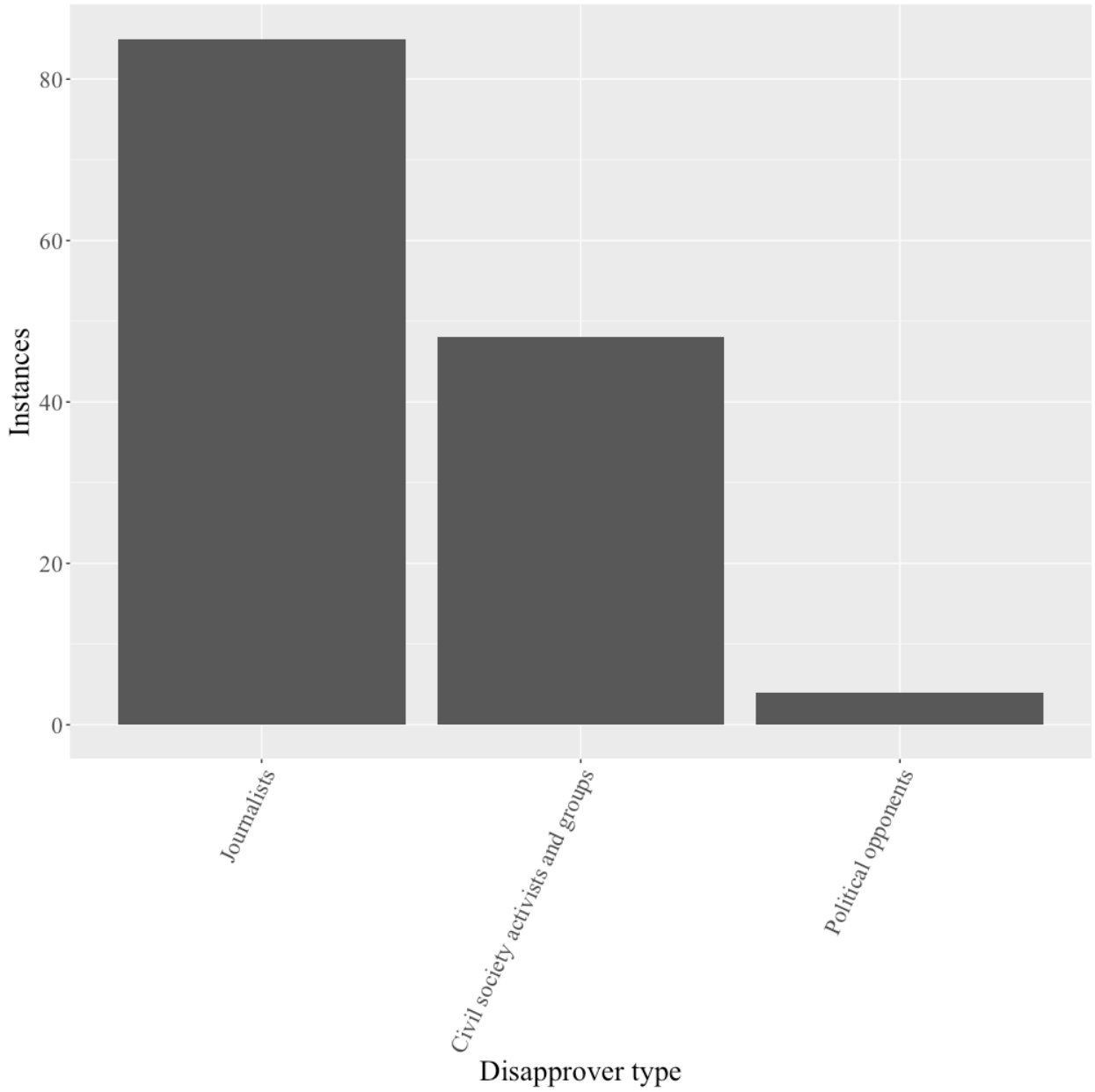


Figure 15

Disapprover type



Types and Modalities of Government Digital Surveillance in Africa

Digital surveillance technologies enable governments to monitor entire populations and specific targets alike, but their deployment at scale is particularly momentous. Targeted surveillance requires that government operatives actively infect the devices of or otherwise track particular individuals or groups; remotely installable spyware facilitates such targets' surveillance but does not dramatically limit the involvement of intelligence personnel. In contrast, mass surveillance generates swathes of data that can be readily retrieved, analyzed, and used—including to target specific individuals and groups—without expending limited resources.

