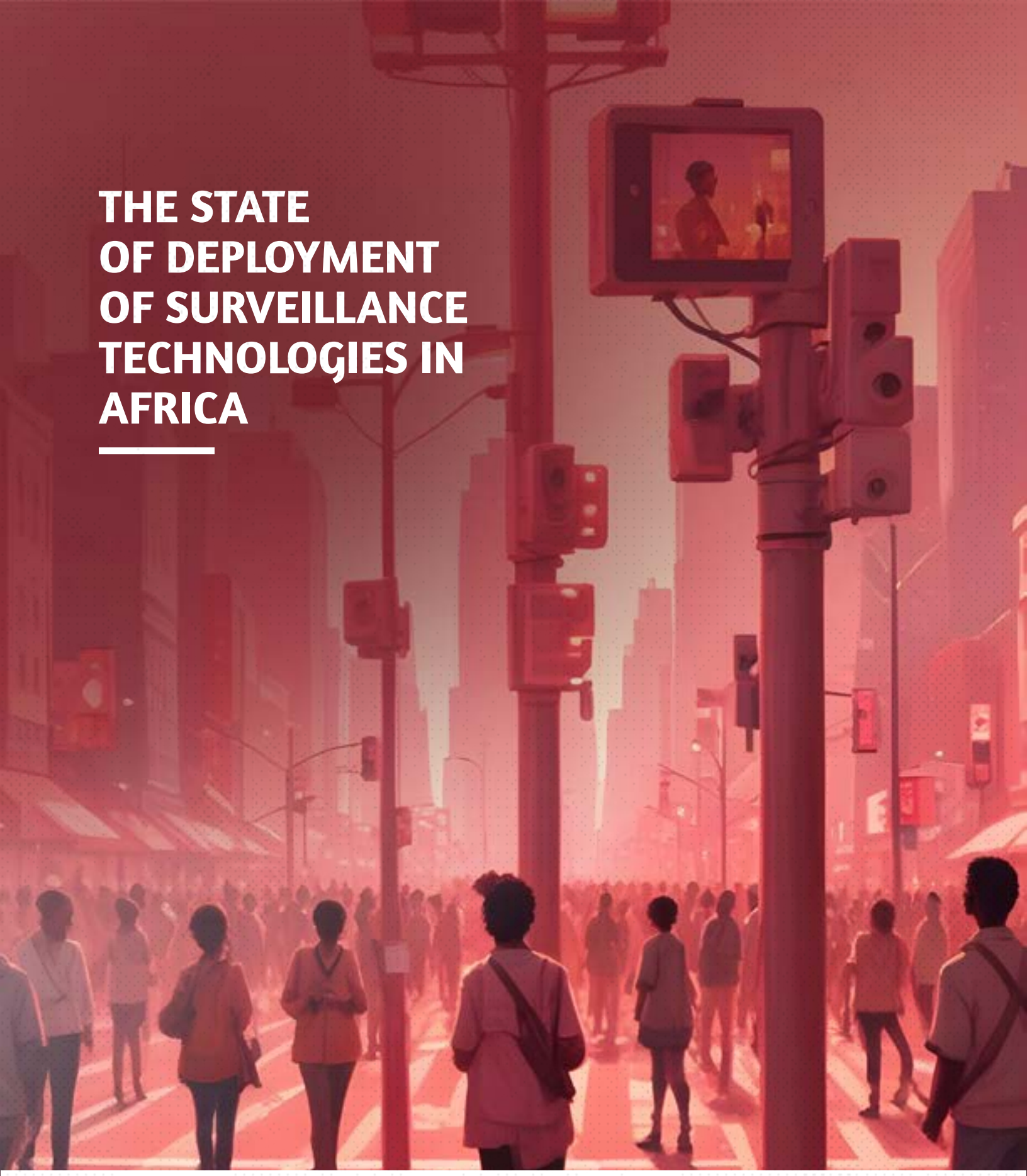
THE STATE OF DEPLOYMENT OF SURVEILLANCE TECHNOLOGIES IN AFRICA



PARADIGM INITIATIVE

THE STATE OF DEPLOYMENT OF SURVEILLANCE TECHNOLOGIES IN AFRICA

May 2024

Published by:
Paradigm Initiative with support from Open Society Foundation

Written by:
Mugambi Laibuta, Kuda Hove, Ridwan Oloyede and Aishat Salami

Editorial support:
Professor George Nyabuga and Ihueze Nwobilor

Design & Layout:
Kenneth Oyeniyi

Table of Contents

Executive Summary

Technologies such as the Internet and mobile telephony are ubiquitous in Africa, making it easier to access and share information, and communicate. The technologies have made it possible to digitise government services, such as the introduction of biometric registration and smart cities, empowering citizens to mobilise and exercise freedom of expression and association. Concomitantly, however, these technological developments present serious challenges particularly because they undermine democracy and bolster authoritarian rule as governments across the continent use them as tools and methods to monitor or surveil, manipulate, censor, and control their populace thus violating fundamental rights and freedoms. This is often premised on the notion that technology is essential to the advancement of national security, crime prevention and investigation, law enforcement, economic stability and wellbeing, public emergency and safety. Nonetheless, the report finds that surveillance technologies such as mobile spyware, internet interception, communication surveillance, biometric ID data gathering, social media monitoring, facial recognition, and car number plate identification are often used for mass citizen surveillance that results in harm.

In Central Africa, this report contends that governments in the region have and continue to use technology to monitor people, intercept their communications, and violate their fundamental rights. The report further posits that the governments of Cameroon, Chad, the Democratic Republic of the Congo (DRC), Equatorial Guinea, Gabon, and Sao Tomé & Principe have normalised surveillance.

According to the report, surveillance practices in East Africa frequently result in unwarranted encroachments upon individuals' privacy rights, thereby adversely affecting their freedom of expression, freedom of the press, freedom of movement, political rights, right to health, right to education, right against discrimination, right to dignity, and right to information access. It asserts that surveillance technology is occasionally used by Kenya, Uganda, Tanzania, and Rwanda to target specific people for abuse, incarceration, and torture because they have expressed divergent opinions. This goes against the policies of the technology companies, as well as statutory provisions, international human rights law, and constitutional safeguards.

The situation in Southern Africa is not any better. Focusing on Angola, the Democratic Republic of Congo, Malawi, South Africa, and Zimbabwe, this report broadly holds that the growing use of surveillance technologies in the countries has become a threat to the fundamental right to privacy.

In West Africa, particularly Ghana, Nigeria, and Senegal – the study countries – the study finds out that challenges such as political instability and the rise of extremist groups that pose significant security threats have exacerbated the deployment of surveillance technologies which in turn violates people's fundamental rights and freedoms.

Overall, the report contends that state surveillance is pervasive throughout Africa, threatening people's fundamental liberties and rights, and imperils democracy, constitutionalism, the rule of law, and human rights.

Introduction

Technological developments present a new frontier of threats to democracy as authoritarian governments seek new tools and methods to consolidate control and undermine fundamental rights and freedoms. Technology has made significant strides in the continent, from the race to the digitalisation of government services, such as the introduction of biometric registration and smart cities, to empowering citizens to mobilise and exercise freedom of expression and association collectively. However, it has also become clear that these new technologies, whilst giving voice to activists around the world, have also served to supercharge long-standing authoritarian survival tactics. Digital technologies have widened the toolbox of authoritarian leaders who continue to appropriate technology to control, monitor, manipulate, and censor their citizens to expand and consolidate power. The situation has seen the rise of digital repression that is supported by a booming spyware and surveillance market and big tech and mobile network companies that are exporting technologies that undermine fundamental human rights and freedoms without any accountability.

In some jurisdictions, the affronts to digital rights include the blatant blockage and take down of content online alongside overt censorship through repressive cybercrime and fake news and hate speech laws. Case in point in Uganda and Nigeria, where a social media ban (X (formerly Twitter) in Nigeria) and a subsequent introduction of the over-the-top tax in Uganda violate freedom of expression and access to information. Internet shutdowns have been commonplace, particularly during elections and political transitions in some countries such as Ethiopia, Uganda, DRC, Zambia, and Eswatini, as a mechanism of stifling the free flow of information for civic organising alongside perpetrating grave human rights abuses including mass killings during the information blackouts. The particulars of digital repression are vast and interconnected, yet the responses have not been cultivated, sustained and coordinated in a manner that can push back on the excesses of the state and network of corporations that sustain the surveillance economy and ecosystem.

Some countries on the continent recognise constitutional and conventional rights to privacy, and various actors have attempted to find solutions to this fast-evolving situation. The efforts remain scattered and fragmented, making it quite difficult to push back on digital repression using surveillance technologies effectively. The weak legal frameworks and a glaring skills gap in digital security and literacy exacerbate this situation in addition to the geopolitical North-South-East dynamics in the scramble and export of surveillance technologies that rely on artificial intelligence without providing any progressive safeguards in the continent.

This presents an opportunity to define responses and implement actions developed by individuals and groups that bear the brunt of digital repression. To this end, Paradigm Initiative, with support from Open Society Foundations, commissioned research covering Central, East, Southern and West Africa. The research mapped the state of deployment of surveillance technologies in those regions of Africa. The research had the following preliminary output: identified specific case studies of deployment of surveillance technologies, mapped actors in the surveillance ecosystem, and evaluated the regulatory framework and privacy laws landscape in the regions. It also identified the challenges and concerns in the regions as it has to do with the subject matter and made recommendations on how the challenges and concerns can be remedied.

The report presents findings from Central Africa, East Africa, Southern Africa and West Africa in that order.

The State of Deployment of Surveillance Technologies in Central Africa

By Salami, Aishat O.

Introduction

There has been a noticeable increase in internet penetration,[1] access to technological tools, social media usage, and use of cyberspace for social movements in many parts of Central Africa.[2] In addition, there have been developments in adopting international and regional instruments[3] and establishing national regulatory frameworks to protect citizen digital rights. Concomitantly, increased connectivity and progress has come with an unprecedented wave of surveillance mechanisms in the region.

Many Central African governments have adopted technological means to monitor citizens,[4] intercept their communications, and subvert their rights.[5] While state surveillance is not inherently unlawful, governments are only expected to conduct it when it is completely and legally necessary,[6] for

1 Africa: Internet Penetration by Country 2023. Statista. Retrieved October 18, 2023, from https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

2 Big Brother in the Middle-East and North Africa: The expansion of imported surveillance technologies and their supportive legislation. Retrieved October 21, 2023 from https://repository.gchumanrights.org/server/api/core/bitstreams/06ccd147-b5d3-43e3-9841-746638bade73/content.

3 Digital rights in Africa: Regional Policies - diplo resource (2023, January 18). Retrieved October 23, 2023 from https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-africa-continental-regional-policies-initiatives/.

4 Jili, B. Surveillance Tech in Africa Stirs Security Concerns – Africa Center. Africa Center for Strategic Studies. Retrieved October 23, 2023, from https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/.

5 How Enhanced State Surveillance is Hurting Digital Rights in Africa - CIPESA. (2023, June). Retrieved October 18, 2023, from https://cipesa.org/?dl_name=How_Enhanced_State_Surveillance_is_Hurting_Digital_Rights_in_Africa_Brief.pdf

6 State Surveillance and its Impacts on Children - UNICEF. Retrieved October 23, 2023 from https://www.unicef.org/globalinsight/media/1101/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf.

instance, "to prevent terrorism, monitor critical security threats, and investigate crime".[7] Over the last decade, many Central African governments have enhanced their efforts to normalise surveillance, incur substantial costs to acquire surveillance technologies,[8] implement data collection programmes, and mandate collecting biometric data and intercepting communication by telecommunication intermediaries.[9]

While variations have occurred in the regional categorization of the Central Africa nations, eight countries have consistently emerged, and are as contained within the United Nations-defined Central Africa region: Cameroon, Chad, the Democratic Republic of the Congo (DRC), Equatorial Guinea, Gabon, and Sao Tomé & Principe.[10] Out of these, only Cameroon and CAR lack data protection laws.[11] However, a vast majority of the legislation remain antiquated and out of step with contemporary "necessary and proportionate" principles.[12] Most of the laws not only allow surveillance but also compel telecom providers to assist in communication interception, [13] restrict encryption usage,[14] demand the "localisation" of personal data, and bestow quasi-independent powers on the regulatory authority.[15] The near absence of comprehensive oversight for surveillance activities exacerbates these worries. The scenarios detailed in this report therefore underscore the immediate need for a unified regional strategy that addresses data protection and privacy in the region while simultaneously meeting security requirements and upholding individual rights.

This section of the report provides a comprehensive analysis of surveillance patterns in Central Africa, with the Republic of Congo (Congo Brazzaville), Gabon, and the Central African Republic (CAR) serving as specific examples. A comprehensive analysis will be given of these countries by considering their unique regulatory frameworks, prevalent use cases, challenges faced, and the specific concerns raised by citizens and privacy experts alike. By narrowing the lens to these countries, the aim is to provide a nuanced analysis of the intersection between surveillance technologies, governance, and individual privacy in Central Africa.

The Republic of Congo

The Republic of Congo, also called Congo Brazzaville, is a francophone nation situated in Central

7 How Enhanced State Surveillance is Hurting Digital Rights in Africa - CIPESA. (2023, June). Retrieved October 18, 2023, from https://cipesa.org/?dl_name=How_Enhanced_State_Surveillance_is_Hurting_Digital_Rights_in_Africa_Brief.pdf

8 Fides, A. AFRICA - African Governments spend a total of $1 billion per year on Surveillance Technologies: Basic Human Rights at Risk - Agenzia Fides. Retrieved October 18, 2023, from http://www.fides.org/en/news/74310.

9 CIPESA. Collaboration on International ICT Policy for East and Southern Africa (CIPESA)) Retrieved October 18, 2023, from https://cipesa.org/.

10 Jamal A. Guides: African Studies and African Country Resources @ Pitt: Central African Countries. Retrieved October 23, 2023 from https://pitt.libguides.com/c.php?g=12378&p=65816.

11 Home - Privacy Lens.' Retrieved October 23, 2023 from https://privacylens.africa/.

12 Legality, Necessity and Proportionality - Privacy International. Retrieved October 23, 2023 from https://privacyinternational.org/our-demands/legality-necessity-and-proportionality.

13 Article 12, Gabon Cyber Security and cybercrime Order No. 15/PR/2018. (2018, February 23) Retrieved October 21, 2023 from droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf.

14 Article 145, Law No. 9-2009 of November 2009 regulating electronic communications. Retrieved October 20, 2023 from https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf.

15 Article 157, Law No. 9-2009 of November 2009 regulating electronic communications. Retrieved October 20, 2023 from https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf.

Africa[16] with a population of more than 6 million people.[17]

Like many of its neighbours, Congo Brazzaville has adopted surveillance technologies, citing the need for national security and stability,[18] especially in light of past political unrest and coup attempts.[19] To facilitate this, the government has also established legal structures to allow communication interception, with the judiciary purportedly overseeing this process. The moves by the government have also raised concerns among the nation's activists and journalists, who fear they are being monitored.[20] Although the Republic of Congo has a data protection law[21], there are concerns about its effectiveness, especially in the face of increasing state surveillance in the country.

Case Studies of Surveillance Deployment in the Republic of Congo

i. There have been reports that surveillance technologies are being deployed to monitor political opponents in Congo Brazzaville.[22] Specifically in May 2018, during the high-profile trial of General Jean-Marie Mokoko[23], one of the evidence presented to the court by the prosecution in proving its case of an attempted coup d'etat against President Denis Sassou Nguesso's regime were some of the telephone conversations of General Makoko that were intercepted. During the trial, one of the officers responsible for monitoring the general's telephone communications gave evidence that the general had plotted the coup with some external persons using a DRC - registered SIM card.[24] While there is no clear evidence to show if a warrant was obtained before intercepting General Makoko's telephone communications, the alleged intercepted communications are said to be instrumental in the court's sentencing of the general to 20 years in prison for breaching state security and illegally possessing weapons.[25]

16 Republic of the Congo: History, Flag, Map, Population, Capital, Language, & Facts - Britannica. (October 10, 2023) Retrieved October 19, 2023, from https://www.britannica.com/place/Republic-of-the-Congo.

17 Congo Population - Worldometer. Retrieved October 19, 2023, from https://www.worldometers.info/world-population/congo-population/.

18 Democratic Republic of Congo, past, present, and future? - Forced Migration Review. (November 2010) Retrieved from October 19, 2023, from https://www.refworld.org/pdfid/4cfe0ffc2.pdf.

19 Political Fragility in Africa: Are Military Coups D'etat a never-ending Phenomenon. Retrieved October 19, 2023, from https://www.afdb.org/sites/default/files/documents/publications/economic_brief_-_political_fragility_in_africa_are_military_coups_detat_a_never_ending_phenomenon.pdf

20 Attacks on Journalists on the Rise in East and Southern Africa. - Amnesty International. (May 3, 2023) Retrieved October 19, 2023, from https://www.amnesty.org/en/latest/news/2023/05/east-and-southern-africa-attacks-on-journalists-on-the-rise/.

21 Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel. Retrieved October 20, 2023, from https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf.

22 Bazenguissa-Ganga, R. (1999). The spread of political violence in Congo-Brazzaville. African Affairs, 98(390), 37–54. Retrieved October 19, 2023, from https://www.jstor.org/stable/723683.

23 Congo Drags Ill Former Army Chief Mokoko Back to Prison - AfricaNews. (October 2, 2021) Retrieved October 20, 2023, from https://www.africanews.com/2021/10/02/congo-drags-ill-former-army-chief-mokoko-back-to-prison/

24 Procès Jean-Marie Michel Mokoko: La Cour présente les preuves de l'accusation | adiac-congo.com: Toute l'actualité du Bassin du Congo. (n.d.). Retrieved October 19, 2023, from https://www.adiac-congo.com/content/proces-jean-marie-michel-mokoko-la-cour-presente-les-preuves-de-laccusation-83187

25 Ibid.

Instances of surveillance in public spaces in Congo have also been reported.[26] There is a proliferation of surveillance cameras in public areas of several major cities, such as Brazzaville and Pointe-Noire.[27] Related to these is the Congolese Observatory of Human Rights report[28] which chronicles the detention and release of about 13 people and the disappearance of another 30 detainees at the Regional Territory Surveillance Directorate (DRST) in Pointe-Noire. [29]

ii. There have also been occurrences of digital surveillance and its linkage to internet shutdowns in the country. The Republic of Congo has, especially during an election period, experienced telephone, internet, and media blackouts, suspicious cyber activities or citizens' limited use of messaging platforms.[30] The government is believed to use these means to intercept communications during politically uncertain times by controlling communication flow and gaining unauthorised access to people's devices and communications.[31]

iii. Reports have cited the death, disappearance, detention, and questioning of journalists and activists,[32] with some of the cases handled by the "Direction régionale de la sécurité du territoire," or the Regional Territorial Security Directorate of Congo. Also, Amnesty International documented in its 2000 annual report,[33] that a number of journalists who had been critical of the government had been threatened and intimidated. Further, a number of individuals in the country have expressed concerns about feeling constantly monitored and receiving warnings from unknown phone numbers. While most of these claims cannot be verified, as 'surveillance is often shrouded in secrecy'[34], the climate of surveillance and its accompanying feelings of fear and suspicion contributed to the 2022 Freedom House country report [35] which considers Congo 'not free', has a score of 17 out of 100 points.

---

26 Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa - CIPESA. (February 2022). Retrieved October 17, 2023, from https://cipesa.org/wp-content/files/reports/Privacy-Imperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-Africa-Report.pdf.

27 *Republic of the Congo: Freedom in the World 2022 Country Report*. Freedom House. Retrieved October 20, 2023, from https://freedomhouse.org/country/republic-congo/freedom-world/2022.

28 'Congo Brazzaville: L'arbitraire de L'État, La Terreur des Milices' International Federation of Human Rights Leagues and Congolese Observatory of Human Rights (1999). Retrieved October 20, 2023, from https://www.fidh.org/IMG/pdf/rap-braz.pdf.

29 Refugees UNHC for, 'Refworld | Republic of Congo (Congo-Brazzaville): The Territory Surveillance Division (Division de La Surveillance Du Territoire, DST), Including Its Mandate, Its Activities and Its Role in the Internal Security of the Country - Refworld. Retrieved October 20, 2023, from https://www.refworld.org/docid/3f7d4d732a.html.

30 Congo Holds Presidential Elections under Media Blackout - AlJazeera. Retrieved October 23, 2023, from https://www.aljazeera.com/news/2016/3/20/congo-in-media-blackout-for-presidential-elections.

31 Freedom House. (2022). Republic of the Congo: Freedom in the World 2022 Country Report. Retrieved from https://freedomhouse.org/country/republic-congo/freedom-world/2022.

32 Supra at note 19.

33 Amnesty International. (2000). Amnesty International annual report 2000. Retrieved October 23, 2023, from https://www.amnesty.org/en/documents/pol10/0001/2000/en/.

34 Global Information Society Watch. (2014). 2014 - Communications surveillance in the digital age. Retrieved October 23, 2023, from https://giswatch.org/2014-communications-surveillance-digital-age.

35 Freedom House. (2022). Republic of the Congo: Freedom in the World 2022 Country Report. Retrieved October 19, 2023, from https://freedomhouse.org/country/republic-congo/freedom-world/2022.

iv. There have been unconfirmed reports about Congo Brazzaville's collaboration with foreign entities and companies specialising in surveillance technologies. This collaboration, if true, might have bolstered the country's capacities in digital surveillance, enabling more sophisticated monitoring of the opposition and activists.

v. Citizens believe the government monitors their private mail, telephone conversations, and other digital communications.[36] The belief is hinged on the cases of detention and questioning of individuals who are considered to support the opposition, flowing from their digital communications. For instance, in March 2021, Alexandre Ibacka Dzabana, a Congolese human rights activist, was arrested ten days before the presidential election. His arrest was based on his alleged contact and digital communications with persons who intended to destabilise the electoral process.[37]

Regulatory Frameworks and Privacy Laws in the Republic of Congo

i. Law No. 9-2009 regulating the electronic communications sector[38]
   1. Article 125 of the law[39] prohibits persons other than the users from listening, intercepting, storing communications and data, or engaging in any means of interception or surveillance without the consent of the users concerned, except where such person is legally authorised to do so. The provision goes further to allow technical storage of such communication.
   2. Article 127[40] provides that when location data of users or subscribers of public networks is to be processed, such processing must be done within the period necessary for the provision of value-added services. Further, it must be anonymised, or processed only with the consent of users.
   3. Article 130[41] provides for the identification of subscribers at the time of subscribing to telephone services. It further allows operators of the communication networks to retain electronic communications data. Designated individuals, authorised agents of the security agencies and the national police are empowered to require the operators to reveal the information stored by them.

36 U.S. Department of State. (n.d.). Republic of Congo. Retrieved October 20, 2023, from https://2009-2017.state.gov/j/drl/rls/hrrpt/2000/af/763.htm.

37 AfricaNews. (2021, March 12). Congo: Human rights activist arrested 10 days before election. Africanews. Retrieved October 20, 2023, from https://www.africanews.com/2021/03/12/congo-authorities-arrest-top-human-rights-activist-10-days-before-presidential-election/.

38 Law No. 9-2009 of November 2009 regulating electronic communications. Retrieved October 20, 2023, from https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf

39 Article 125, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

40 Article 127, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

41 Article 130, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

4. Article 145[42] provides for the supply, transfer, import and export of cryptology.[43] It ensures that the regulatory authority has the technical characteristics and source code of the cryptology software.
5. Article 146[44] provides that the regulatory authority must be notified when cryptographic tools are supplied or brought into the country to be used for purposes other than authentication and control.
6. Article 156[45] prohibits employees in the communications sector from unauthorised disclosure of the contents of electronic communications.
7. Article 157[46] of the law forbids people from intercepting and listening to the electronic communications of others. It also provides exceptions for cases where the authorisation of the public prosecutor is sought. It lists such instances to include purposes such as ensuring state security and public order and the application of criminal and tax laws.
8. Article 177[47] prescribes imprisonment for a duration of three to six months or a monetary fine ranging from 1,000,000 to 5,000,000 CFA francs for cryptographic service providers who establish an independent network without prior authorisation, provide cryptology services without the required authorisation, or continue to offer cryptology services after the expiration of the required authorisation. It further gives the court power to confiscate the cryptology equipment in favour of the regulatory agency.
9. In accordance with Article 180[48], offenders are subject to a prison term ranging from one to six months and a monetary penalty of 2,000,000 to 12,000,000 CFA francs, with the exception of exceptional circumstances specified in the legislation.

ii. Law No. 26-2020 of June 2020 on cybersecurity[49]

1. Article 21 (Law No. 26-2020 of June 2020)[50] of the Act prescribes 10 years as the retention period of connection and traffic data by network operators and electronic communications

42 Article 145, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

43 Cryptology is a way of securing communications. See 'Cryptology - an Overview | ScienceDirect Topics' <https://www.sciencedirect.com/topics/computer-science/cryptology#:~:text=Cryptology%20is%20the%20science%20of,messages%20to%20recover%20their%20meaning.> accessed 20 October 2023.

44 Article 146, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

45 Article 156, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

46 Article 157, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

47 Article 177, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

48 Article 180, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

49 Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

50 Article 21, Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

providers in Congo. It also allows them to install monitoring mechanisms, and the data therefrom may be accessible during legal investigations.

2. Article 38 (Law No. 26-2020 of June 2020)[51] gives the national security agency information systems the power to ban, temporarily or definitely withdraw, or order fines against service providers that employ cryptology technology.
3. Article 97[52] requires service providers to keep communications confidential. It further prescribes fines for failure to comply.

iii. Law No. 29-2019 of October 10, 2019 on the protection of personal data[53]

1. Article 23[54] provides for cross-border transfer of personal data.[55] It requires that for any transfer of personal data from Congo to a third country, the data controller must pre-inform the commission. The Commission then confirms that such a third country is in compliance with the sufficiency or adequacy test.
2. Article 24[56] provides exceptions to the rule on cross-border data transfers. Such as if the transfer is one-off, not massive and the person to whom the data relates has expressly consented to their transfer, or if the transfer is necessary for protecting the person's life or safeguarding public interest.
3. Article 37[57] provides for authorisation from the commission before processing some categories of sensitive personal data. Such as genetic data and data on commission of offences.

Concerns of Surveillance Deployment in the Republic of Congo

i. Surveillance operations are not subject to independent oversight.

The law[58] requires the authorisation of the public prosecutor in situations where interception is required, such as when ensuring state security and public order or for the application of criminal and tax laws. However, the Conseil supérieur de la magistrature or Judicial Service Council, which

51 Article 38, Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

52 Article 97, Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

53 'Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel.' <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf> accessed 20 October 2023.

54 Article 23 'Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel.' <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf> accessed 20 October 2023.

55 Cross border transfer of data refers to the transmission of personal information from one jurisdiction to another. See 'Cross-Border Data Transfers' <https://iapp.org/resources/article/cross-border-data-transfers/> accessed 21 October 2023.

56 Article 24 'Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel.' <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf> accessed 20 October 2023.

57 Article 37 'Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel.' <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf> accessed 20 October 2023.

58 Article 157, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf > accessed 20 October 2023.

is responsible for the administration of justice in the country, is under the President's authority.[59] Additionally, the President appoints the members of the Supreme Court and the magistrates.[60] These provisions point to the lack of independence of the judiciary and justify the concerns of experts and residents in Congo that cases are often decided to please the government.[61] As a result, there is no way to determine if the government is spying on people because the executive arm of the government still oversees surveillance in Congo.

ii. Prohibitive policies that impose limitations on the privacy and freedom of expression of individuals.
The various provisions of the law[62] which restrict the supply of cryptographic communication tools,[63] require renewal of cryptology licences from the regulator[64], imposition of fines for establishing independent networks without prior authorisation,[65] and limit service providers from encrypting communications, undermine the digital rights of citizens. This is because these laws restrict the ability of service providers and telecommunication companies to secure and assure users of the privacy of their communications, thereby making it easy for surveillance to be perpetrated.

iii. Increased potential for misuse of user data and other risks to digital rights.
The law[66] provides a 10-year retention period for connection and traffic data and permits network operators and electronic communications providers to install monitoring mechanisms. This provision raises concerns regarding individual privacy. Additionally, it has broader implications for digital rights, as the government can abuse it to target political opponents and stifle dissent.

iv. There is an inadequacy of legal safeguards. Although the law[67] prohibits the unauthorised disclosure of electronic communications by individuals in the communication service, the

59 Article 171, <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100814/133756/F-270153886/COG-100814%20(EN).pdf> accessed 21 October 2023.

60 Article 172, <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100814/133756/F-270153886/COG-100814%20(EN).pdf> accessed 21 October 2023.

61 'UPDATE: The Legal System of the Republic of the Congo (Congo-Brazzaville): Overview and Research - GlobaLex' <https://www.nyulawglobal.org/globalex/Congo_Brazzaville1.html> accessed 21 October 2023.

62 Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf > accessed 20 October 2023.

63 Article 146, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf > accessed 20 October 2023.

64 Article 145, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf > accessed 20 October 2023.

65 Article 177, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf > accessed 20 October 2023.

66 Article 21, Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

67 Article 156, Law No. 9-2009 of November 2009 regulating electronic communications <https://admin.theiguides.org/Media/Documents/Congo-Loi-2009-09-communications-electroniques.pdf> accessed 20 October 2023.

provision essentially equates to the standard confidentiality clauses often found in employment contracts. It appears more geared towards safeguarding business interests than genuinely aiming to prevent the unlawful interception of communications. This approach does not adequately provide for the protection of individual privacy. It also raises concerns over the potential misuse and abuse of surveillance in the country.

v. Compelled assistance by service providers. The provision of the law[68] which compels stringent requirements on cryptology or encryption service providers before communications can be encrypted, prescribing of temporary or definitive withdrawal of providers' licences, fines and penalties to ensure compliance of cryptology service providers, are all means of giving the government and its agents, through the regulator, unlimited access to and control over private data.

vi. There is a lack of sufficient awareness among the Congolese people about the spread of surveillance in the country and its dire implications. The lack of public debate by the people will encourage the adoption of more surveillance tools by the government and increase the violations of digital rights in the country.

vii. There is an accumulation of data without regard for global privacy standards. Through the provision of law,[69] which mandates the localisation of data within the Republic of Congo, the government and its agencies gain easy access to and control of information. Moreso, checks and balances can be boycotted without the need to adhere to international global practises and privacy standards.

68 Article 38, Law No. 26-2020 of June 2020 on cybersecurity <https://www.sgg.cg/JO/2020/congo-jo-2020-23.pdf> accessed 20 October 2023.

69 Article 23, 'Congo - Loi N° 29-2019 Du 10 Octobre 2019 Portant Protection Des Données à Caractère Personnel.' <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110224/136994/F543159909/COG-110224.pdf> accessed 20 October 2023.

Recommendations

Government

i. When the government invokes exceptions such as state security, national defence, or prevention of terrorism to intercept communications, they should explicitly demonstrate the specific risks they aim to address. It must be evident that these actions are in the broader interest of the nation and not solely for the benefit of the government.

ii. The government, in consultation with human rights organisations and experts, should be mandated to undertake a thorough human rights impact assessment prior to the deployment of any surveillance tools.

Legislators and Policymakers

i. Legislators and policymakers, in partnership with international human rights groups and legal specialists, are recommended to undertake a comprehensive examination of existing laws to align them with global human rights norms and best practices. Essential elements of this framework should mandate user notifications, enabling individuals to contest surveillance activities, and the creation of autonomous oversight entities to monitor and regulate the government's surveillance actions and its representatives.

ii. Legislators and policymakers should establish legal frameworks to protect whistleblowers who expose instances of unauthorized or illicit surveillance activities.

Civil Society Groups and relevant stakeholders

i. There should be collaborations involving civil society groups, media organisations, and other relevant stakeholders to foster citizen engagement and awareness regarding surveillance practices. This collective effort will help in demanding that the government maintain transparency and accountability in its deployment of surveillance tools within the country.

ii. Civil society groups and all relevant stakeholders should collaborate in advocating for greater government transparency and accountability.

iii. Civil society groups, legal experts, and concerned citizens should jointly contest ambiguous legal provisions that are susceptible to misuse in court.

iv. Stakeholders, including academic institutions, civil society groups, and international organisations, should collaborate to fund and conduct in-depth research to elucidate the government's surveillance capacities.

v. Communication service providers, in collaboration with civil society groups and oversight bodies, should release detailed transparency reports outlining government requests for intercepted communications.

vi. Civil society groups should collaborate with media outlets to diligently investigate, document, and bring to light instances of unauthorised access, surveillance, and non-compliance by the government and its agencies.

Gabon

Gabon is a country in central Africa that shares borders with the Republic of Congo to the south and east, Cameroon to the north, and Equatorial Guinea to the northwest(World Bank)[70] with a population of 2,450,861[71].

The country's complex political landscape, interspersed with sporadic dissent, encourages the government to maintain a tight grip on potential opposition movements by leveraging advanced surveillance technologies to fortify its political position. Central to the government's surveillance capabilities is the nation's unified ICT framework, which has largely developed under state patronage. This close intertwining of state influence and ICT infrastructure has enabled the seamless integration of surveillance tools in Gabon.

The widespread deployment of surveillance tools in the country raises substantial concerns regarding privacy breaches and the potential misuse of personal data. It not only curtails the digital rights of the Gabonese but also threatens to stifle the democratic ethos of the nation. Although Gabon has made strides in building some data protection mechanisms,[72] concerns remain about their effectiveness in the face of increasing state surveillance.[73]

Case Studies

i. The Government of Gabon is reported[74] to have a unit where intercepted communications within the country, especially during election periods, are regularly transmitted. It is said that the interception unit, Système d'Interception Légal des Appels Modulaires, is well equipped, and the surveillance tools can work on a number of platforms.[75] Practices such as these raise concerns about infringement of rights and the freedom of the people. It would also occasion the need for self-censorship and the fear of speaking or freely partaking in democratic processes in the country.

ii. There are reports on the proliferation of surveillance technologies in the country. For instance, FinFisher, a global spyware company based in Munich, Germany, is linked to having been operational

70 'Gabon' (World Bank) <https://www.worldbank.org/en/country/gabon> accessed 23 October 2023

71 'Gabon Population (2023) - Worldometer' <https://www.worldometers.info/world-population/gabon-population/> accessed 18 October 2023.

72 Law No. 001/2011 on the protection of personal data <http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20112.pdf> accessed 23 October 2023.

73 'Gabon' (United States Department of State) <https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/gabon/> accessed 23 October 2023.

74 'Inside Africa's Increasingly Lucrative Surveillance Market' (The Africa Report.com) <https://www.theafricareport.com/22841/inside-africas-increasingly-lucrative-surveillance-market/> accessed 21 October 2023.

75 'Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa' (CIPESA, February 2022) <https://cipesa.org/wp-content/files/reports/Privacy-Imperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-Africa-Report.pdf> accessed 17 October 2023.

in the country.[76] There are also talks that French company Nexa Technologies[77] formerly Amesys telecommunication surveillance system and its software, Cerebro are operational in the country.

iii. It was reported[78] that the communications of some delegates of the European Union who were sent to observe the country's elections in 2016 were intercepted. Excerpts from the close to 20 recordings from the wiretap that revealed the lack of trust of the observers in the election output were obtained by the Journal du Dimanche. [79]

iv. Internet Shutdowns: Gabon has experienced a number of internet shutdowns, especially in the build-up to the announcement of the 2016 presidential election, which ushered the Bongo family into their fifth decade of rule in Gabon.[80] The same was also reported during the August 2023 election, where 64-year-old Ali Bongo, who got into power in 2009 after his father's rule, was seeking to run for a third term. The nationwide internet shutdown lasted for several days, with the government citing online disinformation as its basis for the internet shutdown and the imposition of night curfew. Activists and various human rights organisations have raised concerns about the government using the shutdown as a way to control and limit the public's communications during the election period.[81]

v. Surveillance of Activists and Journalists: There have been many unconfirmed reports[82] from journalists and activists in the country of being monitored and followed, receiving threatening calls from unknown numbers, and receiving phishing emails that were targeted at infiltrating their communications. This suggests the arbitrary use of surveillance to suppress dissent in Gabon.

vi. There is the deployment of surveillance cameras in public places, such as in Libreville, the capital city of Gabon.[83]

Regulatory Frameworks and Privacy Laws

A. Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018.[84]

1. Article 12[85] of the Order requires network operators and communications service providers

76 'Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware' <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf> accessed 21 October 2023.

77 'Nexa Technologies' (Nexa Technologies) <https://www.nexatech.fr> accessed 21 October 2023

78 'International' (lejdd.fr) <https://www.lejdd.fr/International> accessed 21 October 2023.

79 Ibid.

80 'EU Observers Were Wiretapped during Gabon Vote: Report' (www.euractiv.com, 3 October 2016) <https://www.euractiv.com/section/global-europe/news/eu-observers-were-wiretapped-during-gabon-vote-report/> accessed 21 October 2023.

81 Obangome GW, 'Gabon Cuts Internet, Imposes Curfew amid Election Voting Delays' Reuters (26 August 2023) <https://www.reuters.com/world/africa/gabon-vote-president-bongo-seeks-extend-56-year-family-dynasty-2023-08-26/> accessed 21 October 2023.

82 Refugees UNHC for, 'Refworld | Gabon Journalists Summoned over Critical Articles' (Refworld) <https://www.refworld.org/docid/4f70250623.html> accessed 23 October 2023.

83 'Installation and Maintenance of Security Surveillance System at UNOCA, Libreville, Gabon' <https://www.ungm.org/Public/Notice/39035> accessed 23 October 2023.

84 Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

85 Article 12, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

to retain connection and traffic data for ten years. It further requires the installation of data traffic monitoring mechanisms on their networks and an operational management center within the country.

2. Article 21[86] of the Order prohibits persons from listening to or unlawfully intercepting communications and traffic data without the consent of the users. It provides exceptions when the consent of the user or legal authorisation is obtained. It further allows for the technical storage of such communications.
3. Article 31[87] gives judicial police officers the power to access means of transport and any premises used for conducting business and request or take copies of related communications, upon summonses, to aid their investigations.
4. Article 32[88] allows the judicial police officer to keep copies of the documents under seal, but with the prior approval of the public prosecutor.

a. Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon[89]
   1. Article 17[90] of the Order requires intermediaries to identify makers of content and keep the information of all electronic transactions.
   2. Article 83[91] requires that the authorisation of a competent authority be obtained before importing, exporting or supplying cryptology for commerce.
   3. Article 84,[92] mandates the supplier, importer or exporter of cryptology to provide the technical characteristics of cryptology to a competent authority.
   4. Article 113[93] requires the approval of a cryptology service provider by the competent authority.

b. Order No. 00000015 on cyber security and the fight against cybercrime[94]
   1. Cryptology Regulations: Article 28[95] outlines specific stipulations regarding the use and

86 Article 21, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

87 Article 31, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

88 Article 32, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

89 Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon, <https://bit.ly/3ceRLvr> accessed 21 October 2023.

90 Article 17, Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon, <https://bit.ly/3ceRLvr> accessed 21 October 2023.

91 Article 83, Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon, <https://bit.ly/3ceRLvr> accessed 21 October 2023.

92 Article 84, Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon, <https://bit.ly/3ceRLvr> accessed 21 October 2023.

93 Article 113, Order No. 00000014 / PR / 2018 of February 2018 regulating electronic transactions in Gabon, <https://bit.ly/3ceRLvr> accessed 21 October 2023.

94 Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

95 Article 28, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

dissemination of cryptology in Gabon. It makes it clear that things like using, providing, importing, and exporting cryptology are legal as long as its only goal is to verify the integrity of a message or authenticate a communication. However, if encryption is sought for any other purpose, it mandates a prior declaration and subsequent authorization. Essentially, authorisation must be obtained before deploying cryptology in Gabon.

2. Decryption Requirements: Article 34[96] provides for the decryption of encrypted data upon demand by the relevant authority.
3. Article 36[97] empowers judicial authorities to issue warrants for data searches to combat cybercrime and ensure cybersecurity in the country.
4. Article 37[98] places an obligation on cryptology service providers to permit decryption when requested by judicial police officers or other authorised representatives.
5. Article 48[99] imposes a punishment of fine or terms of imprisonment for failure to provide decryption.
6. Article 52[100] prescribes terms of imprisonment or option of fine, or both imprisonment and fine for distributing prohibited cryptology tools.

c. Law No. 001/2011 on the protection of personal data[101]
   1. Article 94[102] provides for cross-border transfer of data when the receiving jurisdiction has a sufficient level of protection.

d. Deliberation No. 090 of September 22, 2020 relating to the bill on the regulation of electronic transactions in Gabon.[103]
   1. Article 17[104] requires service providers, subject to the law on personal data, to retain the identification data of persons who contributed to the creation of the content services of which they are providers.

96 Article 34, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

97 Article 36, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

98 Article 37, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

99 Article 48, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

100 Article 52, Order No. 00000015 on cyber security and the fight against cybercrime <https://bit.ly/3kF2W5c> accessed 21 October 2023.

101 Law No. 001/2011 on the protection of personal data <http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20112.pdf> accessed 23 October 2023.

102 Article 94, Law No. 001/2011 on the protection of personal data <http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20112.pdf> accessed 23 October 2023.

103 Journal Officiel de La République Gabonaise' <https://journal-officiel.ga/17800-090-cnpdcp/> accessed 21 October 2023.

104 Article 17, Journal Officiel de La République Gabonaise' <https://journal-officiel.ga/17800-090-cnpdcp/> accessed 21 October 2023.

2. Article 28[105] provides for protection of personal data and privacy of electronic commerce.

Concerns of Surveillance Deployment in Gabon

As the nation embraces digital advancements for security and governance, the unintended consequences have become increasingly apparent. From intrusive facial recognition systems to online monitoring, the pervasive surveillance apparatus has raised concerns about personal freedom, data security, and the democratic values that underpin Gabonese society.

i. The requirement of the Gabonese law[106] which restricts the supply or importation of cryptology or encryption and compels service providers to provide technical characteristics and source code of cryptology software, defeats the purpose of using cryptology to secure communication and undermines the digital rights of citizens.[107] This provision and similar provisions on cryptology serve as one of the bases on which the government relies for decrypting encrypted communications. Moreso, the limitations are also against the spirit of global privacy frameworks, and more specifically, Principle 40(3) of the Declaration of Principles on Freedom of Expression and Access to Information in Africa.[108]

ii. Although the Law[109] provides for the destruction of data collected upon the instruction of the public prosecutor, it does not provide a specific retention period before such destruction. The lack of precision in this instance could be easily abused. More than that, the public prosecutor's decision is at best a weak attempt to keep an eye on surveillance, since the public prosecutor's office is not separate from the government and cannot be used as an institutional way to check surveillance.

iii. The requirement for intermediaries to install data traffic monitoring mechanisms on their networks and to keep connection and traffic data for a period of 10 years is an attempt at allowing surveillance. As aptly put by the Electronic Frontier Foundation 2021[110] 'Government-mandated data retention impacts millions of ordinary users, compromising online anonymity which is crucial for whistle-blowers, investigators, journalists, and those engaging in political

105 Article 28, Journal Officiel de La République Gabonaise' <https://journal-officiel.ga/17800-090-cnpdcp/> accessed 21 October 2023.

106 Article 30, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023.

107 Mapping and Analysis of Privacy Laws and Policies in Africa, (Collaboration on International ICT Policy for East and Southern Africa (CIPESA)) <https://cipesa.org/> accessed 21 October 2023.

108 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (African Commission on Human and Peoples' Rights, 17 April 2020) <https://achpr.au.int/en/node/902> accessed 22 October 2023.

109 Article 32, Gabon Cyber Security and cybercrime Order No. 15/PR/2018 of February 23, 2018 <droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf> accessed 21 October 2023

110 'Mandatory Data Retention' (Electronic Frontier Foundation) <https://www.eff.org/issues/mandatory-data-retention> accessed 22 October 2023.

speech'.[111]

iv. The centralised government control of the country's telecommunications provider, Gabon Telecom, also raises concerns around unhinged access to data by government, the lack of necessary checks, and the possibility of misuse of data.

111 Ibid.

Recommendations

Government

i. When the government invokes exceptions such as state security, national defence, or prevention of terrorism to intercept communications, they should explicitly demonstrate the specific risks they aim to address. It must be evident that these actions are in the broader interest of the nation and not solely for the benefit of the government.

ii. The government should maintain transparency regarding its surveillance mechanisms and technologies.

iii. The government, in consultation with human rights organisations and experts, should be mandated to undertake a thorough human rights impact assessment prior to the deployment of any surveillance tools.

Legislators and Policymakers

i. Legislators and policy makers, in partnership with international human rights groups and legal specialists, are recommended to undertake a comprehensive examination of existing laws to align them with global human rights norms and best practices. Essential elements of this framework should mandate user notifications, enabling individuals to contest surveillance activities, and the creation of autonomous oversight entities to monitor and regulate the government's surveillance actions and its representatives.

ii. Legislators and policymakers should establish legal frameworks to protect whistleblowers who expose instances of unauthorized or illicit surveillance activities.

Civil Society Groups and Relevant Stakeholders

i. Key stakeholders, including civil society and industry experts, should advocate for increased participation from the private sector in the telecommunications industry. This diversification can reduce governmental dominance, making it more challenging for unwarranted surveillance activities to occur.

ii. There should be collaborations involving civil society groups, media organisations, and other relevant stakeholders to foster citizen engagement and awareness regarding surveillance practices. This collective effort will help in demanding that the government maintain transparency and accountability in its deployment of surveillance tools within the country

iii. Civil society groups, legal experts, and concerned citizens should jointly contest ambiguous legal provisions that are susceptible to misuse in court.

iv. Civil society groups should collaborate with media outlets to diligently investigate, document, and bring to light instances of unauthorised access, surveillance, and non-compliance by the government and its agencies.

v. Stakeholders, including academic institutions, civil society groups, and international organisations, should collaborate to fund and conduct in-depth research to elucidate the government's surveillance capacities.

vi. Civil society organisations, media entities, and relevant stakeholders are recommended to

bolster security measures and adopt best practices to shield themselves from potential digital surveillance threats.

Communication Service Providers

i. Communication service providers should consistently disclose to users the methods, timings, and recipients involved in the sharing and processing of their data.

Central African Republic (CAR)

The Central African Republic is a French-speaking country in the central region of Africa, with Bangui as its capital. It is one of the least populated countries in Africa and is also considered one of the least populated countries in the world, and its internet and mobile phone penetration rates are also among the lowest in the region.

CAR has, in the past years, witnessed a number of conflicts and has been plagued with political and security instability for more than two decades. With the unstable times in the country, the government is said to deploy surveillance tools to monitor communications, potentially suppress dissent, and ensure its continuity of power. It has also had to allow foreign forces on peacekeeping missions, who for information sharing, bring in external surveillance capabilities within the CAR territory. Sadly, the regulatory framework for surveillance in the country is not as advanced as in most other countries, neither is there a data protection framework within the country. The absence of these frameworks raises legitimate concerns about the digital rights of citizens and their data sovereignty. There is also the concern that surveillance could be normalised and abused by the government, even after overcoming the sad realities of the state of insecurity in the country.

Case Studies

i. In the wake of the various political instability plaguing the country, there have been allegations that the government of CAR is monitoring the communications of its people to stay abreast of rebel movements,[112] dissenting voices and groups suspected to be potential threats. There are documents revealing that the government 'controlled the national radio station and monitored radio transmissions and telephone conversations'[113] in CAR. In fact, the government is said to openly monitor communications of people within the country, while broadcasting some telephone communications over the government-controlled radio station.[114]

ii. Journalists, activists, and various individuals in the opposition camp in CAR have also

112 'Conflict in the Central African Republic' (Global Conflict Tracker) <https://cfr.org/global-conflict-tracker/conflict/violence-central-african-republic> accessed 23 October 2023.

113 Department Of State. The Office of Electronic Information B of PA, 'Central African Republic' <https://2001-2009.state.gov/g/drl/rls/hrrpt/2001/af/8301.htm> accessed 23 October 2023.

114 Ibid.

raised allegations of suspicion of wiretapping and different means to intercept their communications, especially during election periods. One such incident was the invasion of the house of the opposition leader, Jean-Paul Ngoupande, and the subsequent arrest of some of his political supporters.[115]

iii. Journalists and activists have also reported getting death threats based on their intercepted communications. After the 2001 coup, the editor of Le Citoyen, a newspaper in CAR, 'received death threats and was accused by the government of "fueling hatred among the population". On July 24, three employees of the newspaper were also arrested.[116]

iv. The presence of military troops from third countries seeking to ensure peacekeeping within the CAR has also allowed for external surveillance technologies and capabilities to be deployed within the country. Notable are the presence of countries such as Russia;[117] and its private security company, Wagner; and China, both regarded as powerhouses for surveillance technologies. The government also reportedly relies on the UN peacekeeping mission, which has been present on the ground for years, for information sharing.

v. In an attempt to restrict the communications of citizens, there are reports of the blocking of SMS services in the country.[118]

vi. With the use of social media tools as instruments of social mobilisation, especially by the youth and opposition groups, in recent times, there have also been alleged monitoring and shutdown of social media platforms in CAR.

vii. The traditional method of infiltrating opposition groups is also reported as being in effect in CAR. The police also rely on the incessant banditry incidents to conduct warrantless searches in the country.[119] Additionally, there are reports on the use of drones to monitor larger conflict areas within the country.

Regulatory Frameworks and Privacy Laws

In the country's digital space, the three notable laws that are in force are: 'the Law 18.002 of January 17, 2018 regulating electronic communications in the Central African Republic; Law 17.020 of May 19, 2017 which established a Regulatory Authority for Electronic Communications and Email in the Central African Republic; and Law 17.009 of February 21, 2017 which regulates postal activities in the Central

115 'Country Reports on Human Rights Practices' (Bureau of Democracy, Human Rights, and Labor 2002) <https://www.justice.gov/sites/default/files/eoir/legacy/2013/06/07/hrp01centralafricanrep.pdf> accessed 23 October 2023.

116 Department Of State. The Office of Electronic Information B of PA, 'Central African Republic' <https://2001-2009.state.gov/g/drl/rls/hrrpt/2001/af/8301.htm> accessed 23 October 2023.

117 'Russia's Wagner Group in Africa: Influence, Commercial Concessions, Rights Violations, and Counterinsurgency Failure' (Brookings) <https://www.brookings.edu/articles/russias-wagner-group-in-africa-influence-commercial-concessions-rights-violations-and-counterinsurgency-failure/> accessed 23 October 2023.

118 SMS bloqués en Centrafrique:"Une décision digne d'une dictature", <https://www.france24.com/ fr/20140604-centrafrique-sms-bloques-decision-dictature-bangui-revolte> accessed 22 October 2023.

119 Department of State. The Office of Electronic Information B of PA, 'Central African Republic' <https://2001-2009.state.gov/g/drl/rls/hrrpt/2001/af/8301.htm> accessed 23 October 2023.