Accordingly, mass surveillance predominates in the instances dataset. It accounts for over two thirds of reported instances (253, 68.3%). A quarter of instances (87, 23.4%) involve targeted surveillance. Mass-to-targeted surveillance accounts for the remainder of instances (19, 5.1%; Figure 16). In subsequent paragraphs, I detail the modalities through which governments effect digital surveillance of all three types (Figure 17).

Mandatory digital identity registers make up over a third of all reported instances. I categorize such registers as mandatory when enrollment is either required by law or necessary to access private and/or public services, obtain social benefits, and/or actualize civil rights. I distinguish between mandatory SIM card registration, which is especially widespread, and mandatory digital identity registers created for other purposes.

Of the 120 mandatory digital identity registers reported in the included sources (29.9%), 108 (26.9% of the total) include biometric data. Registration for most systems requires provision of fingerprints and face photographs. Some are, however, more intrusive. Legislation that authorized Kenya's Huduma Namba digital population register specified inclusion of "fingerprints, hand and earlobe geometry, retina and iris scans, and voice samples" (Mayhew, 2019), while the Ugandan government has made plans to collect DNA biometrics for Ndaga Muntu, an equivalent system.

Figure 16

Surveillance type

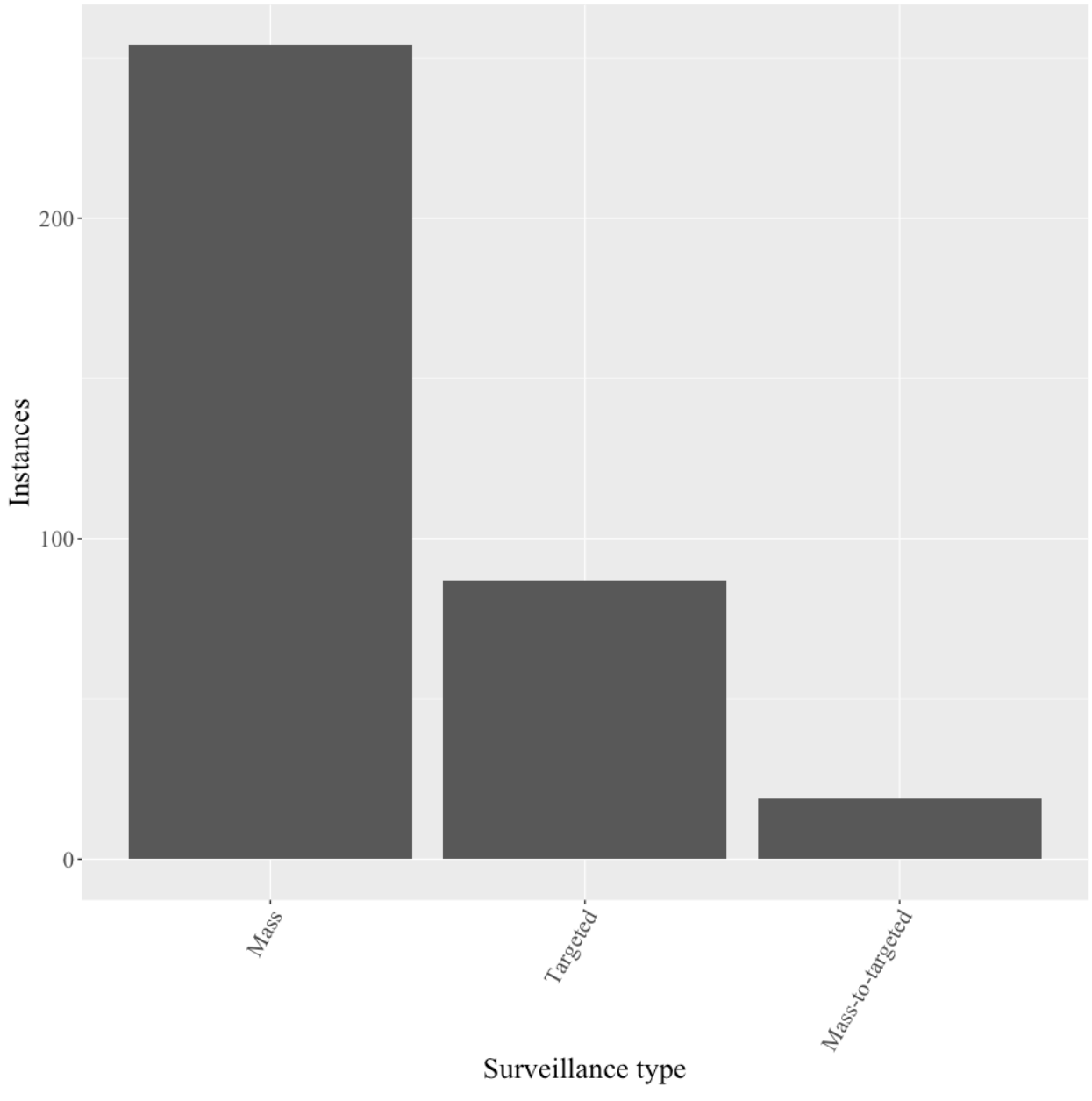
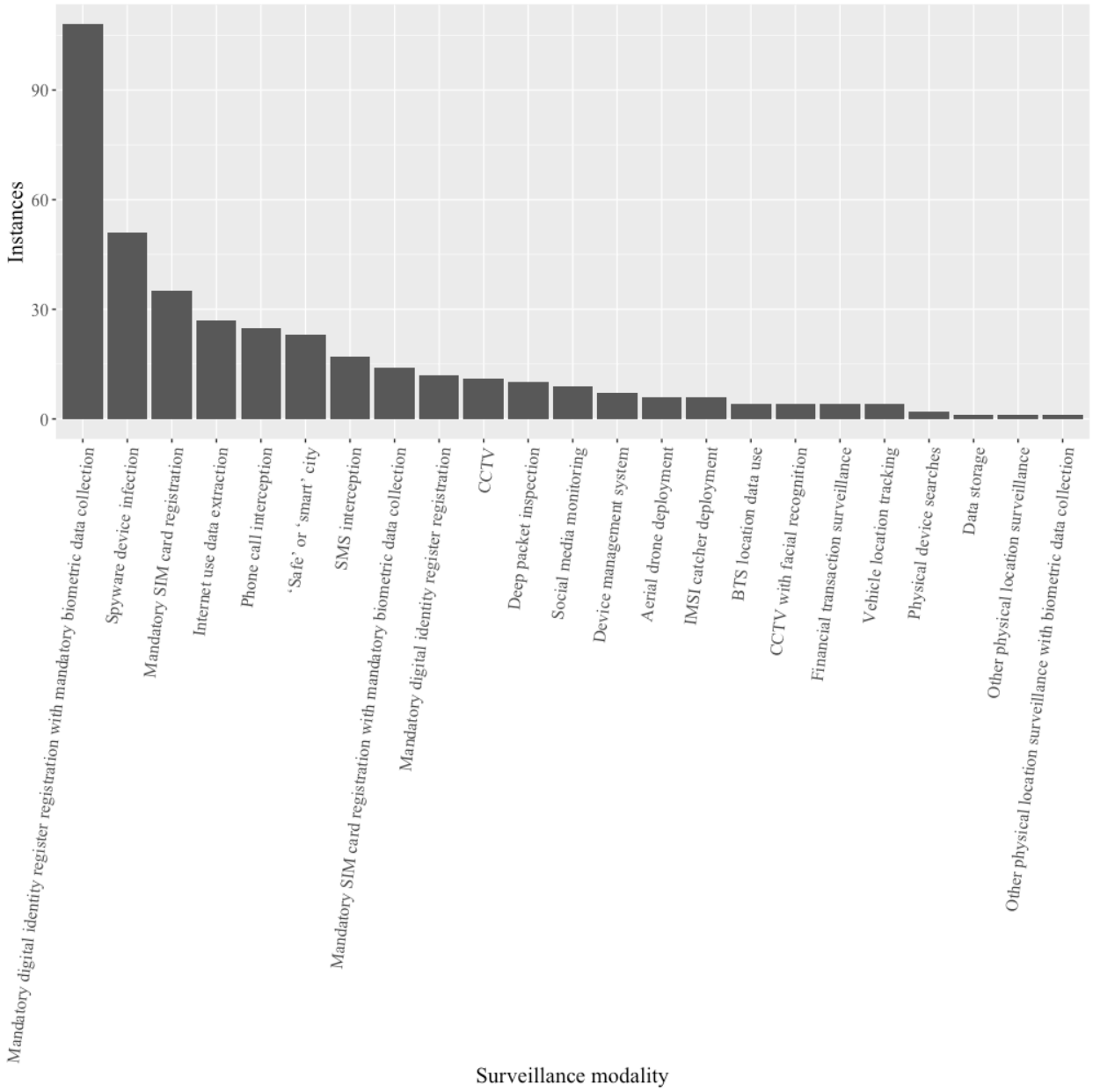