African Republic'.[120] Currently, the Electronic Communications Law of 2018 is the only law regulating electronic communications in CAR.

i. Electronic Communications Law of 2018[121]

1. Article 61[122] of the law places an obligation on operators of electronic communications services to identify all subscribers of their service.
2. Article 100[123] provides for the purpose of supply or use of cryptology to be stated when it involves authenticating or ensuring integrity of communications. In other cases, the authorisation of the authority in charge must be obtained.
3. Article 112[124] requires secrecy of correspondence from operators and their employees, except in relation to protecting public safety or national defence.
4. Article 113[125] prohibits interception of electronic correspondence, except with the prior authorisation of the public prosecutor or an investigating judge when it involves judicial investigation or an authorised person when it involves administrative investigation for the protection public safety or national defence.
5. Article 119[126] allows the collection and processing of data for one year without erasure or being made anonymous, when it is for research or relating to a criminal offence.
6. Article 124[127] provides that with prior authorisation of the public prosecutor, agents duly empowered, can demand for communications processed and stored by operators for purposes of public security, national defense or to prevent acts of terrorism.
7. Article 136(2)[128] provides for exceptions to the interception of communications or secrecy of correspondence. These exceptions include when the consent of the author of the communication is obtained; prior authorisation of the public prosecutor or an investigating judge to protect public security, national defense or prevent acts of terrorism; or by the staff of the regulatory authority for purposes of identifying, isolating or preventing the

120 Communications, 'La République centrafricaine et l'intelligence artificielle dans l'espace numérique' (Paradigm Initiative, 21 October 2022) <https://paradigmhq.org/la-republique-centrafricaine-et-lintelligence-artificielle-dans-lespace-numerique/?lang=fr> accessed 22 October 2023.

121 Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_electroniques_en_RCA.pdf> accessed 22 October 2023.

122 Article 61, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

123 Article 100, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

124 Article 112, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

125 Article 113, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

126 Article 119, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

127 Article 124, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

128 Article 136(2), Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

unauthorised use of a transmission.

8. Article 147[129] prescribes fine and terms of imprisonment for failure to receive prior authorisation before importing cryptology equipment.

Concerns of Surveillance Deployment in CAR

i. Lack of sufficient regulatory frameworks to protect the digital rights of the people. For instance, the noticeable absence of privacy and data protection frameworks in CAR makes it easy for private data to be processed by the government and its agents without a legal recourse for citizens to guarantee their rights or hold the government accountable.

ii. Exploitation by External Actors: The lack of protective measures means that international entities can exploit data vulnerabilities. For instance, it's been noted that foreign technology companies have sometimes provided tools and infrastructure that can be used for surveillance purposes without adequate oversight.

iii. There are vague provisions of the law that prohibit interception of correspondence but provide exceptions in specific cases without setting limits, defining the terminologies or providing appropriate safeguards. Especially considering that the country lacks enough regulatory framework to protect its digital space, these derogations can be easily exploited in the interest of the government.

iv. Since encryption assures individuals of the privacy of their communications,[130] prohibitive regulations such as the provision of Article 100 of the Electronic Communications Law of 2018[131] can be exploited by the government to undermine the digital rights of citizens. The limitations of the provision are also against the spirit of global privacy frameworks, and more specifically, Principle 40(3) of the Declaration of Principles on Freedom of Expression and Access to Information in Africa.[132]

v. Low cyberliteracy level of the citizens, which would make it difficult for them to seek to protect their digital rights. The rapid adoption of digital technologies in the region, combined with limited public awareness of data protection and privacy rights, makes it easier for surveillance technologies to be deployed without public scrutiny.

129 Article 147, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

130 Mapping and Analysis of Privacy Laws and Policies in Africa <https://cipesa.org/?wpfb_dl=454> accessed 22 October 2023.

131 Article 100, Electronic Communications Act of 2018, <https://arcep.cf/images/textes/lois/Loi_18_002_regissant_les_communications_ electroniques_en_RCA.pdf> accessed 22 October 2023.

132 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (African Commission on Human and Peoples' Rights, 17 April 2020) <https://achpr.au.int/en/node/902> accessed 22 October 2023.

Recommendations

Government

i. The government of CAR should collaborate with foreign nations to establish mutual agreements, ensuring that any external surveillance activities by foreign entities are conducted transparently and do not infringe upon the digital rights of CAR's citizens.
ii. When the government invokes exceptions such as state security, national defence, or prevention of terrorism to intercept communications, they should explicitly demonstrate the specific risks they aim to address. It must be evident that these actions are in the broader interest of the nation and not solely for the benefit of the government.
iii. The government should maintain transparency regarding its surveillance mechanisms and technologies.
iv. The government, in consultation with human rights organisations and experts, should be mandated to undertake a thorough human rights impact assessment prior to the deployment of any surveillance tools.

Legislators and Policymakers

i. Legislators and policymakers should urgently implement robust data protection and privacy laws in CAR. They should also set up an independent data protection authority, carefully review current laws to make sure they are in line with global human rights standards and best practises, and make sure there are effective safeguards. Essential elements of this framework should mandate user notifications, enabling individuals to contest surveillance activities, and the creation of autonomous oversight entities to monitor and regulate the government's surveillance actions and its representatives
ii. Legislators and policymakers should establish legal frameworks to protect whistleblowers who expose instances of unauthorised or illicit surveillance activities

Civil Society Groups and Relevant Stakeholders

i. There should be collaborations involving civil society groups, media organisations, and other relevant stakeholders to foster citizen engagement and awareness regarding surveillance practices. This collective effort will help in demanding that the government maintain transparency and accountability in its deployment of surveillance tools within the country.
ii. Civil society groups and all relevant stakeholders should collaborate in advocating for greater government transparency and accountability.
iii. Civil society groups, legal experts, and concerned citizens should jointly contest ambiguous legal provisions that are susceptible to misuse in court.
iv. Stakeholders, including academic institutions, civil society groups, and international organisations, should collaborate to fund and conduct in-depth research to elucidate the government's surveillance capacities.
v. Communication service providers, in collaboration with civil society groups and oversight bodies, should release detailed transparency reports outlining government requests for intercepted communications.

vi. Civil society groups should collaborate with media outlets to diligently investigate, document, and bring to light instances of unauthorised access, surveillance, and non-compliance by the government and its agencies.

Conclusion

It is evident that the nexus of technology, governance, and privacy rights is both dynamic and critical, especially as seen in the spotlighted countries: the Republic of Congo, Gabon, and the Central African Republic. While the potential benefits of these technologies for governance, security, and development are undeniable, their deployment has raised legitimate concerns about individual rights, especially in the absence of comprehensive and modern privacy frameworks.

The specific use cases from each country highlight a spectrum of applications, ranging from legitimate security measures to potential tools for political control. These instances underscore the urgent need for a cohesive regional approach to data privacy, one that harmoniously integrates the necessities of national security, the imperatives of governance and the inalienable rights of the individual.

Furthermore, the recommendations put forth in this report are not just prescriptive but indicative of a broader global discourse on surveillance and privacy. For Central Africa, the way forward lies in fostering dialogue among stakeholders, updating legal and regulatory frameworks in line with global best practices, and promoting transparency and accountability in the deployment and use of surveillance tools.

In essence, the Central African region stands on the precipice of a digital era, where the decisions made today will shape its future trajectory-either towards an inclusive, rights-respecting digital society or one where technology becomes a tool for unchecked power. It is our collective responsibility to ensure the former becomes a reality.

State of Deployment of Surveillance Technologies in East Africa

By Mugambi Laibuta[133]

Introduction

Surveillance is defined as "the monitoring of a competent adult or adults over a period of time without their consent. Surveillance can be carried out on other parties (e.g. children) and it may be carried out with consent".[134] When State/governmental entities engage in surveillance activities, State surveillance refers to the ongoing close monitoring or observation of individuals by State institutions or agencies. Black's Law Dictionary defines surveillance as "close observation or listening of a person or place in the hope of gathering evidence".[135] Close observation includes collection, analysis, storage, and sharing of data, including personal data. Surveillance may be conducted physically or by use of technology. This report focuses on surveillance facilitated through use of technology.

Surveillance has been conducted for as long as humans have existed. There are numerous reasons why a State may carry out surveillance. One reason advanced to justify surveillance is national security. Essentially, the argument is that surveillance is instrumental in creating strategies and responses for a State to protect itself from threats such as internal strife terrorism, espionage, cyber-attacks, and external threats generally. Secondly, surveillance is essential for law enforcement, crime prevention, border control, and immigration. Thirdly, surveillance is key is dealing with public safety issues such

133 Advocate of the High Court of Kenya and Certified Information Privacy Manager.

134 Macnish, K. (2015). An eye for an eye: Proportionality and surveillance. Ethical Theory and Moral Practice, 18, 529-548.

135 Garner, B. A., & Black, H. C. (1999). Black's law dictionary.

as natural disasters, monitoring traffic, and monitoring public events. Fourthly, surveillance provides information for policy making processes especially in areas such as public health, education, transport, and agriculture. Fifthly, surveillance is critical in protecting a State's infrastructure such as transport networks, communications systems, energy infrastructure, border point, and security installations.

Notwithstanding the benefits of surveillance, surveillance technologies such as mobile spyware, internet interception, communication surveillance, biometric ID data gathering, social media monitoring, facial recognition, and car number plate identification can be leveraged to enable mass citizen surveillance that results in harm. Surveillance can cause harm to individuals and societies at large.

It is with the above background in mind that this report interrogates State surveillance in four East African countries, Kenya, Uganda, Tanzania, and Rwanda. The research methodology applied is desktop research.

In relation to these four countries, this report, first sets out harms that may be occasioned by State surveillance. Secondly, it highlights the constitutional provisions that may allow states to legally carry out surveillance. Thirdly, it outlines statutory provisions that facilitate surveillance. Fourthly, the report highlights State initiatives that enhance surveillance. Fifthly, it lists non-State actors involved in State surveillance. Lastly, the report provides questions for discussion when responding to State surveillance initiatives.

State Surveillance Harms

Surveillance may result in unnecessary incursions into an individual's right to privacy and negatively impact their right to freedom of expression, freedom of the press, freedom of movement, political rights, right to health, right to education, freedom from discrimination, right to dignity, and right to access information. A CIPESA Report in 2021 indicated that State surveillance negatively impacts communication privacy and the right to anonymity, leading to self-censorship and the exclusion of some individuals and groups from the online public sphere.[136] CIPESA also reported that State surveillance undermines freedom of expression, access to information, right to privacy of communications, and freedom of movement.[137]

Surveillance technology is often deployed by State actors to target specific individuals for abuse, incarceration, and torture for voicing divergent opinions, which is against policies of the technology firms, constitutional safeguards, statutory provisions, and international human rights law. On the right to privacy, Citron and Solove indicate that the harms that are closely related to privacy violations include physical, economic, reputational, emotional, relationship, chilling effect, discrimination, thwarted expectations, control, data quality, informed choice, vulnerability, disturbance, and autonomy

136 CIPESA (2021) State of Internet Freedom in Africa 2021: Effects of State Surveillance on Democratic Participation in Africa. SIFA 21 copy (cipesa.org).

137 Ibid.

harms.[138]

Privacy harms go against constitutional principles and provisions. Kenya, Uganda, Tanzania, and Rwanda have constitutional provisions that protect the right to privacy. Article 31 of the Kenyan Constitution provides that every person has the right to privacy, which includes the right not to have:

a. 'their person, home or property searched;
b. their possessions seized;
c. information relating to their family or private affairs unnecessarily required or revealed; or
d. the privacy of their communications infringed.'

Article 27 of the Ugandan Constitution reads:

'No person shall be subjected to:

- unlawful search of the person, home or other property of that person; or
- unlawful entry by others of the premises of that person.
- No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.'

Article 16 of the Tanzanian Constitution provides:

'Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.

For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.'

Article 23 of the Rwanda Constitution states:

'The privacy of a person, his or her family, home or correspondence shall not be subjected to interference in a manner inconsistent with the law; the person's honour and dignity shall be respected.

A person's home is inviolable. No search or entry into a home shall be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by the law.

Confidentiality of correspondence and communication shall not be waived except in

138 Solove, D. J., & Keats Citron, D. (2021). Privacy Harms.

circumstances and in accordance with procedures determined by the law.'

Apart from privacy violations, surveillance may result in chilling effects to other fundamental rights and freedoms. Murray et al recently published a paper titled 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe'.[139] In the paper they give accounts on the effects State surveillance has on individuals. Below are some of the responses from interviewing individuals in Uganda:

> 'Most of our community or engagements have been curtailed because the people you want to work with are suspicious. They think government [agents] are following them and they are afraid of negative impacts'

> 'At an individual level, surveillance makes it hard for me to freely engage with the population, since they live under fear of intimidation and harassment by the State agents'

> 'The surveillance and arrests have moderated me. I am not as radical as I should be because if I am on TV the surveillance is not only on me, it's also on the owner of the TV. Owners of those media houses feared, and they persuaded me to reduce the tempo ... I was bringing out the truth direct [plainly], now I have to talk in parables'

> 'There is a lot of fear. People can see the brutalization that is happening to activists now and they have opted to stay quiet for their own protection ... Not a lot of people are willing to compromise their safety and the safety of their families, they would rather just conform and not be involved in those discussions. The risk of surveillance has cowered people into submission.'

To avoid the cited harms from occurring, States ought to respect, promote, and uphold fundamental rights and freedoms as set out in constitutional, legislative, and policy texts. The next section outlines some universal principles States ought to consider when deploying surveillance technologies.

Human Rights Principles on State Surveillance

In addition to the constitutional provisions cited in this report, this report adopts the Necessary and Proportionate Principles on the Application of Human Rights to Communication Surveillance as a guide to interrogate State surveillance in East Africa.140 The Principles were advanced by a coalition of civil society organisation as concerns grew on States deploying communication surveillance without requisite legal accountability mechanisms. While the Principles are on focus on communication surveillance, they provide a good guide to assesses State surveillance generally. The principles are listed below.

139 Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2023). The chilling effects of surveillance and human rights: insights from qualitative research in Uganda and Zimbabwe. Journal of Human Rights Practice.

140 See Necessary and Proportionate.

Principle 1: Legality – any limitation to human rights must be prescribed by law. Laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.

Principle 2: Legitimate Aim – laws should only permit State surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

Principle 3: Necessity – surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim.

Principle 4: Adequacy – any instance of State Surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

Principle 5: Proportionality – State surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Huscroft, Miller, and Webber proposed a proportionality test with four questions:

a. 'Does the legislation (or other government action) establishing the right's limitation pursue a legitimate objective of sufficient importance to warrant limiting a right?
b. Are the means in service of the objective rationally connected (suitable) to the objective?
c. Are the means in service of the objective necessary, that is, minimally impairing of the limited right, taking into account alternative means of achieving the same objective?
d. Do the beneficial effects of the limitation on the right outweigh the deleterious effects of the limitation; in short, is there a fair balance between the public interest and the private right?'[141]

Principle 6: Competent Judicial Authority – determinations related to State surveillance must be made by a competent judicial authority that is impartial and independent.

Principle 7: Due Process – due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the public.

Principle 8: User Notification – those under State surveillance should be notified of a decision authorising the surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for

141 Huscroft, G., Miller, B. W., & Webber, G. (eds.). (2014). Proportionality and the rule of law: rights, justification, reasoning. Cambridge University Press.

authorisation.

Principle 9: Transparency – States should be transparent about the use and scope of surveillance laws, regulations, activities, powers, or authorities.

Principle 10: Public Oversight – States should establish independent oversight mechanisms to ensure transparency and accountability of surveillance.

Principle 11: Integrity of Communications and Systems - in order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.

Principle 12: Safeguards for International Cooperation – in response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

Principle 13: Safeguards against Illegitimate Access and Right to Effective Remedy – States should enact legislation criminalising illegal surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected.

With these principles in mind, the next section delves into the constitutional provisions in Kenya, Uganda, Tanzania, and Rwanda that may provide justification for State surveillance.

Constitutional Provisions

For State surveillance to be conducted, constitutional and statutory safeguards ought to regulate it. The safeguards should define why, by whom, when, what, how, and where surveillance is to be carried out in any given country. One of the reasons for these safeguards is the fact that surveillance has an impact on fundamental rights and freedoms of individuals, groups, and communities, and may result in harm.

The constitutional provisions highlighted in this section indicate, first, the constitutional provisions that may justify State surveillance, to wit national security. Secondly, the section highlights constitutional provisions of State agencies that may be involved in State surveillance, and lastly highlights the constitutional principles these agencies must abide by.

Kenya

Article 238 of the Constitution of Kenya sets out the principles on national security. National security is one of the justifications for conducting State surveillance. Article 238 states that "national security is the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests." To this end, the provision further provides that the national security of Kenya shall be promoted and guaranteed in accordance with the following principles:

a. 'national security is subject to the authority of this Constitution and Parliament;
b. national security shall be pursued in compliance with the law and with the utmost respect for the rule of law, democracy, human rights and fundamental freedoms;
c. in performing their functions and exercising their powers, national security organs shall respect the diverse culture of the communities within Kenya; and
d. d. recruitment by the national security organs shall reflect the diversity of the Kenyan people in equitable proportions. National security organs.'

The Constitution further establishes national security organs who are involved in ensuring national security prevails in Kenya. Under Article 239 of the Constitution, the National Security Organs are listed as:

a. the Kenya Defence Forces;
b. the National Intelligence Service; and
c. the National Police Service.

Article 241 states that the Kenya Defence Forces are "responsible for the defence and protection of the sovereignty and territorial integrity of the Republic".

Article 242 establishes the National Intelligence Service and states that the Service is "responsible for security intelligence and counterintelligence to enhance national security" in accordance with the Constitution.

Article 243 establishes the National Police Service, while Article 244 provides that the National Police Service shall "comply with constitutional standards of human rights and fundamental freedoms".

Chapter Four of the Kenyan Constitution provides for the fundamental rights and freedoms that the National Security Organs must abide by. Article 20 of the Kenyan Constitution states that "the Bill of Rights applies to all law and binds all State organs and all persons". This includes national security organs. For any fundamental right or freedom to be limited, Article 24 provides that:

'A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then

only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including:

a. the nature of the right or fundamental freedom;
b. the importance of the purpose of the limitation;
c. the nature and extent of the limitation;
d. the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and
e. the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose.'

The Kenyan Constitution establishes national security organs, sets out principles they must abide by, outlines fundamental rights and freedoms, and specifies circumstances under which the rights and freedoms may be limited.

Uganda

Article 208 of the Ugandan Constitution establishes the Uganda People's Defence Forces. One of the functions of the Defence Forces under Article 209 is to "preserve and defend the sovereignty and territorial integrity of Uganda".

Article 211 of the Ugandan Constitution establishes the Uganda Police Force. As per Article 212, the functions of Uganda Police Force include:

a. 'to protect life and property;
b. to preserve law and order;
c. to prevent and detect crime; and
d. to co-operate with the civilian authority and other security organs established under this Constitution and with the population generally.'

Article 218 of the Ugandan Constitution provides that "Parliament may by law establish intelligence services and may prescribe their composition, functions and procedures." The Intelligence Service was thus established.

On compliance with constitutional provisions, the Article 221 provides for the duty of Ugandan Security organisations to observe human rights. Article 221 state states that "it shall be the duty of the Uganda Peoples' Defence Forces and any other armed force established in Uganda, the Uganda Police Force and any other police force, the Uganda Prisons Service, all intelligence services and the National Security Council to observe and respect human rights and freedoms in the performance of their functions".

On limitation of fundamental rights and freedoms, Article 43 of the Ugandan Constitution offers a general limitation:

'(1) In the enjoyment of the rights and freedoms prescribed in this Chapter, no person shall prejudice the fundamental or other human rights and freedoms of others or the public interest.
(2) Public interest under this article shall not permit-
a. political persecution;
b. detention without trial;
c. any limitation of the enjoyment of the rights and freedoms prescribed by this Chapter beyond what is acceptable and demonstrably justifiable in a free and democratic society, or what is provided in this Constitution.'

The Ugandan Constitution establishes Ugandan Security Organisations, sets out principles they must abide by, outlines fundamental rights and freedoms, and specifies circumstances under which the rights and freedoms may be limited.

Tanzania

Article 147 of the Tanzanian Constitution defines "member of the defence and security forces" to mean "a member in the service of the Defence Forces, the Police Force, the Prisons Service or the National Service". The defence and security forces have the mandate to ensure the "defence and security of the territory and the people of Tanzania".

Article 30 of the Tanzanian Constitution on limitation on enforcement and preservation of basic rights, freedoms and duties states that "the human rights and freedoms, the principles of which are set out in (the) Constitution, shall not be exercised by a person in a manner that causes interference with or curtailment of the rights and freedoms of other persons or of the public interest." The Article also states that provisions of the Constitution which set out the basic human rights, freedoms and duties, do not invalidate any existing legislation or prohibit the enactment of any legislation or the doing of any lawful act in accordance with such legislation for the purposes of:

a. 'ensuring that the rights and freedoms of other people or of the interests of the public are not prejudiced by the wrongful exercise of the freedoms and rights of individuals;
b. ensuring the defence, public safety, public order, public morality, public health, rural and urban development planning, the exploitation and utilization of minerals or the increase and development of property or any other interests for the purposes of enhancing the public benefit;
c. ensuring the execution of a judgment or order of a court given or made in any civil or criminal matter;
d. protecting the reputation, rights and freedoms of others or the privacy of persons involved in any court proceedings, prohibiting the disclosure of confidential information, or safeguarding the dignity, authority and independence of the courts;
e. imposing restrictions, supervising and controlling the formation, management and

activities of private societies and organisations in the country; or

f. enabling any other thing to be done which promotes, or preserves the national interest in general'

The Tanzanian Constitution defines defence and security forces, sets out principles they must abide by, outlines fundamental rights and freedoms, and specifies circumstances under which the rights and freedoms may be limited.

Rwanda

Article 158 of the Rwandan Constitution lists the national defence and security organs as:

a) Rwanda Defence Force;
b) Rwanda National Police;
c) National Intelligence and Security Service.

Article 160 of the Rwandan Constitution states that the Rwanda National Police is "generally responsible for ensuring security of persons and property throughout the country". Article 161 on the National Intelligence and Security Services, states that the Intelligence Service is "generally responsible for internal and external intelligence, as well as immigration and emigration matters, for the prevention of and protection against threats to national security".

On limitation of fundamental rights and freedoms, Article 41 of the Rwandan Constitution states that "in exercising rights and freedoms, everyone is subject only to limitations provided for by the law aimed at ensuring recognition and respect of other people's rights and freedoms, as well as public morals, public order and social welfare which generally characterise a democratic society".
The Rwandan Constitution establishes the National defence and security organs, sets out principles they must abide by, outlines fundamental rights and freedoms, and specifies circumstances under which the rights and freedoms may be limited.

Statutory Provisions

To give effect to the constitutional provisions cited in the previous section, statutory provisions are necessary. Statutory provisions ought to bridge the gap between the broad, foundational principles set out in a constitution and the practical, day-to-day governance processes.

Kenya

National Intelligence Service Act

The National Intelligence Service Act was enacted to provide for the functions, organization and administration of the National Intelligence Service pursuant to Article 239(6) of the Constitution; to give effect to Article 242(2) and other relevant provisions of the Constitution". Section 3 of the Act

outlines the guiding principles of the Intelligence Services to include the need to "observe and uphold the Bill of Rights, values and principles of governance under Article 10(2), the values and principles of public service under Article 232(1) and the principles of national security in Article 238(2) of the Constitution".

Section 5 of the Act indicates that the functions of the Intelligence Service include to:

a. gather, collect, analyse and transmit or share with the relevant State agencies, security intelligence and counter intelligence;
b. detect and identify threats or potential threats to national security;
c. advise the President and Government of any threat or potential threat to national security;
d. safeguard and promote national security and national interests within and outside Kenya;
e. gather, evaluate and transmit departmental intelligence at the request of any State department or organ, agency or public entity;
f. regulate, in co-operation with any State department or agency, the flow of security intelligence between the Service and that State department or agency;'

National Police Service Act

The National Police Service Act was enacted to "give effect to Articles 243, 244 and 245 of the Constitution; (and) to provide for the operations of the National Police Service". As per Section 24 of the Act, the functions of the Police Service include:

a. 'provision of assistance to the public when in need;
b. maintenance of law and order;
c. preservation of peace;
d. protection of life and property;
e. investigation of crimes;
f. collection of criminal intelligence;
g. prevention and detection of crime;
h. apprehension of offenders;'

Prevention of Terrorism Act

The Prevention of Terrorism Act provides for the "detection and prevention of terrorist activities". Section 2 of the Act defines a terrorist act. To gather information, section 34 of the Act provides that "in addition to any power conferred by any other written law, a police officer may, for the purpose of conducting an investigation in relation to the commission of an offence under this Act, apply ex parte to a Magistrate's Court for an order for the gathering of information".

Section 35 of the Act provides for limitation of certain rights in relation to the Act. However, the

limitation must relate to:

a. 'the investigations of a terrorist act;
b. the detection and prevention of a terrorist act; or
c. that the enjoyment of the rights and fundamental freedoms by an individual does not prejudice the rights and fundamental freedom of others.'

Section 35 clarifies that the limitation of rights under the provision relate to the right to privacy, rights of an arrested person, freedom of expression, the media and of conscience, religion, belief and opinion, freedom of security of a person, and right to property. The limitations are to be applied only if they comply with section 35 of the Act cited above.

Section 36 of the Act grants powers for interception of communication, subject to a Court order. Section 36A(1) further states that "the National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary".

Data Protection Act

The Act gives effect to Article 31(c) and (d) of the Constitution, it establishes the Office of the Data Protection Commissioner, it makes provision for the regulation of the processing of personal data, provides for the rights of data subjects and obligations of data controllers and processors. Where processing of personal data for State surveillance is concerns, State agencies must comply with the provisions of the Data Protection Act and Regulations under the Act.

Of concern under the Act is section 51(2)(b) that provides for that processing of personal data is exempt from the provisions of the Act if it is necessary for national security or public interest. The General Regulations under the Act indicate that national security means processing of personal data by a national security organ established under the Kenyan Constitution. But, the Regulations give the Cabinet Secretary powers to exempt data controllers and data processes on the ground of national security.

Uganda

Police Act

The Ugandan Police Act was enacted to provide for the structure, organisation and functions of the police force, a police disciplinary code of conduct, a Police Welfare Fund, and a police tender board. As per section 4 of the Act, the Force's functions include:

a. 'to protect the life, property and other rights of the individual;
b. to maintain security within Uganda; to enforce the laws of Uganda;
c. to ensure public safety and order;

d. to prevent and detect crime in the society.'

Section 21 of the Act lays out the powers and duties of a police office to include to "collect and communicate intelligence affecting the public peace". According to the Code of Conduct of police officers set out in Section 44 of the Act, a police officer should "not take away the liberty or rights of any person without reasonable cause".

Anti- Terrorism Act

The Ugandan Anti-Terrorism Act was enacted to:

> 'suppress acts of terrorism, to provide for the punishment of persons who plan, instigate, support finance or execute acts of terrorism; to prescribe terrorist organisations and to provide for the punishment of persons who are members of, or who profess in public to be members of, or who convene or attend meetings of, or who support or finance or facilitate the activities of terrorist organisations; to provide for investigation of acts of terrorism and obtaining information in respect of such acts including the authorising of the interception of the correspondence of and the surveillance of persons suspected to be involved in acts of terrorism'

Section 7 of the Act lists acts and omissions that may constitute the offence of terrorism. Section 19 of the Act grants powers to authorised officers to "to intercept the communications of a person and otherwise conduct surveillance of a person" under the Anti-Terrorism Act. The purpose for such interception would be:

a. 'safeguarding the public interest;
b. prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism;
c. preventing or detecting the commission of any offence; or
d. safeguarding the national economy from terrorism.'

However, under section 19, the scope of the interception and surveillance allowed is limited to:

a. 'the interception of letters and postal packages of any person;
b. interception of the telephone calls, faxes, emails and other communications made or issued by or received by or addressed to a person;
c. monitoring meetings of any group of persons;
d. surveillance of the movements and activities of any person;
e. electronic surveillance of any person;
f. access to bank accounts of any person; and
g. searching of the premises of any person.'

The Regulation of Interception of Communications Act

The Regulation of Interception of Communications Act provides for the lawful interception and monitoring of certain communications during their transmission through a telecommunication, postal or any other related service or system in Uganda; and provides for the establishment of a monitoring centre.

As per section 4 of the Act, an application for the lawful interception of any communication may be made by the the Chief of Defence Forces or their nominee; the Director General of the External Security Organisation or their nominee; the Director General of the Internal Security Organisation or their nominee; or (d) the Inspector General of Police or their nominee. The warrant for interception of any communication is made to a designated Judge.

Data Protection and Privacy Act

The Act seeks to protect the privacy of the individual and personal data and regulate processing of personal information. The Act provides for data subject rights, obligations of data controllers and processors plus regulate use and disclosure of personal information. Where processing of personal data for State surveillance is concerns, State agencies must comply with the provisions of the Data Protection and Privacy Act and Regulations under the Act.
Section 7(2)(b)(ii) of the Act indicates that personal data may be collected or processed where it is necessary for national security, and for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law.

Tanzania

The Police Force and Auxiliary Services Act

The Police Force and Auxiliary Services Act was enacted to provide for the "organisation, discipline, powers and duties of the Police Force, a Police Reserve and an Auxiliary Police Force". As per section 5 of the Act, the "force shall be employed in and throughout the United Republic for the preservation of the peace, the maintenance of law and order, the prevention and detection of crime, the apprehension and guarding of offenders and the protection of property, and for the performance of all such duties and shall be entitled to carry arms".

Under section 27 of the Act, the powers and duties of a police office are "promptly obey and execute all orders and warrants lawfully issued to him, collect and communicate to his superior officers intelligence affecting the public peace, take all steps necessary to prevent the commission of offences and public nuisances and to detect and bring offenders to justice, and to apprehend all persons whom he is legally authorised to apprehend and for whose apprehension sufficient ground exist".

The Tanzania Intelligence and Security Service Act

The Tanzania Intelligence and Security Service Act was enacted to establish the Tanzania Intelligence and Security Service which under section 5 has as part of its functions, the power to "obtain, correlate,

and evaluate intelligence relevant to security, and to communicate any such intelligence to the Minister and to persons whom, and in the manner which, the Director-General considers it to be in the interests of security". Section 5 has a caveat that:

'It shall not be a function of the Service:

a. to enforce measures for security; or
b. institute surveillance of any person or category of persons by reason only of his or their involvement in lawful protest, or dissent in respect of any matter affecting the Constitution, the laws or the Government of Tanzania.'

Prevention of Terrorism Act

Prevention of Terrorism Act seeks set out "comprehensive measures of dealing with terrorism, to prevent and to co-operate with other states in the suppression of terrorism". Section 4 of the Act defines a terrorism act. The Act also provides for intelligence gathering, on this, section 30 provides that:

'The Minister may, for the purposes of the prevention or gathering detection of offences of terrorism or for the purposes of prosecution of offenders under this Act, give such directions as may appear to him to be necessary to:

a. communication service providers generally;
b. communication service providers of a specified description;
c. any particular communication service provider.

Before giving a direction under this section, the Minister may consult any communication service provider he deems fit to consult.'

Under section 31 of the Act, "a police officer may, for the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order".

Personal Data Protection Act

The Act provides for principles of protection of personal data, it establishes the Personal Data Protection Commission, and provide for improvement of protection of personal data processed by public and private bodies.

Section 58(2) of the Act reads that processing of personal data may be exempted from the provisions of the Act if such processing is held for purpose of safeguarding national safety and security and public interest, for the purpose of prevent or detect crimes, for the purpose of detect or prevent tax evasion, for the purpose of investigation of misappropriation of public funds, and for the purpose of vetting for appointment to any public service position.

Rwanda

Law on Determining the Powers, Responsibilities, Organization and Functioning of the Rwanda National Police

In Rwanda, the Law on Determining the Powers, Responsibilities, Organization and Functioning of the Rwanda National Police provides direction on the powers and functions of the Police Force. Article 6 of the Law states that the National Police shall serve to ensure "safeguarding the fundamental rights guaranteed by the Constitution and other laws", "maintaining safety and security of people and property", and "understanding the people's right to monitor its activities".
Section 7 sets out the responsibilities of the Police to include:

a. 'ensuring compliance with the law;
b. maintaining public order inside the country;
c. ensuring safety and security of people and property;
d. assisting any person in danger;'

Section 8 highlights that the Police are also to be engaged in "preventing, detecting and investigating offences".

Law Governing Information and Communication Technologies

Article 123 on the Law Governing Information and Communication Technologies states that "notwithstanding the provisions of the Constitution of the Republic of Rwanda of 2003 revised in 2015, an electronic communications network or service provider must equip the electronic communications network and service with technical instruments and features that allow and facilitate the lawful interception of electronic communications and monitoring".

Law on Regulating the Interception of Communications

The Law establishes methods of interception of communications. The law defines interception to mean "any act of listening, recording, storing, decrypting, intercepting, interfering with, or carrying out any other type of surveillance over voice or data communications without the knowledge of the user and without explicit permission to do so".

Article 3 of the Law states that "interception of communications shall be considered lawful where it is done in the interest of national security". Under Article 6, "only Government authorities of the relevant security organs as provided for by the Constitution of the Republic of Rwanda shall be authorized to apply for an interception warrant".
Article 7 emphasises that a "communication service provider shall ensure that systems are technically capable of supporting interceptions at all times upon request by the competent organ, in accordance with the provisions" of the Law.

Law on Regulating the Protection of Personal Data and Privacy

The Law aims at the protection of personal data and privacy and determines their processing. Article 52 on retention of personal data provides that a data controller or a data processor may retain personal data for a longer period for purposes of protection national security.

Conclusion

Applying some of the principles set out in section three of this report, some gaps or grey areas may be identified.

On legality and legitimate aim for State surveillance, the statutory provisions in Kenya, Uganda, Tanzania, and Rwanda spell that out. National security features heavily as the overarching legitimate purpose to carry out surveillance.

On availability of competent judicial authorities, a deep dive into the cited statutes and constitutional provisions indicates that before surveillance is conducted, State agents ought to seek orders/warrants from the courts. There are no public records available to verify whether this is always the case, bringing into question transparency in State surveillance.

On public oversight, constitutional commissions such as human right commissions plus parliaments ought to provide required oversight over State agencies carrying out surveillance. However, questions will arise on the effectiveness of such oversight. In Kenya, the National Intelligence Service Act sets oversight mechanism including the National Intelligence Service Council, parliamentary oversight, and the Intelligence Service Complaints Board. The Intelligence Service Complaints Board has never been established even with court orders mandating the same.

On integrity of communication systems, it is clear from provisions in Uganda and Rwanda specifically that the systems are open to access by State agencies as mandate by law.

The national security exemptions under the data protection laws in Kenya, Uganda, Tanzania, and Rwanda while legitimate may be subject to abuse if the data protection oversight authorities are not afforded the independence they require to carry out data protection audits for State agencies.
Bearing this above in mind, the next section gives examples of State initiatives that works towards facilitating State surveillance by providing databases with troves of personal identifiable information.

Initiatives Enhancing Surveillance

Setting up surveillance systems is a process that takes decades. Kenya, Uganda, Tanzania, and Rwanda have over time set up initiatives that make surveillance easier. With technology and access to data processed under these initiatives, surveillance capabilities are enhanced while making individuals vulnerable to State surveillance harms. A few initiatives are highlighted below.

Kenya

Mandatory SIM Card Registration

Regulation 4 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 requires all mobile network providers to register all SIM card subscribers. Regulation 5 lists the information required for SIM card registration to include:

> 'full names; identity card, service card, passport or alien card number; date of birth; gender; physical address; postal address, where available; any other registered subscriber number associated with the subscriber; an original and a copy of the national identity card, service card, passport or alien card; an original and a copy of the birth certificate, in respect of registration

of minors; subscriber number in respect to existing subscribers; an original and true copy of the certificate of registration, where relevant; a letter duly sealed by the chief executive officer or the person responsible for the day to day management of the statutory body.'

Digital Number Plates

In 2022, Kenya launched the digital number plates system that requires all motor vehicle owners to apply for new digital number plates. The digital number plates contain a QR code, National Transport Safety Authority serial number, the Kenyan flag, a hologram, and a micro-chip. The digital number plates are aimed at eliminative duplication of number plates and allow law enforcement to track vehicles and provide tools for the Kenya Revenue Authority to track tax evaders.[142]

CCTV Network

Around 8 years ago, the Kenyan government installed a CCTV network across major cities, mainly in Nairobi and Mombasa.

Digital Identity Cards

Section 9A of the Registration of Persons Act provides for the National Integrated Identity Management System (NIIMS). The government registered people to get digital IDs. The programme was halted by the courts but recently the government has come up with a new initiative.

A new initiative was launched to provide a Unique Personal Identifier to all Kenyans at birth. The number is to serve as the registration number for all government services including enrolment to educational institutions, national health insurance, for taxation purposes, and national social security.

Uganda

Intelligent Transport Management System (ITMS)

Recently, the Ugandan government announced the adoption of the Intelligent Transport Management System (ITMS) that requires the re-registration of all motor vehicles, motorcycles, and other vessels. The System will use updated license plates to issue traffic fines, as a measure of monitoring to allegedly curb theft, and to enhance safety.[143]

CCTV System

The Ugandan government installed a CCT network managed through a National Command Centre.

Mandatory SIM Card Registration

Section 9 of the Regulation of Interception of Communications Act provides:

'(1) Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, it shall obtain:

(a) the person's full name, residential address, business address, postal address and his

142 How to apply for digital number plates. How to apply for digital number plates (the-star.co.ke).

143 Intelligent Transport Management System (ITMS). Intelligent Transport Monitoring System (ITMS) - infrastructure.go.ug.

or her identity number contained in his or her identity document, if applicable;
(b) in the case where the person is a business organization, its business name and address and the manner in which it is incorporated or registered.'

Tanzania

Mandatory SIM Card Registration

The 2010 Electronic and Postal Communications Act requires the Communication Regulatory Authority to maintain a database of all subscriber information. Under Section 89 of the Act all subscriber information is to be kept by the Tanzania Communications Regulatory Authority which maintains a database of subscriber information. Under section 93 of the Act, "Every person who owns or intends to use detachable SIM card or built-in SIM card mobile telephone shall be obliged to register SIM card or built in SIM card mobile telephone".

Registration of VPN Users

In early October 2023, the Tanzania Communications Regulatory Authority cited Regulation 16(2) of the Electronic and Postal Communications (Online Content) Regulations to reiterate that no one should use or distribute technology that allows or helps users to have access to prohibited content. The Authority was making reference to use of VPNs and demanded that anyone using VPNs must declare their VPN and their IP address to the Authority. The Authority indicated that it would take stern action against anyone not complying with the notice.

Rwanda

Mandatory SIM Card Registration

Regulation 4 of the Regulations On Sim Card Registration Issued by Regulatory Board Rwanda Utilities Regulatory Agency requires that "any licensee operating in the Republic of Rwanda shall register all subscribers and SIM card holders using its network and services in accordance with the provisions of these regulations".

Single Digital ID system

The Rwandan government is in the process of putting in place a single digital identity system for Rwandans, stateless persons, and children at birth. It was reported that:

'The enactment of the new law relating to enrolment into a single digital identity system will enable the country to close the existing gap in the current population identification system to a more advanced, effective, and efficient delivery of services in both private and public sectors.'[144]

144 Stateless Persons, Newborns to Get Rwandan Digital ID. Stateless Persons, Newborns to Get Rwandan Digital ID – KT PRESS.

Conclusion

From the list of initiatives above, Kenya, Uganda, Tanzania, and Rwanda have been progressively setting up initiatives that provide State agencies with a large amount of real time data that may be used for surveillance activities.

The principles that come into question is whether such initiatives are proportional to the legitimate objectives they seek to achieve. For example, a court decision in Kenya in *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology*[145] that halted the implementation of the Digital ID faulted the government for not carrying out a data protection impact assessment that would have identified the proportionality, harms, and risks of the programme. Data protection and human rights impact assessment are necessary in State surveillance initiatives.

State actors in many cases usually engage non-State actors in their surveillance activities. Technology for surveillance is mainly provided for by private sector actors. The next section identifies some of these actors in Kenya, Uganda, Tanzania, and Rwanda.

Non-State Surveillance Actors

As stated above, technologies used by State actors to carry out surveillance are in most cases developed by private corporations. These technologies are predominantly sourced from China, Israel, the European Union, and the USA. This section lists some of the private actors in State surveillance in Kenya, Uganda, Tanzania, and Rwanda.

Jili offers a few reasons as to why China has made great in road in providing surveillance technology to African countries.[146] One, "Africa's significant digital infrastructure gap is being addressed through Chinese investment and state support." Two, "China plays a monopolistic role in Africa's telecommunications sector, supplying approximately 70 percent of the continent's digital infrastructure". Three, "surveillance tools are typically purchased as part of a package of ICT systems, which include data centres, closed-circuit television (CCTV) systems, and high-tech biometrics that are integrated and used in tandem with AI". Four, "African state and city officials in Kenya, Uganda, Ethiopia, South Africa, and other countries are reaching out to Chinese firms to aid their varying domestic aims. Together these examples illustrate the establishment of local digital governance regimes. They are not simply a derivative of a Beijing concocted vision, rather, Chinese firms are acquiescing to the ambitions of their host.".

The involvement of non-State actors in providing surveillance infrastructure raises multiple concerns:

a. Are States able to able to provide sufficient oversight to the private companies as they put in place surveillance technologies?
b. What level of access do the private companies have on State data, personal data, and intelligence processed by the technologies?
c. What is the extent of accountability for the private companies when their technology is used

145 Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Ex Parte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party) [2021] eKLR.

146 Belelani, J. (2020 May 15) What is driving the adoption of Chinese surveillance technology in Africa? What is driving the adoption of Chinese surveillance technology in Africa? - DFRLab.

for human rights abuses?

d. What are the legal safeguards in the contractual relation between States and the private contractors?
e. Who has effective control over the deployed surveillance technology?
f. What is the security of data processed from surveillance programmes?
g. To what extent do the private contractors consider ethical concerns related to their technology?
h. How are commercial interests balances vis a vis public interest?

Kenya

Safaricom

Safaricom describes itself as "purpose-led technology company providing a wide range of services and solutions, including mobile voice, messaging, data, financial and converged services, and digital services that enable commercial and personal platforms as well as ecosystem partnerships".[147] Safaricom is Kenya's leading telecommunication company with over 60% of the market share.

In 2014, the Government of Kenya signed a contract with Safaricom, the dominant telecommunications company in Kenya to roll out a National Surveillance, Communication and Control System, for Nairobi and Mombasa. According to a press release by Safaricom:

> 'The development effectively means that Safaricom can now embark on the process of building the secure communications and surveillance network. The solution will also include the installation of cameras in the two cities to provide real-time footage to the National Police Operations Centre.'[148]

NSO

NSO is an Israeli company that offers cyber intelligence services around the world. A 2018 Citizen Lab Report revealed NSO Pegasus infections in Kenya.[149] According to the Citizen Lab Report, Pegasus is produced by an Israel-based "Cyber Warfare" vendor NSO Group. The use of Pegasus is:

> 'To monitor a target, a government operator of Pegasus must convince the target to click on a specially crafted exploit link, which, when clicked, delivers a chain of zero-day exploits to penetrate security features on the phone and installs Pegasus without the user's knowledge or permission. Once the phone is exploited and Pegasus is installed, it begins contacting the operator's command and control (C&C) servers to receive and execute operators' commands, and send back the target's private data, including passwords, contact lists, calendar events,

147 Safaricom Who we are – Safaricom

148 Government Gives Official Go-Ahead to Safaricom for Security Contract. Government Gives Official Go-ahead To Safaricom For Security Contract.

149 Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.

text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone's camera and microphone to capture activity in the phone's vicinity.'

Circles

Circles is also a cyber surveillance company related to NSO. A 2020 Citizen Lab Report revealed that *Circles* surveillance software was used in Kenya.[150] According to the Report:

> 'Circles is a surveillance firm that reportedly exploits weaknesses in the global mobile phone system to snoop on calls, texts, and the location of phones around the globe. Circles is affiliated with NSO Group, which develops the oft-abused Pegasus spyware. Circles, whose products work without hacking the phone itself, says they sell only to nation-states. According to leaked documents, Circles customers can purchase a system that they connect to their local telecommunications companies' infrastructure, or can use a separate system called the "Circles Cloud," which interconnects with telecommunications companies around the world.'

Huawei

Huawei is a Chinese company and provides information and communications technology (ICT) infrastructure and smart devices around the world. It is reported that Huawei:

> '... offers a range of products, services, and business solutions for telecom carriers, including wireless network, fixed network, cloud core network, carrier software, IT infrastructure, network energy, professional services, and network rollout services. It also builds a digital infrastructure platform utilizing cloud computing, software-defined networking, big data, and IoT to enable the digital transformation of the government, public utilities, finance, energy, transport, and manufacturing industries.'

A report by Huawei in 2016 indicated:

> 'Huawei Safe City Solutions have been widely deployed across the globe. For example, Huawei helped Kenya improve public safety by establishing safe city systems consisting of a Computer-Aided Dispatch (CAD) system, broadband trunking eLTE, video surveillance, and intelligent analysis (license plate recognition and traffic violation detection). According to Kenya's annual police report, the crime rate in the regions covered by the system declined by 46 percent in 2015 compared to the previous year. In particular, the solution played a vital role in ensuring the safety of Pope Francis during his visit to Kenya on November 26, 2015.'

Uganda

Huawei

Reports indicate that Uganda's CCTV network was provided by Huawei from China.[151] In 2019 a report

150 Marczak, B., Scott-Railton, J., Prakash Rao, S., Anstis, S., & Deibert, R. (2020). Running in circles: Uncovering the clients of cyberespionage firm circles.

151 CCTV cameras finally arrive. CCTV cameras finally arrive | Monitor.

appeared in the Wall Street Journal that stated:

> 'In Kampala, Uganda, Huawei employees reportedly helped Uganda's cyber-surveillance unit break into the WhatsApp group belonging to Bobi Wine, a political opponent to the current Ugandan president Yoweri Museveni. The Huawei employees used spyware made by an Israeli company to break into the WhatsApp group, which led to Wine's arrest, as well as the arrest of dozens of his supporters.'[152]

Gamma International GmbH

Research reveals that Gamma Group is an Anglo-German technology company that sells surveillance software to governments and police forces around the world. A Privacy International Report in 2015 disclosed that Gamma group sold their FinFisher software to the Ugandan government.[153] FinFisher is software that may be covertly installed on targets' computers by exploiting security lapses in the update procedures of non-suspect software. Privacy International in its 2015 Report stated:

> '...Chieftaincy of Military Intelligence (CMI) and Uganda Police Force (UPF), acting on presidential orders, used an intrusion malware, short for malicious software, to infect the communications devices of key opposition leaders, media and establishment insiders. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili), according to documents acquired by Privacy International...'

The Report further stated that:

> 'Covert FinFisher 'access points' in the form of fake Local Area Networks (LANs) were installed within Parliament and key Government institutions. Actual and suspected Government opponents were targeted in their homes. Fake LANs and wireless hotspots were set up in apartment estates and neighbourhoods where many wealthy Ugandans and expatriates live.'

NSO Pegasus

A 2018 Citizen Lab Report revealed NSO Pegasus infections in Uganda.[154]

Rwanda

NSO Pegasus

A 2018 Citizen Lab Report revealed NSO Pegasus infections in Kenya (Citizen Lab, 2018). According to the Citizen Lab Report, Pegasus is produced by an Israel-based "Cyber Warfare" vendor NSO Group. In 2021, an Amnesty International Report revealed:

> 'New evidence uncovered by Amnesty International and Forbidden Stories has revealed that Rwandan authorities used NSO Group's spyware to potentially target more than 3,500

152 Huawei technicians have been helping governments in Uganda and Zambia spy on their political opponents, a new report says. Huawei technicians have been helping governments in Uganda and Zambia spy on their political opponents, a new report says | Business Insider Africa.

153 Privacy International (2015) For God and My President: State Surveillance In Uganda.

154 Citizen Lab (2018) HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.

activists, journalists and politicians. It was also used to infect the phone of Carine Kanimba, Paul Rusesabagina's daughter, of Hotel Rwanda fame.'

Conclusion

The examples listed in this section indicate that States will in many occasions deploy technology provided by private corporation to carry out legitimate and illegitimate surveillance activities. Pegasus, Circles, and Finfisher are examples of extrajudicial use of surveillance technologies by state actors.

Huawei and Safaricom are examples of legitimate use of private actors' technology. However, the questions raise in the beginning of this section must be addressed.

Responding to State Surveillance

From the above discussions, conversations in the convening on Countering Surveillance and Digital Repression in Africa should look at the following when considering strategies to responding to State surveillance:

- Who are the State actors engaged in surveillance?
- Who are the individuals or communities subject to surveillance?
- Who are the non-State actors involved in State surveillance?
- Why is State surveillance carried out?
- What information is sought when State surveillance is carried out?
- What are the constitutional and legislative provisions justifying State surveillance?
- What are the constitutional and legislative provisions providing checks, balances, and oversight with regards to State surveillance?
- What is the role of data protection authorities in State surveillance?
- How is State surveillance carried out?
- Is there access to effective remedies where State surveillance is concerned?

Surveillance Technologies Used in Southern Africa

By Kuda Hove

Introduction

The growing use of surveillance technologies in Southern African countries has become a pervasive force impacting the fundamental right to privacy. These technologies, embraced for diverse purposes spanning from law enforcement and national security to private and corporate interests, have sparked a complex interplay between the quest for security and the safeguarding of individual privacy. This research paper delves into the expanding influence of surveillance technologies in Southern Africa, the driving factors behind this trend, and the intricate implications they present for the cherished right to privacy, security, and civil liberties across the region.

Surveillance technologies have emerged as a compelling force altering the landscape of privacy in Southern Africa. The region comprises a diverse array of nations, each with its own distinctive historical, political, and socio-economic characteristics. In this dynamic setting, the growing use of surveillance technologies is profoundly affecting the balance between the need for enhanced security and the preservation of personal privacy. These technologies encompass a wide spectrum of tools, including closed-circuit television (CCTV) systems, mass telecommunications surveillance, facial recognition, biometric data collection, and social media monitoring or intelligence gathering.

The rise of surveillance technologies in Southern Africa is inextricably linked to a pressing desire to fortify public safety and security. In the face of escalating crime rates, governments and municipalities have turned to surveillance systems, particularly CCTV, to observe public spaces and discourage criminal activities.

However, as the influence of surveillance technologies expands throughout Southern Africa, it brings to the forefront a series of intricate ethical, legal, and human rights dilemmas, prominently among them, the right to privacy. The delicate equilibrium between security and individual privacy is increasingly at risk. Concerns surrounding potential government overreach, the potential for abuse of surveillance powers, and the violation of citizens' rights have been raised vociferously by civil society organisations,

privacy advocates, and the general public. Instances of unlawful surveillance, unauthorised data collection, and human rights violations have surfaced, engendering contentious debates and legal challenges.