Figure 17

Surveillance modality



Foundational (Gelb & Clark, 2013) digital population registers such as Huduma Namba and Ndaga Muntu provide governments with detailed data that they put to manifold uses. In Cameroon, without an identity card provided to population register enrollees "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, 2022a). Presentation of the analogous Ghana 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, 2023b).

Other, functional (Gelb & Clark 2013), digital identity systems serve more specific purposes. The governments of Algeria, Benin, Cameroon, Côte d'Ivoire, Liberia, Kenya, Morocco, Mozambique, Niger, Nigeria, South Africa, Tunisia, Uganda, Zambia, Zimbabwe, and possibly Gabon have created biometric voter registers. To exercise their right to vote, adult citizens of those countries have to submit biometric data to authorities. Voters, for example those in the Democratic Republic of the Congo's 2023 presidential election, have also been effectively disenfranchised where logistical or technical challenges have prevented their registration. Enrollment in other systems enables access to public or private services. Public health insurance schemes in Côte d'Ivoire, Ghana, Kenya, and Nigeria collect the biometric data of registrants. Kenya's Min-

istry of Education maintains a nationwide digital student register. The governments of Guinea, Mozambique, and Zimbabwe have established biometric land title registries. Nigerian and Ugandan authorities collect biometrics from criminals. Cameroon, Equatorial Guinea, Ghana, and South Sudan have registers that contain the biometric data of public servants. Issuance of driver's licenses requires submission of biometrics in Burundi, Madagascar, Morocco, Nigeria (with plans for similar measures in South Africa). Algerian, Burundian, Kenyan, Madagascan, Moroccan, and Zimbabwean governments collect such data from passport applicants; for example, Kenyans need the "new East African Community (EAC) biometric passports if they want to be able to leave the country" (Macdonald, 2022b). Burkina Faso and Cameroon have introduced biometric visas. In Guinea, Nigeria, and Rwanda, enrollment in cash transfer and other social welfare schemes requires provision of biometrics. The Nigerian government issues dedicated biometrics-based Bank Verification Numbers necessary to open accounts with financial institutions. Such registration creates a link between account holders' identities and fund transfers, including payment card purchases, enabling authorities to monitor transactions through requests for thusly collected data. Three reported instances involve financial transaction surveillance, which is mass in each case.

SIM card registration is mandatory in all countries listed in the instances dataset, with biometrics collected in a third of them (14 instances, 3.5%, in addition to the 35 instances, 8.7%, of SIM card registration without biometric data collection). Unregistered SIM cards have been disconnected from telephony networks in Ghana, Mozambique, Nigeria, Tanzania, Uganda, and Zimbabwe. Described as "a monster especially to civil society leaders and other opinion leaders," SIM card registration in Botswana has been linked to "a lot of cases of trade unionists

and some ruling party politicians whose cell phone conversations were being tapped" (Motlogelwa, 2008).

In addition to collecting information about SIM card users, some governments have explored the creation of device management systems and registration of individual devices. The Nigerian government's plans to establish a device management system that would "serve as a repository for keeping records of all registered mobile phones' International Mobile Equipment Identity [IMEI] and owners of such devices" sparked fears "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). Seven instances of government digital surveillance (1.8%) involve creation of device management systems.

Governments also engage in mass surveillance of internet use. Egyptian, Ethiopian, Kenyan, Libyan, Moroccan, Nigerian, Sudanese, Tunisian, and Zambian authorities have deployed DPI tools; in Egypt, the government has used a DPI system "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). The dataset lists 10 instances of DPI (2.5%). Bulk collection of internet traffic data complements DPI deployments. Notably, the governments of Nigeria and South Africa have tapped undersea fibre-optic cables to intercept internet data flows. Internet use data extraction, a category that also includes targeted interception of such data, accounts for 27 instances of government digital surveillance (6.7%). Social media content is of particular interest to governments. Angolan, Kenyan, Nigerian, South African, Tanzanian, and Ugandan authorities have used social media monitoring software to keep tabs on public online communications. Uganda's social media moni-

toring centre was set up "to weed out those who use [social media] to damage the government and people's reputations" (Privacy International, 2019b). Included sources document nine instances of social media monitoring (2.2%).