The legal and regulatory framework governing surveillance technologies in Southern Africa varies from one country to another. While some nations have implemented comprehensive laws regulating surveillance practices, most countries in the region lack such regulations, leading to a fragmented landscape of standards. These disparities can result in uncertainty and the potential for misuse of these technologies, further exacerbating concerns about privacy violations.

This paper examines the surveillance landscape in five southern African countries namely, Angola, the Democratic Republic of Congo, Malawi, South Africa and Zimbabwe. Each country discussion is divided into the following categories, an overview of country level case studies which provides examples of surveillance technologies used in each country, a discussion of that country's laws and policies which relate to privacy and surveillance, followed by a discussion of the actors who have been identified or reported to be using surveillance, and then a discussion of the surveillance technologies and techniques reported to be in use in that focus country.

A section of this paper then follows with a focus on the challenges and concerns – this section builds on the themes and trends from the different country reviews and case studies. Finally, the paper will conclude with policy recommendations which each of the focus countries, as well as countries in the region can implement to ensure that state sponsored surveillance activities are conducted within the boundaries of universally accepted human rights principles.

Angola

Angola is a Lusophone country which gained its independence from Portugal in 1975. Soon after independence, the country was plunged into civil war which stretched intermittently from 1975 until 2002.[155] In the 48 years since 1975, Angola's ruling party has remained the People's Movement for the Liberation of Angola ('MPLA').

The MPLA led government has been accused of various human rights violations which include abductions, arbitrary detention and torture.[156] These violations have usually targeted government critics which have at times included journalists, civil society actors, members of opposition political parties and human rights activists or defenders. Criticism of the MPLA led government stems mainly from the government's corruption when it comes to the management of Angola's natural resources which include oil and diamond deposits.[157]

It is not surprising therefore, that surveillance activities in Angola can be traced back to the need to protect the Angolan diamond fields during the country's civil war. At that time, it was important for the MPLA to gain and maintain control of the diamond fields because the diamonds provided a source of income needed to finance the MPLA's war efforts against the opposing National Union for the Total Independence of Angola (UNITA).[158]

According to research,[159] Arkady Gaydamak, an Israeli businessman operating in Angola in the 1990s was instrumental in the establishment of an intelligence and surveillance system which led to the dispossession of diamond fields from UNITA control and eventually the capture and death of UNITA's leader Jonas Savimbi in 2002. Savimbi's death then paved the way for a ceasefire which marked the end of the civil war. Military intelligence service[160] established and trained with help from Israeli intelligence personnel coordinated by Arkady Gaydamak – this was primarily set up to conduct surveillance activities which stopped UNITA's ability to profiteer from the diamond trade.

Malware

There are also case studies of state sponsored surveillance activities in modern day Angola, these case studies are useful in highlighting the nature of surveillance technologies used by the Angolan government. In 2013, security researchers discovered that Rafael Marques' laptop had been compromised by malware which took several screenshots of Marques' activities and sending the

155 The Angolan Civil War (1975-2002): A Brief history | South African History Online. (n.d.). https://www.sahistory.org.za/article/angolan-civil-war-1975-2002-brief-history.

156 BBC NEWS | World | Africa | UN reports Angola "torture" abuse. (n.d.). http://news.bbc.co.uk/1/hi/world/africa/7018226.stm.

157 Overview of corruption and anti-corruption in Angola https://www.transparency.org/files/content/corruptionqas/257_Corruption_and_anti_corruption_in_Angola.pdf.

158 Verde, R. S. (2021). Angola at the crossroads: Between kleptocracy and development. https://openlibrary.org/books/OL29542537M/Angola_at_the_Crossroads

159 Verde, R. S. (2021b). Israeli involvement in electronic surveillance in Angola: a step towards transparency or the sophistication of illegal practices? https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/angola_report.pdf.

160 Digital surveillance in Angola and other "Less important" African countries. (2014, February 27). Global Voices Advox. https://advox.globalvoices.org/2014/02/26/digital-surveillance-in-angola-and-other-less-important-african-countries/.

screenshots to a to a server in India.[161] Marques is an investigative journalist who has written widely about money laundering and corruption in Angola's diamond trade. Several months after the discovery of the malware on his laptop, Marques was detained and tortured by suspected state security agents.[162]

Malware has also been used by private actors to surveill and target public infrastructure, for example in 2019, SONANGOL, the then parastatal responsible for the production of oil and gas in Angola was the target of a cyberattack which attempted to destroy its database.[163] This cyberattack was only partially successful and was able to delete some folders, shared, data, documents and applications on the parastatals local network.

Telecommunications Surveillance

The Mitterrand-Pasqua Affair or Angolagate is a political scandal that involved the sale of arms by France to Angola in the 1990s during the Angolan civil war despite a UN ban on arms trading with Angola.[164] This political scandal led to the arrest of a number of high profile French politicians. Related to this research, investigations into the Mitterrand-Pasqua Affair also uncovered the sale of undisclosed telecommunications surveillance equipment to Angola by a French company. The equipment was used by Angolan intelligence agencies to listen to GSM cell phones and track down the coordinates of satellite telephones. According to research from Africa Confidential,[165] this surveillance equipment had at one point sometime before 2001, allowed the MPLA to target Savimbi using the coordinates of his satellite phone.

In April 2013, a Club-K investigative report revealed that state security agencies were allegedly planning to implement an electronic monitoring system with capabilities to track among other things, email and other digital communications.[166] This equipment was reportedly imported from Germany, and it was set up at the Cabo Ledo base of the Technical and Operational Battalion (*Batalhão Técnico Operacional–BATOPE*).[167] This equipment was reportedly set up in late 2013, and in early 2014, researchers reported finding proof that at least one major ISP hosting a spyware system directly on its server, as part of the German company setup.[168] It has been reported that this system is capable of regional surveillance as well.[169]

Surveillance Actors in Angola

State Actors

161 Ibid.

162 Ibid.

163 De Morais, R. M. (n.d.). Ataque Cibernético à Sonangol. https://www.makaangola.org/2019/08/ataque-cibernetico-a-sonangol/

164 Welle, D. (2009, December 31). Corruption in France. *dw.com*. https://www.dw.com/en/how-angolagate-shook-french-political-foundations-to-the-core/a-5035505

165 Winners and losers in Angolagate. (2024, March 9). Copyright 2024 Africa Confidential. https://www.africa-confidential.com/article-preview/id/336/Winners_and_losers_in_Angolagate

166 Refworld - UNHCR's Global Law and Policy Database. (2024, February 11). *Freedom on the Net 2014 - Angola*. Refworld. https://www.refworld.org/docid/549025e70.html

167 Alemães montam sistema de escuta em Angola. (n.d.). http://www.club-k.net/index.php?option=com_content&view=article&id=14932:alemaes-montam-sistema-de-escuta-em-an-gola&catid=11:foco-do-dia&Itemid=130

168 See footnote 12

169 Verde, R. S. (2021b). Israeli involvement in electronic surveillance in Angola: a step towards transparency or the sophistication of illegal practices? https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/angola_report.pdf

Reports on the identity of surveillance actors in Angola have mainly pointed to state intelligence agencies such as the State Security and Intelligence Service (SINSE) and External Intelligence Service (SIE). Both entities have reportedly received training and support from the Israeli Police's Training Institute and Mossad or ex-Mossad officials. Furthermore, Israeli trained SINSE individuals, have been placed as provincial directors or as analysts or research experts in strategic government departments.

As recently as 2020, the Mitrelli Group provides Israeli security equipment to the Angolan intelligence services.[170] The Angolan military through its Technical and Operational Battalion (*Batalhão Técnico Operacional–BATOPE)* has also been identified as one of the state arms which utilise German sourced electronic communication surveillance technologies with mass surveillance capabilities.[171]

Private actors

Private intelligence agencies such as the Israeli firm, Black Cube, founded by former members of Mossad have been involved in surveillance activities in Angola. Black Cube's activities in Angola were revealed during Isabel dos Santos' court action against Angolan President João Lourenço.[172] She stated that the Israeli company was specifically chosen for its experience in uncovering conspiracies. According to dos Santos, the surveillance firm was able to gather many hours of audio and video recordings that prove a government sponsored conspiracy against her.

Other private actors in Angola include the Mobile Network Operators and Internet Service Providers due to their close proximity to high ranking and influential members of the ruling MPLA party. For example, the former top adviser to the head of the Intelligence Bureau at the Presidency, General Leopoldino do Nascimento, was at the same time, the chairman and shareholder of Unitel. The deputy CEO and Chief Technology Officer of Unitel, Amílcar Safeca, is the brother of Aristides Safeca, the former secretary of the state for ICT who at the same time was a shareholder of Movicel. Meanwhile, the head of the Intelligence Bureau, General Manuel Hélder Vieira Dias "Kopelipa," had a majority share (about 59 percent) in Movicel.[173]

This strong state presence in the ownership structure of Angola's telecommunications, particularly the mobile phone operators coupled with a weak rule of law, suggests that state is more than likely able to wield their influence over service providers when desired. As reported by Club-K in 2014, one unnamed Internet Service Provider was hosting spyware which matched the German sourced electronic monitoring system.[174]

Democratic Republic of Congo

170 Verde, R. S. (2021b). Israeli involvement in electronic surveillance in Angola: a step towards transparency or the sophistication of illegal practices? https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/angola_report.pdf

171 Refworld - UNHCR's Global Law and Policy Database. (2024, February 11). Freedom on the Net 2014 - Angola. Refworld. https://www.refworld.org/docid/549025e70.html

172 AfricaNews. (2021, March 31). Isabel dos Santos accuses Angolan govt of 'conspiracy to seize her assets' Africanews. https://www.africanews.com/2021/03/31/isabel-dos-santos-accuses-angolan-govt-of-conspiracy-to-seize-her-assets/

173 Refworld - UNHCR's Global Law and Policy Database. (2024, February 11). Freedom on the Net 2014 - Angola. Refworld. https://www.refworld.org/docid/549025e70.html.

174 Refworld - UNHCR's Global Law and Policy Database. (2024, February 11). Freedom on the Net 2014 - Angola. Refworld. https://www.refworld.org/docid/549025e70.html.

The Democratic Republic of Congo ('DRC') shares some similarities with Angola, for example, both countries have vast amounts of natural resources and both countries have experienced prolonged civil wars. One major difference though is that the DRC is a Francophone country that gained independence from Belgium in 1960. It would be another 59 years before the country witnessed a peaceful transfer of power which was marked by the inauguration of President Félix Tshisekedi in 2019. However, there are parts of the country where the national army is still engaged in fighting with various rebel groups.[175]

In post-independent DRC, there have been numerous reports of government critics being targeted and silenced through a variety of human rights violations. These violations have at times enabled by different types of digital surveillance techniques as discussed below.

Digital Surveillance

Prince Murhula, a Congolese journalist has written about the surveillance and proliferation of WhatsApp and social media groups and platforms as a way to control and censor information shared over those platforms.[176] It is reported that this practice was popularised by former President Joseph Kabila's regime between 2016 and 2018 when he sought ways to extend his rule. Seeing that he was failing to stifle online dissent, then then President Kabila's government turned to internet shutdowns as a way to silence its online critics at one point shutting down the internet for almost 21 days.[177]

CCTV

In early 2016, the government rolled out the use of Closed Circuit Television equipment in the capital city, Kinshasa. This CCTV equipment was introduced under the guise of promoting public safety, but privacy and civil rights experts argued that this was more of an attempt to monitor and quell any public demonstrations or dissent against the then national President.[178]

Telecommunications and mobile phone interception

Privacy and Freedom of Expression Transparency reports from Mobile Network Operators such as Orange offer a glimpse into the frequency of government requests for interception and access to customer records. Orange's 2020 transparency report reports that the Congolese processed 9 applications for interception of communications and made 1154 information requests.[179] These requests were from a range of state-controlled stakeholders, such as government agencies, judicial authorities, or the police, for a variety of data, including call details, customer identification data, geolocation, billing and payment data.

175 Al Jazeera. (2023, May 19). What is the latest conflict in the DR Congo about? Al Jazeera. https://www.aljazeera.com/features/2022/6/21/explainer-what-is-the-latest-conflict-in-the-drc.

176 Tungali, A. (2021). Surveillance of public spaces and communications in the Democratic Republic of the Congo. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_02_2021_surveillance_of_public_spaces_drc_masterset.pdf

177 See footnote 22

178 Tungali, A. (2021). Surveillance of public spaces and communications in the Democratic Republic of the Congo. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_02_2021_surveillance_of_public_spaces_drc_masterset.pdf

179 Orange. (2020). Orange Transparency Report on Freedom of Expression and Protecting Privacy 2020 data. https://ia902501.us.archive.org/8/items/orange-transparency-report-freedom-of-expression-and-protecting-privacy-2020/Orange%20transparency%20report%20freedom%20of%20expression%20and%20protecting%20privacy%202020.pdf

Social Media Surveillance

There has been growing demonstrations over the state of the country's economy, martial law and general living standards across the DRC.[180] Police have acted swiftly and sometimes lethally to quell such protests. Information about peaceful protests against government is sometimes shared over social media platforms and groups. There have been reports of social media surveillance which has led to the arrest of government critics, journalists and other civil society actors who are critical of the country's government.

In April 2022, Mwasimo Ndungo King an activist with the *Lutte pour le Changement* (Fight for Change – LUCHA) was arrested for comments he made on social media which were deemed to be critical of government.[181] The activist was later charged with contempt to the army, and public authorities under Article 87 of the Military Penal Code.

Surveillance Actors in the Democratic Republic of Congo

State Actors

Several state actors are involved in surveillance activities in the DRC. The first state actor is in the form of the National Police. Their involvement is mainly in surveillance for criminal investigation purposes. It has also been reported that the police have been involved in the protection of private mining interests.

Article 60 of the Telecommunications Act identifies the Minister of Internal Affairs, the Minister in charge of Territorial Defense and Security or the Chief Intelligence Officer as the instrumental actors in the granting of surveillance warrants or orders.

In addition to the national police, other state actors include the National Intelligence Agency (ANR) and the Military Detection of Anti-Patriotic Activities (DEMIAP). These two agencies conduct surveillance activities in relation to maintaining state security and other national intelligence-gathering interests. DEMIAP, is the military intelligence section of the Armed Forces of the Democratic Republic of the Congo (FARDC).[182]

On the other hand, the Superior Council for Audiovisual Communication (CSAC) is there to monitor the activities of media practitioners in the country.

Malawi

Malawi gained its independence from British rule in 1964. In the early years of post-independence Malawi, the country's first President Hastings Banda declared the country a one party state. President Banda and his ruling party would remain in power until 1994. After 1994, the country has held elections every 5 years but a conflation between the ruling party and government means that the ruling party has often used government structures and resources to maintain its grip on power.

180 DR Congo: Peaceful protests violently repressed. (2023, May 30). Human Rights Watch. https://www.hrw.org/news/2023/05/29/dr-congo-peaceful-protests-violently-repressed

181 Frontline Defenders. (2022, April 6). Democratic Republic of Congo: human rights defender and LUCHA member Mwamisyo Ndungo King charged. https://www.frontlinedefenders.org/sites/default/files/ua_drc_mwamisyo_ndungo_king_06042022_eng_final1.pdf.

182 Tungali, A. (2021). Surveillance of public spaces and communications in the Democratic Republic of the Congo. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_02_2021_surveillance_of_public_spaces_drc_masterset.pdf.

Telecommunications surveillance

Telecommunications surveillance is one of the most commonly reported forms of surveillance in Malawi. Between 2009 and 2011, the Malawi Communications Regulatory Authority (MACRA) spearheaded the acquisition and rollout of the Consolidated ICT Regulatory Management System (CIRMS).[183] The CIRMS was acquired at an initial cost of $22,9 million and an additional $13 million for software upgrades over the course of 10 years.[184]

According to MACRA, the CIRMS was implemented to help the authority monitor the overall quality of services delivered by Mobile Network Operators operating in Malawi. Additionally, it would be useful in the helping the regulator verify telecommunication companies' revenue and tax levels. However, CIRMS has a number of capabilities which include the ability to record and capture telecommunications in real time.[185] CIRMS has been dubbed the 'spy machine' by privacy activists and civil society actors.[186]

The privacy concerns over the implementation of CIRMS were so serious that Kennedy Makwangwala, a Malawian citizen filed a court case seeking an injunction to stop the implementation of CIRMS. Additionally, four Mobile Network Operators that operate in Malawi also criticised the planned implementation of CIRMS. One of the MNOs' criticisms was that the government claimed that once in place, CIRMS would be used for the 'lawful interception' of communications even though Malawi did not have any law which provided for the legal interception of communications.[187] These court challenges continued between 2012 and 2017 when the system was finally implemented.[188]

Telecommunications surveillance which includes social media monitoring has led to the arrest of several government critics. Recent reports have revealed the suspected use of telecommunications surveillance led to the arrest of investigative journalist Gregory Gondwe for his journalistic work.[189] In a similar case, citizens such as Chidawawa Mainje have been arrested for criticising the country's President over WhatsApp messages.[190]

In 2019, the Malawian Minister of Information and Telecommunications Technology announced the government's plans to monitor and trace individuals who 'abuse' social media. At the time, the country

183 Gondwe, G., Gondwe, G., & Gondwe, G. (2020b, July 24). Hiding behind laws to accomplish digital surveillance | The Nation Online. The Nation Online. https://mwnation.com/hiding-behind-laws-to-accomplish-digital-surveillance/.

184 Malawi Voice. (2023, June 14). Request for MACRA Board to probe the purchase of Consolidated ICT Regulatory Management System (CIRMS) machine. Malawi Voice. https://www.malawivoice.com/2023/06/14/request-for-macra-board-to-probe-the-purchase-of-consolidated-ict-regulatory-management-system-cirms-machine/.

185 Chitsulo, L. (2020, July 27). Macra speaks on Cirms | The Nation Online. The Nation Online. https://mwnation.com/macra-speaks-on-cirms/.

186 Contributor. (2023, September 4). Malawi telecom operators fight regulator on CIRMS. https://communicationsafrica.com/security/malawi-telecom-operators-fight-regulator-on-cirms.

187 Contributor. (2023, September 4). Malawi telecom operators fight regulator on CIRMS. https://communicationsafrica.com/security/malawi-telecom-operators-fight-regulator-on-cirms.

188 Chitsulo, L. (2020, July 27). Macra speaks on Cirms | The Nation Online. The Nation Online. https://mwnation.com/macra-speaks-on-cirms.

189 'Hacking of Platform for Investigative Journalism website not a mere coincidence.' (2022, April 15). MISA Malawi. https://malawi.misa.org/2022/04/15/hacking-of-platform-for-investigative-journalism-website-not-a-mere-coincidence/.

190 Masina, L. (2022, May 2). Malawi Police arrest nurse for harassing president online. Voice of America. https://www.voanews.com/a/malawi-police-arrest-nurse-for-harassing-president-online-/6554047.html.

did not have any laws which define or describe what actions amount to 'abuse' of social media.[191] According to the Minister of ICT, there were some Malawian who were abusing social media. The Minister also indicated that this move was one of the government's ways of regulating the use of social media platforms.

Surveillance Actors

Surveillance in Malawi is reported to be mainly driven by state actors, primarily the Minister of Information and Communications Technology. This ministry has mainly been in the lead of telecommunications surveillance activities in the country. In addition to the Ministry of ICT, the Malawian Police is also responsible for surveillance as it relates to the investigation of alleged criminal offences. There is no publicly available information on whether the police shares information with other state actors, but this is suspected to be the case, especially when the investigations involve government critics and other persons of interest to the ruling party.

The National Intelligence Service, formerly known as the National Intelligence Bureau, is the country's intelligence gathering agency in matters which relate to national security and national interests.[192] The National Intelligence Bureau as it was known then, operated for a period of at least 15 years without any legal provision until 2018 when the National Intelligence Service Act was gazetted.[193] This law only became operational in February 2021.[194]

The fact that the country operated a national institution which primarily conducted surveillance activities without any enabling legislation shows just how little regard, the Malawian government has had for regulating or regularising state surveillance activities. This is also underscored by the fact that it took another 4 years for the government to fully operationalise the National Intelligence Service Act.

The Malawian Army has been reportedly involved in intelligence gathering activities. In November 2023, the Army was part of the institutions gathering intelligence for the purpose of slowing down the currency trading on the parallel market. This was after the national currency; the Kwacha lost an estimated 44% of its value against the US$.[195] It is highly likely that the army is also involved in the gathering of intelligence in areas of national interest.

South Africa

South Africa is one of the most economically developed countries in Southern Africa and one with some of the highest criminal rates in the region.[196] As a result, the country has invested heavily into technologies with surveillance capabilities primarily for the purpose of fighting crime.

---

191 Nyasa Times Reporter (2019, January 20). Malawi govt to trace individuals who abuse social media - Malawi Nyasa Times - News from Malawi about Malawi. Malawi Nyasa Times - News From Malawi About Malawi. https://www.nyasatimes.com/malawi-govt-to-trace-and-truck-down-individuals-who-abuse-social-media/.

192 Chimjeka, R. (2015, March 21). *Malawi moves to legitimise intelligence bureau | The Nation Online*. The Nation Online. https://mwnation.com/malawi-moves-to-legitimise-intelligence-bureau/.

193 *National Intelligence Service Act, 2017*. (2018, November 2). https://malawilii.org/akn/mw/act/2018/30/eng@2018-11-02.

194 Nyasa Times Reporter (2023, June 22). *Chakwera officially inaugurates first ever National Intelligence Service Complaints Tribunal - Malawi Nyasa Times - News from Malawi about Malawi*. Malawi Nyasa Times - News From Malawi About Malawi. https://www.nyasatimes.com/chakwera-officially-inaugurates-first-ever-national-intelligence-service-complaints-tribunal/.

195 Mpofu, T (2023, November 15) *Malawi deploying army, intelligence operatives to enforce currency trading rule after 44% devaluation*. https://www.intellinews.com/malawi-deploying-army-intelligence-operatives-to-enforce-currency-trading-rule-after-44-devaluation-301358/

196 Okafor, C. (2023, September 28). Top 10 African countries with the highest crime rates. *Business Insider Africa*. https://africa.businessinsider.com/local/lifestyle/top-10-african-countries-with-the-highest-crime-rates/htgcw5f?op=1

CCTV

In the mid-1990s South Africa began introducing Closed Circuit Television (CCTV) infrastructure in major cities to combat crime. This adoption was mainly driven by Business Against Crime of South Africa (BACSA).[197] Over the years, city authorities have taken a more central role in introducing, managing and upgrading CCTV systems. This has led to different levels of CCTV network densities across the different cities. In some instances, some of the city authorities control their own CCTV network as well as CCTV networks owned and operated by private actors.[198]

Some of the challenges reported by city authorities and the police include vandalism, frequent power outages, and damage to fibre cables by construction companies. As a result of these challenges, the City of Johannesburg reported that only an estimated 50% of its CCTV cameras were still operational.[199]

In recent years, private actors have become more involved in the implementation of CCTV networks. Vumacam is one such private actor, in 2014, the company joined forces with Fibrehoods to introduce what they called the fibre-to-the-home project. This project was aimed at 42 suburbs in Johannesburg and Cape Town. It would see the extension of optical fibre internet mainly to use as a backbone network for CCTV technology in those suburbs.[200]

Vumacam's CCTV needed this high speed internet network because their CCTV technologies reportedly had video analytics capabilities which were not only used to prevent crime but to also identity vagrants so they could be weeded out of the affluent suburbs.[201] Vumacam's CCTV footage feeds into private security companies.

Vumacam's CCTV cameras reportedly make use of iSentry, a software developed for the Australian military to detect unusual behaviour. This software issues alarms when it determines something is "abnormal"—like loitering pedestrians and prioritises video streams for review by human operators in a control room.[202]

Drones

In July 2023, the South African Police Service announced that the force had started rolling out drones in the investigation of crime and for the targeted tracing of individuals wanted for serious crimes like murder and rape.[203] A South African government spokesperson revealed that the government had set aside an estimated US$105 million for the purchase of drones and police vehicles.[204] The use of drones

197 SaferSpaces (n.d.). *Closed circuit television (CCTV) and crime prevention*. https://www.saferspaces.org.za/understand/entry/closed-circuit-television-cctv-and-crime-prevention

198 Ibid.

199 Ibid.

200 Staff Writer. (2014, September 15). New fibre-to-the-home suburbs announced. *Business Tech*. https://businesstech.co.za/news/internet/68486/new-fibre-to-the-home-suburbs-announced/.

201 Kwet, M. (2019, November 22). Smart CCTV networks are driving an AI-Powered apartheid in South Africa. *Vice*. https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa.

202 Ibid.

203 Magcaba, B. (2023, July 16). SAPS introduces drones for enhanced police visibility and suspects tracking - SABC News - Breaking news,. *SABC News - Breaking news, special reports, world, business, sport coverage of all South African current events. Africa\'s news leader.* https://www.sabcnews.com/sabcnews/saps-introduces-drones-for-enhanced-police-visibility-and-suspects-tracking/.

204 Mkhwananzi, S. (2023, June 8). *SAPS to set aside R2 billion to buy drones, vehicles to crackdown on crime*. IOL. https://www.iol.co.za/news/politics/saps-to-set-aside-r2-billion-to-buy-drones-vehicles-to-crackdown-on-crime-ad75aa1b-529d-4b66-a965-4ce37696d88e.

has also been proposed for border security and monitoring purposes.[205] The drones proposed for use in border patrols are reportedly being developed in association with the South African Airforce.[206]

Bulk or Mass Surveillance

South Africa has a well-established telecommunications infrastructure which makes it possible to conduct telecommunications surveillance on a massive scale. For example, the South African National Communications Centre conducted bulk interception in terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).[207] The South African government justified this by stating that mass surveillance was used for counterterrorism and law enforcement purposes. The Amabhungane case in South Africa revolved around a legal challenge to the RICA. Amabhungane, an investigative journalism organisation, along with its partners, challenged the constitutionality of RICA, claiming it allowed for overly broad surveillance and lacked adequate safeguards to protect individuals' privacy.

The case sought to highlight concerns that RICA was used to enable mass surveillance and potentially violate the right to privacy. The plaintiffs argued that the law allowed for warrantless interception of communications and did not require sufficient oversight or checks and balances to prevent abuses.

In July 2019, the High Court of South Africa ruled in favour of Amabhungane, declaring certain sections of RICA unconstitutional. The court found that the law lacked the necessary safeguards to protect against unlawful surveillance and ordered that the law be amended within two years to address these deficiencies.

This case represents a significant legal challenge to surveillance laws in South Africa, with potential implications for privacy rights and surveillance practices in the country. The ruling underscores the importance of balancing national security needs with the protection of individual privacy and civil liberties, and it highlights the role of legal challenges and civil society organisations in addressing these concerns.

Actors of surveillance

Surveillance actors in South Africa are a mixture of state security actors as well as private actors. Laws such as RICA are enforced by public agencies like the State Security Agency which is responsible for national security.

The South African Defence Forces which are comprised of the Army and the Airforce are also involved in the strategic development and use of surveillance technologies. In addition to these state actors, the South African Police Service are also involved in the surveillance of individuals and entities suspected to be involved in criminal activities.

205 Fraser, L. (2023, February 5). South Africa's big push to use drones for security and border control. *South Africa's Big Push to Use Drones for Security and Border Control*. https://businesstech.co.za/news/technology/662267/south-africas-big-push-to-use-drones-for-security-and-border-control/.

206 Fraser, L. (2023, February 5). South Africa's big push to use drones for security and border control. *South Africa's Big Push to Use Drones for Security and Border Control*. https://businesstech.co.za/news/technology/662267/south-africas-big-push-to-use-drones-for-security-and-border-control/.

207 *Bulk surveillance is unlawful, says the High Court of South Africa*. (n.d.). Privacy International. https://privacyinternational.org/news-analysis/3212/bulk-surveillance-unlawful-says-high-court-south-africa.

Other government agencies such as the South African Revenue Service (SARS) have used social media monitoring to collect intelligence on suspected tax dodgers and defaulters. Foreign communications surveillance has been carried out by the National Communications Centre (NCC) of the country's civilian intelligence agency, the State Security Agency (SSA). It was temporarily halted by the country's apex court after the court found that there was no specific legal authority for the NCC to carry out foreign surveillance.

Private actors that are involved in surveillance activities in South Africa include private security firms who control and operate CCTV networks, they also are involved in the surveillance of private institutions such as banks.

Zimbabwe

Targeted physical surveillance

Physical surveillance relies on a variety of technologies and tools to monitor individuals, locations, and activities. These technologies are commonly employed by law enforcement agencies, intelligence organisations, private investigators, and security personnel for various purposes, including criminal investigations, security, and monitoring.

The awareness of being monitored can lead individuals to self-censor their actions, expressions, or online activities, fearing repercussions or surveillance-related consequences. This self-censorship can deter people from freely expressing their opinions, especially on sensitive or politically charged topics, out of fear of being identified, targeted, or penalised by authorities. Additionally in Zimbabwe, targeted physical surveillance is used to hinder political activism, protests, or dissenting movements by intimidating individuals or groups engaged in such activities. Research shows that the fear of surveillance discourages people from participating in activities critical of the government or those advocating for change.

Telecommunications Surveillance

In 2014, it was reported that Iran gifted Zimbabwe with a range of communications surveillance tools which included unspecified spy-phone software, IMSI catchers, and other programs to monitor personal computers.[208] IMSI catchers work by simulating cell phone towers or cell phone base stations for the purpose of harvesting information from cell phone devices within the IMSI catcher's range. IMSI catchers are usually used for communication interception, denial of service and service downgrading, and location tracking. The government has disclosed that it uses location tracking technologies to investigate crime. In 2020, the government used opposition political Member of Parliament Joana Mamombe's alleged location data to dispute her claims that she was abducted and tortured by state security agents.

This case also confirmed the use of interception or triangulation data. The trio were arrested on 13 May 2020, but never appeared in court, as police recanted their arrest. The trio were found in the early

208 Gwagwa, A. E., & Hove, K. (2016). Use of IMSI catchers in Zimbabwe's domestic law enforcement. *Strathmore*. https://www.academia.edu/30051415/Use_of_IMSI_Catchers_in_Zimbabwes_Domestic_Law_Enforcement.

hours of 15 May 2020 narrating a torrid ordeal under the hands of their captors. The state disputed this. The trio was subsequently arrested for lying about their torture and charged with communicating or publishing false statement prejudicial to the state and defeating or obstructing the course of justice.[209]

The state in contesting this abduction narrative produced a graphical presentation enabled by cell phone triangulation. The "travel flow chart" was published in the Sunday Mail, a state-controlled paper.[210] The President[211] and Home Affairs Minister subsequently issued statements confirming the use of this surveillance technology.[212]

As part of efforts to disprove the abduction narratives and medical reasons raised during the continuation of the case, video footage of Joana Mamombe in a supermarket were disclosed. The footage was posted on social media handles of ZANU PF officials, and journalists.[213] The single state-controlled television station (ZBC TV) aired a 15-minute video disputing the abduction story, with footage from cameras from different public outlets showing the trio's movements.[214]

Earlier in March 2020, Joanna Mamombe had been arrested on allegations of subverting a constitutionally elected government after calling the government "authoritarian". These remarks were posted on Facebook between January 14-16 according to the state.[215] Clearly, the opposition MP was under surveillance.

Social Media Surveillance

The government of Zimbabwe announced in 2021 that it had set up a team to monitor social media posts in the country.[216] This followed other announcements like in March 2020, when an army official, announced the army would start snooping into private communications between citizens to "guard against subversion", claiming that the use of social media posed a threat to national security.[217] In September 2020, the ruling, Zanu PF, also highlighted that it would be deploying activists on social media to counter online narratives that are not favourable to it. In October 2020, President Emmerson Mnangagwa addressed Zanu PF members at the party's headquarters in Harare, where he said through the use of ICTs, the government had the capacity and had been able to track the locations of certain individuals and their communication details.[218]

209 Amnesty International. (2023, June 13). Zimbabwe: Further information: Opposition activists rearrested; one charged - Amnesty International. https://www.amnesty.org/en/documents/afr46/2906/2020/en/.

210 Mail, S. (2020, June 7). Mamombe abduction: Car owner speaks out. The Sunday Mail. https://www.sundaymail.co.zw/mamombe-abduction-car-owner-speaks-out.

211 The President was speaking at public event. Video clip on file with researchers

212 https://twitter.com/ZiFMStereo/status/1268467649123622912.

213 https://twitter.com/rangamataire/status/1306602703922098176.

214 ZBC News. (2020, September 9). Alleged abduction of MDC Alliance trio: Unravelling "an almost perfect hatchet job". [Video]. YouTube. https://www.youtube.com/watch?v=REw_x2L-mmQ.

215 Radio Nehanda. (2019, March 10). 'Subversion charge used to cripple opposition' Nehanda Radio. https://nehandaradio.com/2019/03/10/subversion-charge-used-to-cripple-opposition/.

216 The Newsday. (2021, November 4). Govt sets up team to monitor social media. NewsDay. https://www.newsday.co.zw/2021/11/govt-sets-up-team-to-monitor-social-media.

217 The NewsDay. (2020, March 3). Army to monitor social media. NewsDay. https://www.newsday.co.zw/2020/03/army-to-monitor-social-media?cn-reloaded=1

218 SlyMediaTv. (2020, October 12). Pres Mnangagwa "#July31 now a Movement it's a project of our detractors funded from outside." [Video]. YouTube. https://www.youtube.com/watch?v=Pn_Q_JpdYbE.

CCTV Surveillance

CCTV cameras are used security purposes in places such as banks, border control points and also in and around government infrastructure. Some of these CCTV cameras are reported to have facial recognition capabilities.[219]

Surveillance Actors

In Zimbabwe, state-sponsored surveillance is led mainly by military institutions. The Military Intelligence Department (MID) has assumed an increasing role in civilian affairs following the coup of November 2017. Significant militarisation of public institutions continues threatening to dilute civilian affairs and institutions.

Other actors are the Police Internal Security and Investigations (PISI), another intelligence gathering branch, and the Zimbabwe Intelligence Agency which is reported to work closely with the Central Intelligence Organisation (CIO).

Regulatory Framework for Privacy Laws

Surveillance laws are necessary to set out the limits within which the state may exercise surveillance. Ideally, these laws must embody internationally accepted fundamental rights and constitutional principles. This section focuses on the various laws that affect and regulate surveillance in some southern African countries.

Privacy, a Constitutional Right

All five countries covered in this research have Constitutions in place which all respectively recognise the right to privacy.

Article 32(1) of Angola's Constitution of 2010 states that every person has the right to privacy in their "personal and family life". Article 31 of the Democratic Republic of Congo's Constitution of 2006 as amended by the Law 11/2002 of 20 of January 2011, protects every person's right to a private life and the privacy of their communications. The section states that the right to privacy may only be violated in terms of specific laws.

In Malawi, the right to privacy is enshrined in Article 21 of the 1994 Constitution. The protection is extensive and protects a person's right to privacy of their home, the privacy of their communications and protection from seizure of their property. The 2013, Zimbabwean Constitution protects the right to privacy in Section 57. The Constitution states that the right to privacy covers the right not to have one's property seized or searched, the right to private communications and also the right to protection from having one's health condition disclosed.
It is worth noting that each of these countries have supreme Constitutions. What this means is that the Constitution is superior to any laws, policies or practices in that country. Therefore, any laws or

219 Burt, C. (2018, June 14). Zimbabwe to use Hikvision facial recognition technology for border control. Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/201806/zimbabwe-to-use-hikvision-facial-recognition-technology-for-border-control.

government actions including those relating to surveillance should be in line with the constitutional provision, in this case, the constitutional rights to privacy. However, the practice in each of the five countries is that there are some laws that still contradict the letter and spirit of the national Constitution, particularly the right to privacy.

National Data Protection laws

Angola has a national data protection law in the form of Law No. 22/11 on the Protection of Personal Data. The national Data Protection Authority was established in terms of Decree No. 214/16. In the Democratic Republic of Congo, data protection is regulated in terms of the law on telecommunications, information and communication technology N° 20/017 of 25 November 2020. The DRC also has a Bill from December 2022 to ratify the Malabo Convention.[220]

Malawi currently does not currently have a data protection law in place. The country has, however, recently gazetted a Data Protection Bill.[221] The Bill was gazetted on 7 December 2023 and is now set to be deliberated in the country's parliament. In South Africa, the national data law is the Protection of Personal Information Act, 2013 (POPIA). Zimbabwe's data protection law is the Cyber and Data Protection Act, 2021.

The national data protection laws in Angola, South Africa and Zimbabwe have been influenced by the EU's General Data Protection Regulations (GDPR). This is the sense that, the laws define main data protection concepts such as the data subject, the main principles of data protection and provide for sanctions when those data protection principles are violated.

In a similar way to the constitutional provisions set out in the previous section, the data protection laws if properly implemented would reduce the instances of unjustified surveillance in the five countries covered in this report. But data protection laws are disregarded leading to rampant, uncurbed surveillance.

Interception of Communications Laws

Interception of communication laws plays a crucial role in ensuring national security and law enforcement, but their operation carries inherent risks. To mitigate these risks, it is essential that such laws are well-crafted, subject to strict oversight, and adhere to principles of proportionality and necessity. The responsible application of these laws is essential to safeguard individual privacy, protect civil liberties, and maintain the balance between security and freedom in a democratic society.

Angola's Law no. 11/20, on Mobile Identification or Location and Electronic Surveillance is used to conduct communications surveillance mainly through the interception of communications. In DRC the interception of communications is achieved through the use of Sections 52, 54, 59 and 60 of the country's Telecommunications Act which sets out the conditions under which the interception of communications may be undertaken. Although, the Telecommunications Act provides sets out the procedure to apply for interception of surveillance warrants, there is little oversight to ensure that no interception is conducted without such warrants or to provide recourse to private individuals who

220 Laws of the World. (n.d.). Law in Democratic Republic of Congo - DLA PIPER Global Data Protection. https://www.dlapiperdataprotection.com/index.html?t=law&c=CD.

221 DataGuidance (2023, December 8). Malawi: Parliament introduces bill on data protection. https://www.dataguidance.com/news/malawi-parliament-introduces-bill-data-protection.

later discover that they have been the targets of unwarranted surveillance activities.

In Malawi, interception of communications is conducted in terms of the Electronic Transactions and Cyber Security Act, No. 33 of 2016, coupled with the Communications Act, No. 34 of 2016. In South Africa, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) is the legal framework that governs telecommunications surveillance in the country. RICA requires individuals and organisations to register their SIM cards and provides a legal framework for the monitoring and interception of communications for specific purposes, such as national security and law enforcement.

RICA requires telecommunication service providers to register subscriber information and retain customer data for a certain period. As has been discussed above, this law was found to be unconstitutional in parts and the government was tasked with revising the law in a way which would bring it within the provisions of the right to privacy as enshrined in the South African Constitution and also the Protection of Personal Information Act.

In Zimbabwe, the interception of communications in conducted in terms of the Interception of Communications Act. Under this law, the various telecommunication service providers operating in Zimbabwe, must use their own resources to acquire and install the required technical and functional features of the facilities and devices to that enable the interception of communications in terms of the ICA. The nature of these interception technologies is not specified.

Mandatory SIM Card Registration Laws

All 14 Southern African Development Community member countries have mandatory SIM card registration laws which require that telecommunications service providers must get a subscriber's personal information at the time the subscriber is signing up for the relevant intermediary's service. This personal information must include the person's full name, residential address, business address and postal address and his or her national identity number.

As a result, mobile network users must provide some form of biometric national identity document when registering for a prepaid mobile service plan or mobile money service account. Acceptable forms of ID are usually a driving licence (if it shows the person's national unique identity number), a national identity card, or a valid passport.

At a global level, several privacy and freedom of expression advocates have published literature on the ways that mandatory SIM card registration laws restrict the enjoyment of the right to privacy and create a chilling effect on free speech.[222] This is because mandatory SIM card registration laws allow states "...to know the identity of the owner of a SIM card, and thus who is most likely making a call or sending a message."[223] However, none of the telecommunications companies that are part of this research has publicly pushed back against the mandatory SIM card registration or suggested other less intrusive methods to confirm service users' identities.

If telecommunications companies assessed the effect of national laws on the right to privacy and

222 Privacy International (n.d.). 101: SIM card registration. https://privacyinternational.org/explainer/2654/101-sim-card-registration

223 Ibid.

freedom of expression, they would find that mandatory SIM card registration laws unjustifiably restrict the exercise of the right to privacy and the enjoyment of freedom of speech. By continuing to enforce SIM card registration requirements, telecommunications companies potentially expand each respective country's government's surveillance apparatus. The same is also true for other licensing requirements, which for example, require that telecommunications service providers install hardware and or software that permits the real time interception of communications sent over their network infrastructure.[224]

Challenges and Concerns

Proliferation of Technologies that May be Repurposed for Surveillance

There are a number of technologies which are currently being adopted in Angola, DRC, Malawi, South Africa and Zimbabwe which may easily be repurposed for surveillance purposes. Examples of such technologies include national data centres which are used to store biometric data processed during the civil registration process. Civil registration databases contain information which may be used to investigate crimes or keep track of persons of interest. Mission creep or the repurposing of these databases is easily done when there are no legal and policy safeguards which outlaw of using civil registry records for other purposes outside the scope for which the data was collected.

Smart city initiatives often rely on the deployment of technologies which may be repurposed for mass surveillance uses. A smart city is a city that employs advanced digital technologies and data-driven strategies to address urban challenges effectively. These technologies are utilised to optimise city operations, improve services, and enhance the overall quality of life for residents. Several countries in the southern African region have launched or announced plans to launch smart city initiatives within their borders, some examples are discussed below.

In pursuit of smart cities vision, most cities are installing cameras, arguably for safety and security. Abuse of these installations is inevitable. The absence of frameworks legislative frameworks that protect privacy means that video footage can be used for other purposes. Private technology companies that manufacture and distribute surveillance equipment have considerable interests in southern African countries and operate carte blanche.[225]

Apart from self-preservation interests, the benefits of surveillance enabling technologies such as smart cities are 'The benefits of the Safe City project are hard to verify and appear exaggerated.'[226]

Lack of Public Information on Government Spending on Surveillance

It is difficult to determine the actual amount of govt expenditure on surveillance because of a culture which is against access to information and because spending on surveillance is often done under secretive state defence expenditure or national security expenditure. The inability to determine spending means it is difficult to know how widespread these technologies and activities are. This is worsened by the fact that researchers in the region do not always have the tools to confirm the use of

224 For example, as required by Zimbabwe's Interception of Communications Act, read together with the country's Postal and Telecommunications Act.

225 Hikvision has been supporting Zimbabwe government with building of facial recognition capacities. Huawei was reportedly involved in the building of the cyber security centre at the National Defence University.

226 Jili, B. (2023, May 8). Surveillance tech in Africa stirs security concerns – Africa Center. Africa Center for Strategic Studies. https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/.

surveillance technologies such as malware which targets mobile phones or other means of electronic communications.

The combined lack of publicly available information on government spending on surveillance tech and lack of research tools to pick out tech used leaves room for governments to give embellished versions of how much they surveillance they actually conduct – giving the impression that the government is all seeing cowers a lot more people into self-censorship and goes to reduce their participation in democratic processes.

Lack of Political Will to Regulate Surveillance

Governments have no political will to implement laws which they believe will limit the scope of their surveillance activities. Only government can pass laws, but these laws would effectively limit government's own power to conduct surveillance. However, most southern African countries still have laws which are limited in scope and are sometimes found to be unconstitutional when tested in a court of law. Additionally, most laws apply only to the surveillance of electronic communications, which are only one type of surveillance. On the other hand, no laws or publicly available policies regulate other types of surveillance, for example, where a state security agent physically follows around or observes a targeted individual.

This lack of political will is also reflected in the slow adoption of continental and global instruments which promote and protect the right to privacy and data protection principles e.g., the Malabo Convention.

Lack of Independent Courts and Democratic Institutions

Poor human rights institutions and courts which are partisan, that do not interpret the Constitution or human rights in a way which curbs surveillance technologies. The lack of independence makes it easier for function creep and mission creep to take place. Institutions which collect data as part of the civil registry end up sharing biometric information with law enforcement and state security agencies.

The global surveillance technologies export market led by US, European and Asian suppliers. For example, much of the material that Angola has acquired from Israel came from large sales of equipment considered "surplus" by the Israeli Ministry of Defence.

The legal framework on surveillance is considerably weak and allows the state to conduct pervasive offline and online surveillance. Individuals are left to their own initiatives to deter, detect, and reduce the risk of surveillance. Widespread or dragnet online surveillance might be unsustainable for the state to bear; hence, it leans heavily on social media intelligence gathering, infiltration, and informants, and compelling service providers, private and public to comply with their surveillance or information requests.

Recommendations

There is a need for legal and policy frameworks that increase transparency in surveillance activities and build state accountability in the way it conducts its surveillance activities. These policies and legal provisions must be consistent with human rights practices, in compliance with international and regional standards. The alignment of national laws requires southern African countries to sign on to regional and continental instruments, such as the African Union's Convention on Cyber Security and Data Protection.

Most southern African governments have limited transparency in respect of large state contracts or loans, despite provisions in their national laws. There is need for more transparency around the procurement of technologies to carry out state-sponsored surveillance, as well as technologies which have the potential to be repurposed for surveillance. This contracting transparency must also cover infrastructure development that creates room for abuse of genuine projects to advance surveillance.

Legal limitations to be applied to surveillance activities to ensure surveillance is conducted only when it is lawful, necessary and proportionate. The internet and technology boom has seen many laws being enacted, which together with existing surveillance laws need to be evaluated against human rights principles and standards. Existing surveillance institutions and agencies in most southern African countries have limited accountability, parliamentary or judicial oversight. Reports by any surveillance, capable or empowered, agencies must be presented in Parliament.

The introduction of oversight and accountability measures to specify privacy impact assessments before the adoption and rollout of any technology deployed on a massive scale. Privacy impact assessments must be mandatory for all public agencies, in particular telecommunications agencies, national registration authorities, mobile and telecommunications operators, and access and internet service providers (ASP/ISPs), which reports be publicly available.

Digital rights advocates to be supported to document accurately and investigate any acts of state-sponsored surveillance technologies, along with the nature of the surveillance and its potential harms. Stronger regulation is required to strengthen international and regional mechanisms to hold countries accountable, mainly those manufacturing surveillance capable technologies. All countries that provide and sell surveillance tools which are being used to infringe citizens' fundamental rights, must be held accountable.

State of Deployment of Surveillance Technologies in West Africa

By Ridwan Oloyede

Introduction

Surveillance is characterised by systematically monitoring individuals' activities and information with or without the use of technology, often serving dual roles.[227] On the one hand, it is a mechanism for bolstering national security and preventing and detecting crimes. Still, on the other hand, it can become an avenue for infringing privacy and other human rights. In the West African context, the governments are increasing their spending on surveillance due to increased insecurity. The use has also sometimes resulted in unwarranted consequences, from abuse and misuse, unlawful arrests to the suppression of free speech and even instances of harassment.[228] It has also been perceived as a tool for promoting digital repression and stifling free speech.[229] There are documented incidents of different manifestations of government surveillance, leading to a fear of deprivation of rights, contrary to what a democratic society should represent.

The legal landscape also presents a myriad of challenges. Twelve of the Economic Community of West African States (ECOWAS) member states have enacted data protection laws.[230] However, of these twelve, only ten have established a data protection authority,[231] while two have a law but have yet

227 Lyon, D. (2022). Surveillance. Internet Policy Review, 11(4). Retrieved October 20, 2023, from https://policyreview.info/concepts/surveillance.

228 Adebajo, A. K., 'Kunle. (2023, February 24). How digital surveillance threatens press freedom in west africa. HumAngle. Retrieved October 20, 2023 from https://humanglemedia.com/how-digital-surveillance-threatens-press-freedom-in-west-africa/.

229 ibid.

230 Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, Ghana, Guinea, Mali, Mauritania, Niger, Nigeria, Senegal, and Togo.

231 Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, Ghana, Mali, Mauritania, Niger, Nigeria, and Senegal..

to establish an authority.[232] The remaining four have yet to enact a law or establish an authority.[233] Also, there is a growing trend of enacting laws that enable surveillance and grant sweeping powers to authorities without proper oversight. For example, in 2020, Niger enacted a law to expand the power of law enforcement to conduct sweeping surveillance under the garb of national security.[234] In addition, some of the laws in these countries that enable surveillance lack the essential safeguards synonymous with global best practices.

Further complicating the landscape are obligations imposed on intermediaries like telecommunication providers, such as weakening encryption, extended data retention, real-time monitoring obligations, and more. These sometimes-overreaching obligations can inadvertently broaden surveillance powers beyond their necessary confines.

This report examines the deployment of surveillance technologies in West Africa, focusing on Ghana, Nigeria, and Senegal and the existing regulatory framework for privacy and surveillance. While the report primarily revolves around these countries, references from other countries in the sub-region are added to demonstrate the extent of deployment and offer a broader view of West African surveillance practices. The report employed case studies to highlight how these tools are deployed, from genuine crime prevention to overreaching use capable of curtailing civil liberties. The report concludes with recommendations to different stakeholders on improving the surveillance landscape in the sub-region with safeguards and human rights considerations.

Understanding the Motivations and the Deployment of Surveillance Technologies in West Africa

In the wake of increasing security concerns, ranging from terrorism to urban crime in the sub-region, the last two decades have seen a growing inclination towards the procurement and deployment of surveillance technologies.[235] The adoption of surveillance technologies in West Africa can be attributed to various socio-political, economic, and technological factors. The motivations are multifaceted and deeply intertwined with the sub-region's aspirations, challenges, and geopolitical significance. For example, in Nigeria, the government has cited national security, crime prevention and investigation, economic stability and wellbeing, public emergency and safety, and commitment to international agreements as the basis for surveillance.[236] Other motivations include preventing terrorism, border control and migration, and maritime security challenges. These motivations have manifested in mandatory SIM registration, the linkage of SIM and national identity registration, and the deployment of mass surveillance tools. West African countries, under the aegis of ECOWAS, have also shown an inclination towards collaborative surveillance, especially for transnational threats, with information sharing and joint operations becoming increasingly common.[237] An example is the joint effort to secure

232 Guinea and Togo.

233 Gambia, Guinea-Bissau, Liberia, and Sierra Leone.
Infographics—Privacy lens. (2023, March 11). https://privacylens.africa/infographics/

234 'CIPESA. (2020, August 25). Niger passes new law on interception of communications. Collaboration on International ICT Policy for East and Southern Africa (CIPESA). Retrieved October 22, 2023 from https://cipesa.org/2020/08/niger-passes-new-law-on-interception-of-communications/.

235 (Terrorism and Organised Crime – Amani Africa, n.d.) Retrieved March 3, 2024, from https://amaniafrica-et.org/tag/terrorism-and-organised-crime/.