The continent's governments do not limit their use of digital technologies to the surveillance of online activities. Four reported instances involve vehicle location tracking (1%). They include mandatory installation of digital location trackers in all vehicles in Uganda. More commonly reported has been the deployment of CCTV surveillance systems, some of which comprise regular CCTV cameras (15 instances in total, or 2.7%), at times equipped with facial recognition technology (four instances, or 1%). Increasingly, however, governments opt for the creation of 'safe' or 'smart' cities. In Egypt's New Administrative Capital, "[p]lanting 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" (*Reuters*, 2023). Algerian, Cameroonian, Kenyan, Nigerian, and South African authorities have also deployed such systems, with plans for their installation in Burkina Faso and Mauritius. Included publications report 23 'safe' and 'smart' cities (4.7%).

Data collected through mass surveillance can be readily used to target particular individuals and groups. Some of such mass-to-targeted surveillance relies on tools deployed by governments. Egyptian and Libyan authorities' use of bulk communications monitoring systems "to spy on opposition figures who were later detained and tortured" has attracted considerable media interest (*Agence France-Presse*, 2021). But most reported instances of mass-to-targeted surveillance involve cooperation with service providers. In Ethiopia, the ZSmart customer management system used by Ethio-Telecom, until 2022 the country's only telephony operator, collates

personal identity data, financial records, phone call metadata, SMS content and metadata, and device locations of all subscribers in addition to enabling the recording of phone calls. This information "is regularly used against Ethiopians arrested for alleged anti-government activities" (HRW, 2014, p. 3). Zimbabwean internet and telephony operators "have to provide the government with equipment to sort and intercept communications" (*Associated Press*, 2017). In South Sudan, intelligence "officers assigned to telcos have access to the company databases and can monitor specific phone numbers and even make voice audio recordings of conversations" and have compelled operators "to provide phone numbers, metadata, and call logs belonging to their customers" (*All Africa*, 2020). Included sources report 17 instances of SMS interception (4.2%) and four of the use of BTS data obtained from telephony providers (1%).

Telephony operator cooperation also facilitates (targeted) phone call interception, reported in 25 instances (6.2%). In Eswatini, the House of Assembly Speaker Themba Msibi has expressed "concerns as at times calls sound hollow, making one suspect that a third party could be listening in" (*All Africa*, 2018). The Moroccan government tapped 30,000 mobile phone lines in 2015.

Extraction of device data through installation of spyware is the most common modality through which governments reportedly deploy targeted surveillance. Included sources report 51 instances of device infection (12.7%).

Most reported infection is accomplished remotely. The governments of Egypt, Ethiopia, Nigeria, and Uganda have used Gamma's FinFisher/FinSpy suite, which takes advantage of vulnerabilities in software update systems to covertly and remotely install malware capable of monitoring computer use. The Ugandan deployment, part of operation Fungua Macho ('Open Your

Eyes'), was intended "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). 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" (*Canadian Press*, 2015). Egyptian, Ethiopian, Libya, Moroccan, Nigerian, South Sudanese, and Sudanese authorities have procured Hacking Team's Da Vinci and Galileo remote control systems, which enabled covert collection of emails, text messages, phone call history, address books, and browser search history; keystroke logging; recording of audio from both in-person conversations and phone calls as well as Skype call audio and video; device camera activation; and location monitoring through device GPS access on desktop computers and mobile phones. Predator, purchased from Intellexa, has enabled remote infection of mobile devices by government agencies in Côte d'Ivoire, Egypt, Ghana, and Madagascar as well as by Sudan's Rapid Support Forces. NSO Group's Pegasus, which serves the same purpose, has seen deployments in Algeria, Burundi, Côte d'Ivoire, Egypt, Ghana, Kenya, Libya, Morocco, Rwanda, South Africa, Togo, Tunisia, and Uganda. Ghanaian, Moroccan, Rwandan, and Ugandan governments are known NSO Group clients; foreign intelligence agencies are responsible for Pegasus infections in some of the other countries.