236 Article 7(3) of the Lawful Interception of Communication Regulations (LICR).

237 Limited, D. I.-C. (n.d.). Archives | Economic Community of West African States (ECOWAS). Retrieved October 20, 2023, from https://www.ecowas.int/procurement/archives_m/.

the coastal areas in the sub-region – Gulf of Guinea, which has seen the deployment of modern surveillance technologies such as drones as part of maritime security.[238]
The political instability in the sub-region and the rise of extremist groups that have posed significant security threats have exacerbated the deployment of surveillance technologies.[239] As of July 2023, the sub-region had suffered over 1,800 terrorist attacks within the same year.[240] Surveillance technologies, such as drones and communication interception tools, are being deployed to provide real-time intelligence, aiding pre-emptive strikes and monitoring potential threats. Immigration control to reduce emigration to Europe is also a driving factor. Countries like Mauritania, Niger and Senegal, with funding from the European Union, have deployed biometric systems, tools, and intervention units at border checkpoints to stem emigration and smuggling under border management cooperation.[241] Different governments in the sub-region have also imposed mandatory biometric registration by multiple government agencies. For context, several West African countries have integrated biometric data collection into public service provisions, such as national identity issuance and voter identification.[242]

In addition, the use of Closed Circuit Cameras (CCTV) is springing up in public places such as airports, malls, and transport stations in capital cities like Abuja, Accra, and Dakar, aimed at monitoring public spaces to deter criminal activities.[243] Some countries have acquired technologies that allow for the interception of communication through calls, messages, internet activity or weakening encryption.[244] This is done under the pretext of countering extremism and intercepting potential security threats. The deployment of drones is increasing on the continent.[245] Police and militaries are increasing spending on drones with cameras for monitoring large crowds, reconnaissance, border surveillance and monitoring of vast terrains, especially in the Sahel region marred by terrorist activities, to provide real-time aerial data, which is critical in operations against insurgent groups.[246] For instance, Burkina Faso, Mali, Niger, and Togo have been reported to buy drones from Turkish manufacturers.[247] Law enforcement officers are now reportedly using wearable cameras to record interactions between the police and the public, intended to increase transparency and accountability. For instance, this has been reportedly deployed

238 Navigating security challenges in West Africa. (2023, August 9). https://internationalsecurityjournal.com/security-challenges-west-africa/.

239 West Africa, Sahel requires tangible, long-term support to eliminate terrorism, address humanitarian crisis, special representative tells security council | meetings coverage and press releases. (n.d.). Retrieved October 20, 2024, from https://press.un.org/en/2023/sc15365.doc.htm.

240 Over 1,800 'terrorist attacks' in West Africa in 2023: ECOWAS. (n.d.). Al Jazeera. Retrieved October 20, 2024, from https://www.aljazeera.com/news/2023/7/26/over-1800-terrorist-attacks-in-west-africa-in-2023-ecowas.

241 Frontex planning operations in Senegal and Mauritania, claims NGO. (2022, July 26). InfoMigrants. https://www.infomigrants.net/en/post/42166/frontex-planning-operations-in-senegal-and-mauritania-claims-ngo.

242 African countries embracing biometrics, digital IDs. (2021, February 2). Africa Renewal. https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids.

243 Bhalla, K. H., Nita. (n.d.). The rise of surveillance tech in Africa: What you need to know | Context. Retrieved October 20, 2023, from https://www.context.news/surveillance/the-rise-of-surveillance-tech-in-africa-what-you-need-to-know.

244 Parkinson, Bariyo and Chin, Huawei technicians helped African governments spy on political opponents' Wall Street Journal (2019, August 14) Retrieved October 20, 2023, from https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

245 'Remote horizons expanding use and proliferation of military drones in Africa. Retrieved October 20, 2023 from https://paxforpeace.nl/wp-content/uploads/sites/2/import/2021-05/PAX_remote_horizons_FIN_lowres.pdf.

246 Moody, J. Drones aren't the Sahel's silver bullet. (2023, June 14).Foreign Policy. Retrieved October 20, 2023 from https://foreignpolicy.com/2023/06/14/sahel-western-africa-drones-jihad-ethiopia-mali-burkina-faso-niger/.

247 Ibid.

by the police and another security agency in Lagos State, Nigeria.[248]

According to the AI Global Surveillance Index, three countries in the sub-region—Cote d'Ivoire, Ghana, and Nigeria—reported employing artificial intelligence-enabled surveillance tools.[249] Facial recognition systems are being used and deployed in the sub-region. For instance, in Akwa Ibom State, South-South part of Nigeria, as part of modernising its airport into a smarter one, it has deployed facial recognition technology.[250] These systems can identify individuals by analysing facial features from video feeds. Some governments have deployed tools to monitor social media platforms to gauge public sentiment, track potential threats, detect gatherings and protests, and even crack down on protesters, dissidents, and critics.[251] This has led to the arrest of protesters and journalists in Nigeria.[252] In Niger, security agencies use stingray devices like IMSI catchers, which mimic cell towers, to intercept mobile phone traffic and track the movement of mobile phone users.[253] This is used as part of measures to solve crimes but has reportedly been abused to arrest citizens for non-criminal offences at the instigation of other citizens. Lastly, safe cities initiatives are springing up in major cities across the continent, and they are heavily reliant on surveillance for the promise of improved security.[254]

While extensive, deploying these surveillance technologies in some cases has yet to yield a notable improvement in the sub-region's security landscape, evidenced by the rising state of insecurity in some of the member states.[255] However, while some motivations appear beneficial, the potential misuse of surveillance, where oversight and accountability are lacking, cannot be overlooked. Surveillance can, in specific contexts, have been used to monitor opposition, suppress dissent, and consolidate political power.[256] While deploying surveillance technologies in West Africa is ostensibly cited for insecurity, the rapid adoption rate and the absence of safeguards under existing laws raise pertinent questions about misuse. As West African countries evolve, striking a balance between national security interests and individual privacy rights will be crucial.

248 Business Day. (2022, July 21). Agency deploys 233 body cameras, others in Lagos -. Business day NG. https://businessday.ng/news/article/agency-deploys-233-body-cameras-others-in-lagos/
Police begin use of body cameras in Lagos—Starconnect Media. (2020, June 3). https://starconnectmedia.com/2020/06/police-begin-use-of-body-cameras-in-lagos/
P.M. News. (2021). Lagos deploys more body cameras for LASTMA personnel's use. *pmnewsnigeria.com*. Retrieved from https://pmnewsnigeria.com/2022/08/14/lagos-deploys-more-body-cameras-for-lastma-personnels-use/.

249 'Global Surveillance Index' Retrieved from https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf.

250 Nwafor, 'A'Ibom smart airport terminal to be completed Q1 of 2023' (Vanguard News15 December 2022) Retrieved 20 October 2023 from https://www.vanguardngr.com/2022/12/aibom-smart-airport-terminal-to-be-completed-q1-of-2023/.

251 Nigerian intelligence bought tool to spy on citizens: Report. (n.d.). Al Jazeera. Retrieved October 20, 2024, from https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report.

252 Heightened surveillance by security operatives puts Nigerian journalists under climate of fear (The ICIR- Latest News, Politics, Governance, Elections, Investigation, Factcheck, Covid-19, 31 March 2023). Retrieved October 21, 2023 from https://www.icirnigeria.org/heightened-surveillance-by-security-operatives-puts-nigerian-journalists-under-climate-of-fear/.

253 Des frontières sans frontières : comment l'UE exporte la surveillance pour tenter d'externaliser le contrôle des frontières' (ritimo, 20 January 2021). Retrieved October 22, 2023, from https://www.ritimo.org/Des-frontieres-sans-frontieres-comment-l-UE-exporte-la-surveillance-pour-tenter.

254 Hillman, J. E., & McCalpin, M. (2019). Watching huawei's "safe cities." https://www.csis.org/analysis/watching-huaweis-safe-cities.

255 Keeping jihadists out of northern côte d'ivoire | crisis group. (2023, August 11). https://www.crisisgroup.org/africa/west-africa/cote-divoire/b192-keeping-jihadists-out-northern-cote-divoire.

256 Opposing surveillance. (n.d.). Retrieved 24 March 2024, from https://documents.uow.edu.au/~/bmartin/pubs/07Michael.html.

Country Report

Nigeria

Overview of surveillance technologies deployment

Nigeria has a history of military incursions and disruptions of its democratic process, which often accompany the suppression and repression of human rights.[257] One of the casualties is the right to privacy and heightened surveillance of critics, dissenters, human rights activists, the public, and journalists, among other vulnerable citizens.[258] These concerns and practices have remained despite over two decades of uninterrupted democratic process. Government spending on acquiring surveillance tools increases, often without the attendant's required safeguards. The application of surveillance technology, when deployed by governments, can be grounded in objectives that are not inherently aimed at political repression or restricting freedom of expression, highlighting its lawful potential under certain circumstances.[259] While the government has cited national security, crime prevention and investigation, economic stability and wellbeing, public emergency and safety, and commitment to international agreements as the basis for surveillance, insecurity remains a problem, and the tools have been misused and abused. Surveillance poses challenges and concerns when it is unchecked and arbitrary. Nonetheless, the country is grappling with serious security issues, which have formed the basis for increased government procurement and deployment of these tools.

The Nigerian government has invested a lot in the procurement of surveillance technologies. Funding for surveillance technologies has increased over the last two decades. According to a report by the Committee to Protect Journalists (CPJ), between 2014 and 2017, the government spent at least 127 billion naira on surveillance and security systems, with about 46 billion naira spent on surveillance capabilities in 2017 alone.[260] In 2020, the Nigerian government budgeted $9 billion for surveillance-related activities.[261]According to a report by the Institute of Department Studies (IDS), Nigeria is one of five African countries that spend more than $1 billion every year on surveillance technologies imported from countries like Germany, France, Israel, Italy, China, USA, and the UK, with over $100 million worth of tech imported from China and France.[262] The most common categories of digital surveillance technologies imported by Nigeria, as noted by the report, include internet interception technologies, mobile phone interception technologies, social media surveillance technologies, safe city technologies for surveillance of public space, and biometric ID surveillance technologies.[263]

The deployment of surveillance technologies has evolved from traditional wiretapping to more sophisticated uses like facial recognition, biometric surveillance, the breaking of encryption, the use

257 *The Ogoni crisis: A case-study of military repression in southeastern Nigeria*. (n.d.). Refworld. Retrieved 24 March 2024, from https://www.refworld.org/reference/countryrep/hrw/1995/en/21522.

258 Nigeria: On the brink of civil war? (n.d.). Refworld. Retrieved 24 March 2024, from https://www.refworld.org/reference/countryrep/writenet/1996/en/46405.

259 Feldstein, S. (n.d.). The global expansion of ai surveillance. Carnegie Endowment for International Peace. Retrieved October 23, 2024, from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

260 Budget documents. (n.d.). Retrieved October 23, 2024, from https://budgetoffice.gov.ng/index.php/resources/internal-resources/budget-documents?layout=columns.

261 Ibid.

262 Ghana's democracy at risk due to use of surveillance technology, warns new report. (n.d.). Institute of Development Studies. Retrieved October 23, 2024, from https://www.ids.ac.uk/press-releases/ghanas-democracy-at-risk-due-to-use-of-surveillance-technology-warns-new-report/.

263 Ibid page 15.

of CCTVs and drones, and social media monitoring, among others. Surveillance has become a major tool in the fight against insecurity in Nigeria, but there has also been documented abuse and misuse of these technologies. The abuse has been exacerbated by legitimising surveillance through laws that lack safeguards for responsible use and accountability mechanisms.

The deployment of surveillance technologies has manifested in different ways in the country. A prominent one is using biometrics through multiple mandatory registrations for verification and access services. For context, there is a mandatory SIM card registration requirement, and multiple government agencies require the same biometric to access social services like immigration, financial services (bank verification number), national identity number, driver's license, voter registration and other verification functionalities. The trend is also emerging in subnational units, where states now require residents to register.[264] According to a study, not less than 13 government agencies require mandatory biometrics registration,[265] despite repeated announcements by different governments to consolidate these databases.[266] This requirement has been extended to groups like internally displaced persons and refugees,[267] farmers,[268] students,[269] and social welfare intervention[270] among others.
Using biometric systems in different sectors in Nigeria has become very popular. Biometric systems have been deployed in Nigeria for various reasons, such as fraud prevention and security. In 2010, the Nigeria Communication Commission (NCC) issued a regulation that mandated all telecommunications network providers to register all SIM cards through a biometric technology that captures sensitive personal data that was used to track the activities of "criminals."[271] In 2021, the Nigerian Minister of Communications and Digital Economy, through a directive approved by the president, granted security agencies access to the national identity and SIM registration database for national security reasons.[272] The Minister did not respond to a request for freedom of information to understand the safeguards and which law was relied on.[273] In the same year, the Minister also directed that SIM registration be linked with the national identity number for security reasons.[274] However, research has shown that

264 Agboluaje, R.. (2022, May 23). Makinde flags off residents' registration exercise. The Guardian Nigeria News - Nigeria and World News. https://guardian.ng/news/makinde-flags-off-residents-registration-exercise/.

265 Eke, D., Oloyede, R., Ochang, P., Borokini, F., Adeyeye, M., Sorbarikor, L., Wale-Oshinowo, B., & Akintoye, S. (2022). Nigeria's digital identification (Id) management program: Ethical, legal and socio-cultural concerns. Journal of Responsible Technology, 11, 100039. https://doi.org/10.1016/j.jrt.2022.100039.

266 Nwafor, (2023, October) We will break jinx of non-harmonisation of database in Nigeria - interior Minister. Retrieved 21 October 2023 from https://www.vanguardngr.com/2023/10/we-will-break-jinx-of-non-harmonisation-of-database-in-nigeria-interior-minister/.

267 Angbulu, S. (2022, July 7). Only 84,803 of Nigeria's 3.2 million refugees are registered- FG. Punch Newspapers. https://punchng.com/only-84803-of-nigerias-3-2-million-refugees-are-registered-fg/
Nigeria—Biometric registration report Adamawa state—IDPS on the solutions pathway (20 September 2023) | displacement tracking matrix. (n.d.). Retrieved October 23, 2024, from https://dtm.iom.int/reports/nigeria-biometric-registration-report-adamawa-state-idps-solutions-pathway-20-september?close=true.

268 Editor. (2017, March 21). Nigeria to create biometric farmer database—Identity Week. https://identityweek.net/nigeria-to-create-biometric-farmer-database/.

269 Nigeria's students' loan scheme will be fully automated, fG says. Arise News. Retrieved 24 March 2024, from https://www.arise.tv/nigerias-students-loan-scheme-will-be-fully-automated-fg-says/.

270 Nigeria, Rwanda use digital ID for social welfare payments | Biometric Update. (2024, March 15). Retrieved 24 March 2024, from https://www.biometricupdate.com/202403/nigeria-rwanda-use-digital-id-for-social-welfare-payments.

271 Biometric technology in Nigeria: Examining data privacy concerns. (2022, March 21). African Academic Network on Internet Policy - AANoIP. https://aanoip.org/biometric-technology-in-nigeria-examining-data-privacy-concerns/.

272 Mboho, J. (2022, February 4). Pantami says Buhari has permitted security agencies to access NIMC data. Nairametrics. https://nairametrics.com/2022/02/04/pantami-says-buhari-has-permitted-security-agencies-to-access-nimc-data/.

273 CSOs: NIMC, NCC ignored FOI request on security agencies accessing citizens' data (2022, March 1). Retrieved 21 October 2023 from https://www.thecable.ng/csos-nimc-ncc-ignored-foi-request-on-security-agencies-accessing-citizens-data.

274 FG urges Nigerians to complete NIN-SIM linkage "without delay"' (2023). Retrieved 21 October 2023 from https://www.channelstv.com/2022/03/31/fg-urges-nigerians-to-complete-nin-sim-linkage-without-delay/

there is no empirical evidence to show that mandatory SIM registration solves insecurity.[275] Despite these measures, insecurity remains a problem in Nigeria.[276]

Drones are increasingly being deployed by the military and police for intelligence, surveillance, and reconnaissance, with the military additionally employing them for targeted attacks. As far back as 2018, armed drones have been used by the Nigerian military.[277] Tethered drones have been reported to be used by the Nigerian Police and Immigration, and they have been used "to monitor active crime scenes and coordinate response operations."[278] In addition, mobile phone interception technologies are widely adopted in Nigeria, considering that the use of mobile phones in Nigeria is widespread, with a large percentage of the population using them for communication and internet access.

The Nigerian government reportedly acquired multiple spyware technologies, such as Finfisher, Circles and Fiber Optic Landing Solution, to snoop on calls, texts, and phone locations worth over $18 million.[279] While security reasons support this, adopting these surveillance technologies has been regarded as intrusive and a political repression tactic.[280] In 2017, it was reported that 70% of mobile phones in Abuja were bugged by a covert security unit made up of the Department of State Services (DSS) and the Defence Intelligence Agency (DIA), comprising intelligence units from the Army, Air Force, and Navy.[281] The reason for this mass surveillance was to clamp down on threats to national security. Around the same time, it was reported that the Federal Government had concluded plans with China to build two more space satellites with eavesdropping capabilities. However, progress on this has stalled since.[282] Social media monitoring has also received much attention from the government following concerns about the unregulated nature of social media. IDS's report notes that at least $20 million has been spent on social media surveillance software and services between 2018 and 2021.[283] In 2018, the government directed security agencies to monitor the social media accounts of some prominent Nigerians for "security" concerns.[284] In 2021, a supplementary budget of 4.8 billion naira was passed to procure tools to monitor social media, including encrypted communication tools.[285] One of the tools is capable of monitoring voice calls, SMS, and traffic data, among other things.

275 GSMA, Mandatory registration of prepaid SIM cards: addressing challenges through best practice (2016, April). Retrieved October 20, 2023 from https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf.

276 Nigeria, G. (2022, February 4). One year after NIN-SIM policy, insecurity, scams fester. The Guardian Nigeria News - Nigeria and World News. https://guardian.ng/technology/telecoms/one-year-after-nin-sim-policy-insecurity-scams-fester/.

277 Abdullahi, M. (2021, September 23). Armed drones making a strong entrance in Nigeria's anti-terror campaign. HumAngle. https://humanglemedia.com/armed-drones-making-a-strong-entrance-in-nigerias-anti-terror-campaign/.

278 ADF. (2023, July 17). Nigeria using tethered drones for security. Africa Defense Forum. https://adf-magazine.com/2023/07/nigeria-using-tethered-drones-for-security/

279 Nigerian intelligence bought tool to spy on citizens: Report. (n.d.). Al Jazeera. Retrieved October 23, 2024, from https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report.

280 Adebajo, A. K., 'Kunle. (2023, February 24). How digital surveillance threatens press freedom in West Africa. HumAngle. https://humanglemedia.com/how-digital-surveillance-threatens-press-freedom-in-west-africa/.

281 'Dss bugs 70% of mobile phones in Abuja' | independent newspaper Nigeria. (2017, November 8). https://independent.ng/dss-bugs-70-mobile-phones-abuja/.

282 Ibid.

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

284 FG orders security agencies to monitor social media posts of "prominent Nigerians"' (2018, January 25) Retrieved on 21 October 2023 from https://www.thecable.ng/breaking-fg-orders-security-agencies-monitor-social-media-posts.

285 Iroanusi Q. E., Nigerian Govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls. (N.d.). Retrieved October 23, 2024, from https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html?tztc=1.

Additionally, in 2013, the government awarded a contract to an Israeli company worth $40 million to procure internet communication monitoring tools.[286] The country also spent $2 million on software used to conduct website attacks.[287] In 2017, the Nigeria Communications Commission (NCC) confirmed the government's intention to block the domain names of some websites that they claimed threatened national security.[288] In 2015, internet interception raised concerns among citizens in Nigeria following its widespread use by governors in the southern part of Nigeria[289] to hack phones and computers, giving them access to political opponents' private lives.[290] While these surveillance tools were disguised and approved as national security projects, an investigation revealed that they were personal spying endeavours by the governors to monitor political opponents.[291]

There have been similar reports about mass surveillance by government agencies, which have raised privacy concerns among citizens. In December 2016, the former Governor of Ekiti State accused the State Security Service (SSS) of hacking his phone and leaking a private conversation with his colleague.[292] He also alleged that the SSS recorded telephone conversations of Nigerians who were considered critics of the government.[293] Also, in October 2019, the CPJ reported that the Nigerian military used surveillance technologies to spy on ordinary Nigerians and the press. According to the report, the Nigerian military acquired forensic technology to collect information from phones and computers to monitor people.[294] This is traced to 2019 when CPJ documented using Cellebrite's Universal Forensic Extraction Device (UFED) by Nigerian security forces and how the military targeted journalists' phones and computers with a "forensic search" to reveal their sources.[295] Also, according to a report, 40% of Nigerian journalists have been placed under surveillance in the past.[296]

Another category of surveillance technology common in Nigeria is the deployment of CCTV and smart or safe city initiatives that are springing up. The World Bank describes safe city/smart cities as "technology-intensive" urban centres featuring an array of sensors that gather information in real-time from "thousands of interconnected devices" to facilitate improved service delivery and city management.[297] In 2008, Nigeria paid $470 million to a company to install CCTV cameras across Lagos and Abuja, while $113 million was paid to another company.[298] In 2016, the Lagos State government

286 Ogala E, Exclusive: Jonathan awards $40 million contract to Israeli company to monitor computer internet communication by Nigerians' (N.d.). Retrieved October 23, 2024, from https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html?tztc=1.

287 Ibid.

288 Ibid.

289 Akwa Ibom, Bayelsa, Delta, and Rivers states.

290 Ogala E, 'Nigerian Hacking Governors Forum: Amaechi, Akpabio, Uduaghan hacked phones too' (2015) (N.d.). Retrieved October 23, 2024, from https://www.premiumtimesng.com/news/headlines/187649-investigation-nigerian-hacking-governors-forum-amaechi-akpabio-uduaghan-hacked-phones-too.html?tztc=1.

291 Ibid.

292 Gov. Fayose accuses DSS of leaking his telephone conversation with gov. Wike | Sahara Reporters. (n.d.). Retrieved October 23, 2024, from https://saharareporters.com/2016/12/29/gov-fayose-accuses-dss-leaking-his-telephone-conversation-gov-wike.

293 Ibid.

294 Rozen, J. (2019, October 22). Nigerian military targeted journalists' phones, computers with "forensic search" for sources. Committee to Protect Journalists. https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/.

295 Ibid.

296 'Heightened surveillance by security operatives puts Nigerian journalists under climate of fear (2023, March, 3. Retrieved 22 October 2023 from https://www.icirnigeria.org/heightened-surveillance-by-security-operatives-puts-nigerian-journalists-under-climate-of-fear/.

297 Feldstein, S. (n.d.). The global expansion of ai surveillance. Carnegie Endowment for International Peace. Retrieved March 23, 2024, from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

298 Roberts T., Gitahi J., Allam P., and others, (n 37 Page 20).

announced the deployment of 13,000 CCTVs to tackle crime and improve security,[299] while in 2018, it announced the deployment of an additional 10,000 high-definition surveillance cameras across the state as part of its smart city initiative. Similarly, law enforcement officers in the state are now reportedly using wearable cameras.[300] In addition, the Lagos State government is deploying automated license plate readers for traffic management and traffic offence enforcement.[301]

An emerging trend in deploying surveillance technologies is using facial recognition systems. Akwa Ibom State commissioned a new smart terminal at the airport in May 2023.[302] The new terminal boasts facial recognition, digital self-check-in by a robot, video or scene analytics, static object detection, queue detection, and license plate readers, among other features.[303] In addition, the government has disclosed its intention to deploy facial recognition across airports in the country.[304]

Despite significant investment in surveillance tools, the persistent security challenges suggest a gap between the allocation of funds for procurement and their effective deployment.[305] This disconnect was highlighted by the Minister of the Federal Capital Territory, who noted the police and the SSS's lack of tracking tools amidst rising kidnapping and insecurity in Abuja.[306] However, the minister announced the government approved emergency funds for precise location-tracking technologies.[307] Furthermore, while investigations into arms procurement fraud among government officials[308] and calls for greater transparency in the military's budget[309] have been noted, these concerns underscore the complexity of addressing security issues through technology alone. Additionally, the procurement and deployment of these technologies raise concerns over the lack of safeguards to prevent misuse and abuse, underscoring the importance of implementing checks and balances.

299 Lagos deploys 13,000 CCTV - Daily Trust. (2016, August 18). Https://Dailytrust.Com/. https://dailytrust.com/lagos-deploys-13000-cctv/.

300 BusinessDay. (2022, July 21). Agency deploys 233 body cameras, others in Lagos -. Business day NG. https://businessday.ng/news/article/agency-deploys-233-body-cameras-others-in-lagos/
Police begin use of body cameras in Lagos—Starconnect Media. (2020, June 3). https://starconnectmedia.com/2020/06/police-begin-use-of-body-cameras-in-lagos/

301 Lagos deploys technology to monitor traffic infractions, says highway obstruction attracts N25k fine (2023, July 5). Retrieved 21 October 2023 from https://www.thecable.ng/lagos-deploys-technology-to-monitor-traffic-infractions-says-highway-obstruction-attracts-n25k-fine.
Faminu, G. (2021, February 18). Lagos deploys cameras to combat violation of traffic rules. Business day NG. https://businessday.ng/news/article/lagos-deploys-cameras-to-combat-violation-of-traffic-rules/.

302 Gov Udom commissions Victor Attah international airport terminal | live. (n.d.). Retrieved October 23, 2023, from https://www.youtube.com/watch?v=QSnM6mvGh2w.

303 Nwafor, 'A'Ibom smart airport terminal to be completed Q1 of 2023' (2022, December) Retrieved 21 October 2023 from https://www.vanguardngr.com/2022/12/aibom-smart-airport-terminal-to-be-completed-q1-of-2023/.

304 Aina, D. (2023, March 22). FG to install facial recognition technology at airports. Punch Newspapers. https://punchng.com/fg-to-install-facial-recognition-technology-at-airports/.