Reporting on device data extraction that requires physical access has been, in comparison, scarce. Ghanaian, Nigerian, Senegalese, and Ugandan authorities have obtained Cellebrite's Universal Forensics Extraction Devices and used them to retrieve the mobile phone contents. Physical searches of devices that owners unlock or provide access credentials to, generally under duress (two instances, 0.5%), such as Egypt's "random searches of phones and laptops on the

street, as part of a campaign to thwart online dissent" (Malsin & El-Fekki, 2019), serve an analogous function.

African governments have applied the remaining two modalities to both targeted and mass-to-targeted surveillance. Kenyan, Moroccan, and Ugandan governments have deployed IMSI catchers specifically to locate individual targets, while their Nigerien and Zimbabwean counterparts have passively collected Stingray data subsequently used to identify targets' whereabouts. The instances dataset lists six instances of IMSI catcher use (1.5%), evenly split between targeted (in Kenya, South Africa, and Uganda) and mass-to-targeted (in Niger and Zimbabwe, with two different instances in the latter country) surveillance. Included sources also report six instances (1.5%) of aerial drone deployment. Two of them—in Ethiopia, where federal troops used "high-tech surveillance drones bought from China […] to track and destroy targets" in Tigray (Bariyo, 2020) and in South Africa—involve targeted surveillance. Mass surveillance deployments in Ethiopia and Zimbabwe and mass-to-targeted surveillance in Niger have also relied on drones.

Categorization of the reported instances into the three types and 22 modalities reveals the breadth of government digital surveillance in Africa. Thanks to digital surveillance technologies, authorities on the continent now possess detailed, precise, sensitive, synoptic, and—where needed—continuously updated information about members of national populations, their identifying characteristics, physical locations, public and, oftentimes, private communications, internet and telephony network use, financial transactions, and the content of particularly troublesome individuals' electronic devices. Government access to these extensive personal data has no precedent on the continent and its implications are far-reaching.

Conclusion

Digitalization has presented African governments with surveillance opportunities of which they have readily taken advantage. Deployment of digital surveillance technologies has made it possible for authorities to expand their previously limited knowledge about the populations they govern. My article provides extensive evidence of this important and consequential political phenomenon. The detailed data about 372 distinct instances of government digital surveillance in Africa that I have obtained through review of multiple media repositories as well as non-media publications dwarf those previously available to scholars. The typology I have developed helps to make sense of the collected data—and information about government use of digital surveillance technologies more generally. It enables descriptive inferences concerning government digital surveillance and its key dimensions, including some to which, absent the conceptual framework introduced in the article, scholars have not given much thought. Application of the typology to the data I have gathered uncovers the scale, geographic distribution, rapidity, targets, purposes, types, and modalities of government deployment of digital surveillance technologies reported in the 589 included sources in addition to identifying specific surveillance tools and their developers.

First deployed in Africa in the early 1980s, government digital surveillance became increasingly prevalent on the continent in the 2010s. Reported in 49 countries in every African region, this surveillance has affected the lives of vast numbers of people; most deployments have targeted entire populations, with many others focused on large discrete segments of society, although governments have also frequently trained their digital surveillance apparatuses on specific antagonists in civil society, the media, and the political opposition. Targeted surveillance,

which typically requires active deployment of specialized tools purchased from suppliers such as Cellebrite, Huawei, or Intellexa, is relatively difficult and costly. Governments also rarely willingly disclose such deployment. As such, reported instances of targeted surveillance are considerably less numerous than those of mass surveillance that involves large-scale, passive, routine, and oftentimes continuous collection of personal data that, when needed, can be used to monitor individual targets. Many modalities through which governments deploy mass, as well as mass-to-targeted, surveillance, such as enrollment in mandatory digital identity and SIM card registers, necessitate action on the part of targets, while others—notably 'safe' or 'smart' cities and other CCTV systems with their relatively conspicuous surveillance cameras—have readily detectable physical manifestations; this visibility helps to explain media attention to such surveillance and attendant modalities, which account for the bulk of reported instances. Stated purposes of government digital surveillance tend to emphasize improvements in security conditions, administrative performance, and service quality that may result from its deployment, which disapprovers instead impute to efforts to expand state control over population and restrict civil rights as well as civil society, media, and opposition activities.

The purposes of government digital surveillance, stated and imputed alike, accord with its effects documented by the existing scholarly literature: improved governance and provision of public goods—which may include security enhancements as well as service delivery—but also oppression. The causal chains mediating the relationship between government digital surveillance and these effects need not be complex: deployment of the surveillance technologies available to them in the wake of digitalization enables governments to acquire detailed, precise, and synoptic knowledge about populations, which may consequently become more legible to au-

thorities that can use the information they now possess to improve the performance of a variety of government functions, from coercion to service provision and, therefore, increase state power. In Africa, where societal legibility and quality of governance have long been low, such potential impacts of government digital surveillance would be transformative. The data collected for the article provide no direct evidence of the existence of such a causal relationship. They do, however, point to its possibility, which warrants further investigation by scholars. The evidence I share in the article can offer modest support for such a scholarly endeavour. Given the limitations of reliance on media reporting, the data I have collected are not conducive to identification of broad continental patterns, even if combined with information about changes in state power and governance quality subsequent to government deployment of digital surveillance technologies. At the same time, the extensive evidence of deployment in specific instances that I have gathered makes it possible to examine causal processes that may in individual cases result in such outcomes. The effects of government digital surveillance may also well vary across settings, including due to incentives faced by authorities and societal responses to specific deployments, which merit future research as well.

References

Agence France-Presse. (2021, June 22). French prosecutors charge 4 executives over Libya, Egypt cyber-spying.

Alagbe, J. (2021, July 25). Disquiet over govt's unusual surveillance on citizens. *The Punch*.

All Africa. (2018, August 4). New law on phone personal data.

All Africa. (2020, December 14). Summary of report—inaction on dire security agency abuse.

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*.

Bentahar, Z. (2011). Continental drift: The disjunction of North and Sub-Saharan Africa. *Research in African Literatures*, *42*(1), 1–13.

Bernards, N. (2022). Colonial financial infrastructures and Kenya's uneven Fintech boom. *Antipode*, *54*(3), 708–728.

Brayne, S. (2022). The banality of surveillance. *Surveillance & Society*, *20*(4), 372–378.

Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society*, *9*(1), 205395172110653.
Calzati, S. (2022). 'Data sovereignty' or 'Data colonialism'? Exploring the Chinese involvement in Africa's ICTs: a document review on Kenya. *Journal of Contemporary African Studies*, *40*(2), 270–285.
Canadian Press. (2015, October 15). Report: Poorer, Smaller Nations Investing in Cyberespionage Tools Despite Leaks, Lawsuits.
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*.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.
Cooper, F. (1996). *Decolonization and African society: The labor question in French and British Africa*. Cambridge University Press.
Croicu, M., & Kreutz, J. (2017). Communication Technology and Reports on Political Violence: Cross-National Evidence Using African Events Data. *Political Research Quarterly*, *70*(1), 19–31.
Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., Felzmann, H., Haklay, M., Khoo, S.-M., Morison, J., Murphy, M. H., O'Brolchain, N., Schafer, B., & Shankar, K. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, *4*(2), 205395171772655.
Dauvergne, P. (2022). Facial recognition technology for policing and surveillance in the Global South: A call for bans. *Third World Quarterly*, *43*(9), 2325–2335.
Dietrich, N., & Eck, K. (2020). Known unknowns: Media bias in the reporting of political violence. *International Interactions*, *46*(6), 1043–1060.Earl, J., Maher, T. V., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances*, *8*(10), eabl8198.
Earl, J., Martin, A., McCarthy, J. D., & Soule, S. A. (2004). The Use of Newspaper Data in the Study of Collective Action. *Annual Review of Sociology*, *30*(1), 65–80.
Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.
Feldstein, S., & Kot, B. (2023). *Global Inventory of Commercial Spyware and Digital Forensics* (Version 10) [Dataset]. Mendeley Data.
Ferguson, J. (2015). *Give a man a fish: Reflections on the new politics of distribution*. Duke University Press.
Galič, M. (2022). Smart Cities as "Big Brother Only to the Masses": The Limits of Personal Privacy and Personal Surveillance. *Surveillance & Society*, *20*(3), 306–311.
Giddens, A. (1985). *The nation-state and violence*. Polity Press.
Gohdes, A. R. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science*, *64*(3), 488–503.

Gohdes, A. R. (2024). *Repression in the digital age: Surveillance, censorship, and the dynamics of state violence*. Oxford University Press.
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.
Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42–54.
Guriev, S., & Treisman, D. (2019). Informational autocrats. *Journal of Economic Perspectives*, *33*(4), 100–127.
Hersey, F. (2020, March 8). Biometrics and digital ID in Africa this week: Increasing CCTV surveillance, new ID document contracts. *Biometric Update*.
Human Rights Watch (HRW). (2014). *They know everything we do: Telecom and internet surveillance in Ethiopia*. HRW.
Iazzolino, G. (2021). Infrastructure of compassionate repression: Making sense of biometrics in Kakuma refugee camp. *Information Technology for Development*, *27*(1), 111–128.
Iwuoha, V. C., & Doevenspeck, M. (2023). Dilemmas of 'biometric nationality': Migration control, biometric ID technology and political mobilisation of migrants in West Africa. *Territory, Politics, Governance*, 1–26.
Jentzsch, N. (2012). Implications of mandatory registration of mobile phone users in Africa. *Telecommunications Policy*, *36*(8), 608–620.
Longman, T. (2001). Identity cards, ethnic self-perception, and genocide in Rwanda. In J. Caplan & J. Torpey (Eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton University Press.
Macdonald, A. (2022a, March 8). Cameroon seeks escape from its biometric national ID card woes. *Biometric Update*.
Macdonald, A. (2022b, September 27). Kenya to comply with regional bloc directive on biometric passports from end November. *Biometric Update*.
Macdonald, A. (2023, February 27). Biometrics used at 98% of Nigerian polls; advocates concerned for safety of voters' data. *Biometric Update*.
Malsin, J., & El-Fekki, A. (2019, October 8). Egypt tries to quell online dissent. *The Wall Street Journal*.
Marczak, B., Scott-Railton, J., Rao, S. P., Anstis, S., & Deibert, R. (2017). *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*.
Marshall, M. G. (2020). *Polity5 annual time-series, 1946-2018* [Dataset]. Center for Systemic Peace Data Page.
Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society*, *10*(1), 205395172211351.

Matsiko, A., & Kersting, N. (2023). The integrity of digital policies and political participation in Uganda: A tale of dissent and digital repression? *Commonwealth & Comparative Politics*, *61*(1), 2–29.
Mayhew, S. (2019, March 24). Kenya completes biometric data collection of police as public registration exercise set to begin. *Biometric Update*.
Motlogelwa, T. (2008, July 10). Media uneasy over Sim-card registration. *All Africa*.
Mukhopadhyay, S., Bouwman, H., & Jaiswal, M. P. (2019). An open platform centric approach for scalable government service delivery to the poor: The Aadhaar case. *Government Information Quarterly*, *36*(3), 437–448.
Munoriyarwa, A., & Chiumbu, S. H. (2023). Powers, interests and actors: The influence of China in Africa's digital surveillance practices. In F. A. Kperogi (Ed.), *Digital dissidence and social media censorship in Africa*. Routledge.
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*.
News Press. (2017, June 14). How surveillance, trolls, and fear of arrest affect Egypt's journalists.
Nyabola, N. (2018). *Digital democracy, analogue politics: How the Internet era is transforming politics in Kenya*. Zed Books.
PressWire. (2016, March 31). Magora app technology: Helping one despot at a time.
Privacy International. (2019a). *State of privacy Morocco*.
Privacy International. (2019b). *State of privacy Tunisia*.
Reporters Without Borders. (2024). *World Press Freedom Index 2024* [Dataset].
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.
Roberts, M. (2018). *Censored: Distraction and diversion inside China's Great Firewall*. Princeton University Press.
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.
Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). *Surveillance law in Africa: A review of six countries*. Institute of Development Studies.
Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.
Solomon, S. (2019, November 14). In Uganda, dissidents adapt to evade Huawei assisted government spying. *Voice of America*.
Weitzberg, K. (2017). *We do not have borders: Greater Somalia and the predicaments of belonging in Kenya*. Ohio University Press.

Weitzberg, K. (2020). Biometrics, race making, and white exceptionalism: The controversy over universal fingerprinting in Kenya. *The Journal of African History*, *61*(1), 23–43.
Weitzberg, K., Cheesman, M., Martin, A., & Schoemaker, E. (2021). Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society*, *8*(1), 205395172110067.
World Bank Group. (n.d.-a). *GDP per capita, PPP (current international $)—Africa* [Dataset]. World Bank Open Data.
World Bank Group. (n.d.-b). *Population, total—Africa.* [Dataset]. World Bank Open Data.
Xu, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science*, *65*(2), 309–325.
Ziaja, S., Geray, M., Sebudubudu, D., & Von Schiller, A. (2024). E-government and citizen-state relations: Evidence from a randomized information campaign with the Botswana Unified Revenue Service. *Governance*, gove.12893.