305 Ijaseun, D. (2024, February 19). Has the military tech failed to tame Nigeria's insecurity? Business day NG. https://businessday.ng/politics/article/has-the-military-tech-failed-to-tame-nigerias-insecurity/

306 Shaibu, N. (2024, March 14). FCT police, DSS lack tracking device – Wike. Punch Newspapers. https://punchng.com/fct-police-dss-lack-tracking-device-wike/.

307 Ogunseyin, O. (2024, January 22). Wike announces Tinubu's approval for emergency procurement of digital tracking tools to enhance security. The Guardian Nigeria News - Nigeria and World News. https://guardian.ng/news/wike-announces-tinubus-approval-for-emergency-procurement-of-digital-tracking-tools-to-enhance-security/.

308 Kazeem, Y. (2015, November 18). Nigeria will arrest its ex-security chief for $2 billion arms fraud while Boko Haram ran riot. Quartz. https://qz.com/africa/553028/nigeria-will-arrest-its-ex-security-chief-for-2-billion-arms-fraud-while-boko-haram-ran-riot.

309 Abdullahi, M. (2021, September 13). Nigeria's opaque military budget culture increases risks of corruption. HumAngle. https://humanglemedia.com/nigerias-opaque-military-budget-culture-increases-risks-of-corruption/.

Case Studies

Case study 1: The Use of Surveillance Technology by South-South Nigerian Governors and its Impact on Citizens

This case involves the use of surveillance technology by four former governors in the south-south region of Nigeria, particularly in Bayelsa, Rivers, Akwa Ibom, and Delta states.[310] The investigation uncovered a disturbing pattern of illegal surveillance, phone hacking, and privacy violations carried out by these political leaders, often under the pretext of national security.

Summary of the Surveillance by States

Bayelsa State - The governor's hacking activities, which began in 2012 and lasted through 2013, were exposed when documents from the Italian cyber weaponry firm, Hacking Team, were leaked. The actions were conducted without permission from the Office of the National Security Adviser, which is required to acquire cyber defence tools. This revelation highlighted the misuse of surveillance technology at the state level.

Rivers State - The governor initiated a spying program in 2008 to enhance state security. However, it later became evident that the program was primarily used for political espionage. The C4i technology deployed for this purpose was intended for law enforcement but was co-opted for personal and political gain.

Akwa Ibom State - The government cited concerns about kidnapping to justify the acquisition of surveillance technology. However, these tools were also used to monitor the communications of both private citizens and government officials, especially those in opposition.

Delta State - The governor used similar technology for surveillance, ostensibly to combat kidnapping. However, the extent and purposes of the surveillance were never disclosed during investigations. Unfortunately, no officials were held accountable in all the use cases.

Case study 2: Surveillance and Privacy Concerns Surrounding EFCC's 'Eagle Eye' Mobile Application and the Court's Disturbing Verdict

In 2021, the Economic and Financial Crimes Commission (EFCC) launched a mobile application called "Eagle Eyes" which was designed to assist the agency in receiving complaints and reports from the public.[311] The app lets people snap and upload pictures of suspected financial crimes to the EFCC. The app has been downloaded over 10,000 times. However, the app does not have a privacy notice, and it is embedded with advertisement trackers[312] that are capable of monitoring the activities of anyone who has installed the app and sharing them with advertisers.[313] Shortly after the app was

310 Ogala E (n 84).

311 Ikigai Innovation Initiative challenges the Federal Government and its agencies for violations of digital rights. (2022, September 14). Ikigaination.Org. https://ikigaination.org/ikigai-innovation-initiative-challenges-the-federal-government-and-its-agencies-for-violations-of-digital-rights/.

312 Ibid.

313 Ibid.

launched, Ikigai Innovation Initiative, a civil society organisation, raised concerns and filed a complaint with the National Information Technology Development Agency (NITDA), which functioned as the data protection authority at the time, about the app's lack of privacy notice, which means that the app's processing activities are not disclosed to users, and the use of advertisement trackers without users' knowledge and permission. The app is privacy-invasive as it allows strangers to photograph or record people or their property, thereby violating their rights to privacy, guaranteed under Section 37 of the Nigerian Constitution. After repeated follow-ups and without response, Ikigai filed a case in court.

In court, Ikigai presented evidence of how the trackers can monitor user behaviour and identified third parties receiving data from these trackers. While the EFCC argued that it did not collect personal data like names or email addresses, Ikigai contended that online behavioural profiling constituted personal data. The court ruled in favour of the EFCC, considering the app's societal objective to outweigh individual privacy concerns since it did not collect identifying information. The court failed to recognise the risk of embedding trackers within a public-serving app and sharing data with third parties like advertisers. Such third-party trackers could accumulate comprehensive details about users' online behaviours and preferences, enabling detailed profiling for targeted advertising, content delivery, and beyond. Without transparency around its existence, this could expose sensitive personal information and habits, increasing the risk of data misuse or unauthorised access.[314] At the time of writing this report, an appeal has been filed with the Court of Appeal.

Regulatory Framework and Privacy Laws

Existing Laws and Regulations

Although there is no specific law on surveillance, Nigeria has ratified or is a signatory to several international instruments that guarantee citizens' rights to privacy and freedom from unwanted surveillance.[315] These include the African Charter on the Rights and Welfare of the Child, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the ECOWAS Supplementary Act on Personal Data Protection. Nigeria's surveillance legal framework is domiciled in multiple laws. The closest attempt at direct surveillance regulation was in 2019 when the Lawful Interception of Communications Regulation (LICR) was issued.

The Nigeria Data Protection Act (NDPA), the Nigeria Data Protection Regulation, and its Implementation Framework provide the regulatory framework for data protection in the country. The laws apply to law enforcement and other public authorities, creating different obligations to ensure responsible data processing. However, the NDPA and the Implementation Framework create exemptions to these laws for national security and for the purposes "of the prevention, investigation, detection, prosecution, or adjudication of a criminal offence."[316]

The Freedom of Information Act 2011 provides access to public records for everyone entitled. However, it limits third parties' access to personal information and ensures the confidentiality of personal and

314 Unpacking the Court verdict: Ikigai's challenge to EFCC'S Eagle eye app dismissed. (2023, August 14). Ikigaination.Org. https://ikigaination.org/unpacking-the-court-verdict-ikigais-challenge-to-efccs-eagle-eye-app-dismissed/.

315 Roberts T., Ali A. M., Farahat M., and Others, 'Surveillance law in Africa: A review of six countries' (Institute of Development Studies: 2021). Retrieved 18 October 2023 from https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y.

316 Section 3 (2) (a) & (c) of Nigeria Data Protection Act and Article 2.1 of Implementation Framework.

sensitive data whose access to third parties may negatively impact the rights and freedoms of data subjects.

Several domestic laws enable and limit surveillance activities in Nigeria, which the government and other state actors rely on. For example, the provisions of the Nigerian Constitution limit the fundamental rights of citizens to overriding public interests, provided they are reasonably justifiable.[317] Section 37 guarantees the right to privacy for citizens, their homes, correspondence, telephone conversations, and telegraphic communications. Section 45 allows for restrictions on these rights in the interest of defence, public safety, public order, public morality, or public health. Still, such restrictions must be reasonably justifiable in a democratic society.

Section 45 (2) (e) and (f) of the Cybercrimes (Prohibition, Prevention, etc.) Act permits law enforcement officers to apply for a warrant to search computer systems, decrypt encrypted data, and request data from service providers without notifying the person surveilled. Section 38(1) compels service providers to keep traffic and content data for two years. Section 38(4) stipulates that such data must be used solely for legitimate reasons, but the Act does not specify what constitutes "legitimate." Furthermore, Section 45 permits law enforcement to obtain electronic evidence for criminal probes without informing the subject of the investigation. A bill to amend the Cybercrimes Act 2015 is before the National Assembly.

The Mutual Assistance in Criminal Matters Act permits the interception of telecommunications, postal items, and surveillance. The Act enables countries to share surveillance information relating to a criminal's identification and location solely for criminal investigations.[318] Interception is strictly limited to severe criminal matters, and the Act enforces transparency by mandating the publication of government data requests, which must stem from reasonable suspicion.

The Terrorism Prevention Amendment Act also allows the interception of communications to prevent terrorism. The law empowers law enforcement agencies to intercept communications to prevent and detect terrorist acts with approval from designated authorities.[319] It also allows for investigation without a warrant in cases of verifiable urgency and threats to life.[320]

The Nigerian Communications Commission (NCC) is Nigeria's telecommunications regulator. The NCC Act empowers the NCC to intercept communications in emergencies in the public's interest. One of the criticisms of the Act is that it fails to define key terms such as "public emergency" and "public safety," leaving room for ambiguities that could form the basis for abuse of authority by the government.[321] The NCC has issued some regulations that allow law enforcement agencies to intercept communications and access personal data, thereby exposing citizens to privacy violations.

The Registration of Service Telephone Subscribers Regulations 2011 establishes a central database for subscriber information accessible by security agencies with specified rank requirements.[322] The regulation mandates SIM card registration with biometric data, reducing anonymity. While

317 Section 45 of the Constitution of the Federal Republic of Nigeria, 1999.
318 Part V of the Act.
319 Section 29
320 Section 25
321 Section 148.
322 Part 2.

it guarantees the privacy and confidentiality of subscriber information, it also allows access by security agencies subject to legal requirements and national security considerations.[323] It allows refusing requests that breach constitutional provisions or threaten national security. The Nigerian Communications (Enforcement Process, etc.) Regulations 2019 require licensees to retain call data and provide information to law enforcement agencies, subject to rank requirements and court orders.[324] The Guideline for the Provision of Internet Service 2013 mandates the cooperation of Internet Service Providers (ISPs) with law enforcement agencies in cybercrime investigations and the retention of user information for twelve months.[325]

The Lawful Interception of Communications Regulation (LICR) in Nigeria outlines a legal framework that governs the interception and disclosure of communications, specifying that only designated agencies[326] are authorised to intercept communications, conditional upon obtaining a court warrant.[327] This warrant is contingent upon demonstrating that interception is indispensable for accessing communication data, with the application needing to establish a credible threat to a legitimate aim. Moreover, the regulation empowers these agencies to demand the disclosure of encrypted communications, necessitating service providers under Articles 10 and 11 to facilitate interception capabilities and prohibiting the offering of non-interceptable services. An annual summary of interception activities must be submitted to the attorney general, though it remains confidential and not publicly accessible.[328]

The regulation delineates the conditions under which interception may occur, with and without a warrant, under Articles 7 and 8, respectively. Interception without /warrant requires the law enforcement authority to seek judicial approval retrospectively within 48 hours, failing which the interception is deemed illegal. Furthermore, the LICR stipulates that information obtained from a disapproved interception cannot be used in criminal prosecution,[329] reinforcing the confidentiality and temporary nature of the data collected, which must be destroyed post-investigation. Article 20(1) allows for judicial review by affected individuals or network providers. However, Article 13(4) indicates such warrant applications proceed without notifying the subjects, raising challenges for those wishing to contest surveillance activities because they cannot be notified.

Additionally, the National Security Agencies Act is significant for establishing various intelligence agencies.

Ghana

Overview of Surveillance Technologies Deployment

The deployment of surveillance technology in Ghana is a growing concern, with reports suggesting

323 Article 8.

324 Article 8.

325 Paragraph 6.

326 The agencies listed under the law are the State Security Service, the Nigeria Police Force, and the Office of the National Security Advisor.

327 Article 13(3).

328 Article 19(4).

329 Article 13(2)(d).

that the government's increasing procurement of surveillance technologies is putting Ghana's democratic profile at risk due to the potential to abuse citizen's privacy rights.[330] Ghana has been reported to import surveillance technology from six countries: the UK, Switzerland, Greece, Israel, China, and Taiwan.[331] Research shows that Ghana adopts various forms of surveillance, including mobile interception through the popular Pegasus spyware, which is designed to hack phones and steal personal information.[332] Ghana spent about $300 million on a smart city project to provide nationwide Wifi connectivity and $410 million on a safe city project using Huawei's facial recognition technology.[333] This technology has been used for public space surveillance in markets, airports, etc., raising concerns about privacy and human rights abuses. In addition, Ghana maintains a mandatory biometric passport and identification system. Identification is also linked to SIM cards on registration, which are used to identify during bank transactions.[334]

Freedom House confirms Ghana's use of a surveillance tool called Cellebrite decrypts encrypted devices. In 2020, the then-director of the Criminal Investigations Department (CID) disclosed that Ghanaian security forces have access to Cellebrite. The US and UK governments and Interpol provided the necessary equipment and training for officials on its use. The director also alleged that the tool was deployed mainly to strengthen criminal prosecutions.

In 2018, it became public knowledge that the Ghanaian government was in the process of agreeing with KelniGVG to establish a system enabling real-time physical access to the network infrastructure of mobile network operators in the country.[335] The government issued an executive order mandating network operators to submit comprehensive data to the National Communications Authority Common Platform. This data includes details of calls, merchant codes related to mobile transactions, mobile station international subscriber directory numbers, international mobile equipment identity codes, and geographical site locations.[336] Operators were required to facilitate real-time connectivity to the telecom providers' network switches, ensuring full access to the physical network nodes.[337] Many Ghanaians expressed concern that this was in breach of Article 12 of the 1992 Constitution, which protects the privacy of all persons.[338]

Also, the government announced the establishment of the "Common Place" platform, a technical system that would allow regulators to monitor revenues accrued by telecommunication companies

330 Ghana's democracy at risk due to use of surveillance technology, warns new report. (n.d.). Institute of Development Studies. Retrieved October 23, 2024, from https://www.ids.ac.uk/press-releases/ghanas-democracy-at-risk-due-to-use-of-surveillance-technology-warns-new-report/

331 ibid.

332 Pegg, D., & Cutler, S. (2021, July 18). What is Pegasus spyware and how does it hack phones? The Guardian. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

333 Awal, M. (2021, December 27). Celltel set to roll out us$300million Ghana smart cities project. The Business & Financial Times. https://thebftonline.com/2021/12/27/celltel-set-to-roll-out-us300million-ghana-smart-cities-project/

334 Ibid.

335 Asante, K. (2021, August 2). Ghana: MFWA welcomes high court ruling ordering government to stop collecting personal data. Media Foundation for West Africa. https://www.mfwa.org/ghana-mfwas-welcome-high-court-ruling-ordering-government-to-stop-collecting-personal-data/

336 Ibid.

337 Ghana Executive Instrument. (2020). Establishment of Emergency Communications System Instrument, 2020 (Executive Instrument No. 63). Retrieved from https://commons.laws.africa/akn/gh/act/ei/2020/63/media/publication/gh-act-ei-2020-63-publication-document.pdf.

338 May also violate Section 73 of the ECA and Section 7 of the Communications Service Tax (Amendment) Act, 2013.

operating in the country. [339] Ghanaians challenged the government's action in the Human Rights Court, stating that the system will monitor more than just revenues and warning that it will allow for easy government snooping on calls and messages. In June 2018, the Ghanian Chamber of Telecommunications corroborated the petitioners' point, explaining that the Common Platform "can actively or passively record, monitor or tap into the content of any incoming or outgoing electronic communications traffic, such as voice.[340] Sadly, the court dismissed the petition in 2018 because the petitioners could not prove the potential of a privacy breach occurring and that claims were based on public sentiments and not real evidence.

In 2021, however, a legal practitioner challenged the government's executive order to access subscribers' personal information. The High Court ruled that the data collection violated the Data Protection Act and ordered the state agency, the National Communications Authority (NCA), to stop collecting personal information from mobile phone subscribers. The court also ordered the government to delete data already collected within fourteen days of the court judgement and required Kelni GVG and other actors to pay damages to the plaintiff in the lawsuit.[341]

In 2015, the NCA contracted with Afriwave Telecom Ghana to provide an Internet Clearing House (ICH) for inbound and outbound communications. The ICH will be the single gateway through which voice and data communications can be terminated across local networks and international carriers.[342] Using this technology in the country violates the citizens' privacy rights by monitoring private calls and massive surveillance of text messages, emails, blogs, websites, and social media communications, among others. Despite the pushback from civil society organisations, the government still implemented the technology, citing public interest reasons.[343]

In April 2023, it was reported that the Israeli spyware company QuaDream had sold its Reign spyware to the Ghanaian government.[344] Citizen Lab identified the presence of QuaDream servers in Ghana that may receive data exfiltrated from QuaDream victims or be used for the spyware's one-click browser exploits.[345] Another manifestation is the use of CCTVs in the country; in 2019, the government claimed to have deployed 1,000 cameras across three cities and planned to deploy an additional 8,000 cameras.[346] In 2020, the government announced plans to deploy an additional 10,000 cameras across the country for security purposes.[347]

339 Yeboah K. Ghanaians challenge their government over a telco monitoring program, claiming privacy violations. (2018, July 25). Global Voices. https://globalvoices.org/2018/07/25/ghanaians-challenge-their-government-over-a-telco-monitoring-program-claiming-privacy-violations/

340 Ibid.

341 Asante K.,(n 109).

342 Do you care if your private conversations are monitored? Read this! (2015, February 6). Media Foundation for West Africa. https://www.mfwa.org/country-highlights/do-you-care-if-your-private-conversations-are-monitored-read-this/.

343 The MFWA raised concerns that the centralised communications infrastructure might facilitate communications surveillance or mass censorship.

344 Intelligence, M. T. (2023, April 11). Dev-0196: Quadream's "kingspawn" malware used to target civil society in Europe, North America, the Middle East, and Southeast Asia. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/.

345 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, University of Toronto. https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

346 Gov't to fix 8,000 more CCTV cameras to fight crime | GhHeadlines Total News Total Information. (2019, May 7). https://ghheadlines.com/agency/3news/20190531/123233934/govt-to-fix-8000-more-cctv-cameras-to-fight-crime.

347 Aklorbortu, P. (2020, January 23). Project Alpha: Gov't to purchase 10,000 CCTV cameras to tighten security. Yen.Com.Gh - Ghana News. https://yen.com.gh/144755-surveillance-boost-govt-fix-10000-cctvs-country-fight-crime.html.

Case studies

Case study 1: Calls for a Parliamentary Inquiry into Pegasus in Ghana

Pegasus, developed by the Israeli surveillance technology company NSO Group, has been reportedly used in Ghana. The technology was introduced during John Mahama's National Democratic Congress government in 2016 and spiked concern about citizens' fundamental human rights. There have been calls for a parliamentary inquiry into the use of Pegasus by activists in Ghana, protesting against the state's illegal use of surveillance technology.[348]

This spyware is designed to infiltrate mobile devices, including smartphones. It can enable the remote surveillance of the device's owner, including monitoring calls, messages, and emails and even activating the device's microphone and camera without the user's knowledge or permission. Pegasus has been linked to various governments and used to target journalists, activists, politicians, and others. Despite Ghana's claims that the spyware was not in use in the nation, evidence indicates that Ghanaian officials had received training in using it, and some activists, political opposition, and journalists confirmed that they were targets of the spyware.[349]

Due to the concerns raised about the Pegasus, some government officials involved in its procurement were tried in court, and those found guilty were imprisoned. However, NSO's local representatives in Ghana were discharged and acquitted. In addition, the court found that the government of Ghana had breached the country's Data Protection Act by collecting the personal information of mobile phone subscribers without permission.[350]

Case Study 2: Regulatory Framework and Privacy Laws

Existing Laws and Regulations

Despite the constitutional guarantee of privacy, several laws in Ghana allow the president and law enforcement officials the authority to order the interception and monitoring of communications, sometimes even without a court order. However, some of these laws limit the extent of surveillance, provided that it is in the public's interest.

The 1992 Constitution of Ghana provides for the rights of citizens to the privacy of their homes and communications. It creates a basic platform for the promotion of public policies that safeguard a person's privacy.[351] Article 18 of the constitution protects Ghanaians from interference with privacy, including correspondence and communication. However, where interference is under the law and is necessary for public safety, economic well-being, protection of health or morals, crime prevention, and protection of other people's rights and freedoms, the law permits it.

348 Suraya D. Is Ghana's Government using Israeli kit to spy on activists and dissidents?' (The Africa Report.com). Retreived 18 October 2023 from https://www.theafricareport.com/224982/is-ghanas-government-using-israeli-kit-to-spy-on-activists-and-dissidents/.

349 Benjakob, O (2022) 'NSO Ghana Op Exposed: Never-Before-Seen Pegasus Spyware Footage, Workers' Passports.'

350 Suraya D.,(n 122).

351 Amasah, E., Odoi, R. N., & Arthur, E. (2022). Reasonable expectations of privacy in the digital age: To what extent does Ghanaian law protect individuals' expectations in cyberspace? (SSRN Scholarly Paper 4225869). https://doi.org/10.2139/ssrn.4225869.

The Cybersecurity Act 2020 provides a legal basis for the government of Ghana to conduct surveillance. The Act makes it legal for the government to conduct surveillance on citizens and collect data from mobile network service providers in the interest of national security. Section 71 authorises security officers to collect and record communications metadata, stored or in real-time, under a court order. Although the law provides limitations on the powers of the security agencies, such as conducting surveillance under a court order,[352] it does not include the obligation to disclose the surveillance or notify the people concerned.[353] The citizens are often unaware of the surveillance activities, which violate their fundamental human rights and the right to privacy. Section 76 empowers the Cyber Security Authority (CSA) to compel a service provider to install interception technology to facilitate the government's surveillance powers under the law, while section 77 mandates service providers to retain subscriber information for at least six years and metadata and the content of communications for one year. Law enforcement officials can seek a court order to extend either period.

The Data Protection Act is Ghana's primary data protection legislation. It provides for citizens' privacy rights and creates a data protection commission responsible for implementing the Act. The legislation establishes data rights for Ghanaians, including and provides for data minimisation and data retention limitations by entities that process data. The law's requirements extend to entities that collect or process data in Ghana and to those collecting or processing data that originates from Ghana. Surveillance activities that contradict the fundamental principles of data protection as provided by the Act violate the privacy rights of data subjects.

Under Section 100 of the Electronic Communications Act, the president may, by executive instrument, require operators or providers of electronic communications networks or services to intercept communications to aid law enforcement or national security. The law also mandates all telecommunications operators to keep their subscribers' data for disclosure to the National Communication Authority. This provision is problematic because the government can abuse this authority for other purposes than security. For example, the disclosure of data to the third party, Kelni GVG, to be used to create a monitoring platform was privacy-invasive and not in the public's interest. However, the court declared the data collection to be contradictory to the provisions of the Data Protection Act.[354]

Ghana's Anti-Terrorism Act 2008 also provides legal grounds for the interception of mobile communications. It provides that security forces may, with written consent from the Attorney General, apply to the court for an order to require a communications service provider such as Vodafone to intercept customer communications to obtain evidence of the commission of an offence under the legislation.

Senegal

Overview of Surveillance Technologies Deployment in Senegal

Senegal is one of the countries deploying surveillance technologies to combat security threats.

352 Section 69.

353 Ghana: Freedom on the net 2022 country report. (n.d.). Freedom House. Retrieved October 23, 2024, from https://freedomhouse.org/country/ghana/freedom-net/2022.

354 Asante K,(n 109).

Interception of communications to monitor telephone conversations, although considered illegal, has been reported in the country. In 2021, there was a public outcry about the widespread "wiretapping and telephone spying" incident, wherein the conversations of people were being listened to by the police.[355] This practice became eminent after the outbreak of the "Ousmane Sonko-Adji Sarr" affair. The victims of this incident reported that the police were spying on them, but they were uncertain about the motive behind the surveillance.

Workplace monitoring has also been reported, creating panic for many employees.[356] It was found that Tigo, a telecommunications company, was illegally spying on the conversations of its employees, which in one case led to serious sanctions and a request for explanation due to a text they had sent.[357] This internal surveillance was triggered by the President's decision to review Tigo's operating license contract, previously known as Sentel. Consequently, the company's top management implemented invasive surveillance measures on its workforce. These tactics included telephone tapping, allowing management to intercept employees' conversations and unauthorised access to employee email accounts. Such invasive measures underscore how government decisions can indirectly lead to heightened surveillance within private entities.

Senegal also adopts a mandatory biometric ID system.[358] The country imposes mandatory biometric registration requirements on citizens, which may provide readily available data points for mass surveillance. Despite the government's claims that this system serves the public interest, concerns have been expressed about disregard for data protection principles.[359] The country is one of the African countries with a mandatory SIM registration requirement, and it has been convicted with an increasing body of evidence that it provides an easier means for law enforcement to monitor people and facilitate generalised surveillance.[360] Also, the European Union provides funding to the government to combat irregular migration.[361]

In Senegal, drones are employed as a surveillance mechanism to survey its vast territories. The Senegalese government collaborates with the European Union's agency, Frontex, which specialises in border control and security, to regulate migration through surveillance.[362] Frontex supports EU member states by overseeing their external borders and deploying various surveillance tools, including

355 Diop, R. (2021, March 24). Écoutes et espionnage téléphonique au sénégal / une pratique sous le feu des radars: Outils de dissuasion ou élément redoutable contre les infractions? KEWOULO. https://kewoulo.info/ecoutes-et-espionnage-telephonique-au-senegal-une-pratique-sous-le-feu-des-radars-outils-de-dissuasion-ou-element-redoutable-contre-les-infractions/.

356 Rédaction, L. (2011, November 30). Tigo et le scandale des écoutes téléphoniques. Senenews - Actualité au Sénégal, Politique, Économie, Sport. https://www.senenews.com/actualites/societe/tigo-et-le-scandale-des-ecoutes-telephoniques_17135.html.

357 Ibid.

358 CEDAO: Les Sénégalais, premiers bénéficiaires de la carte d'identité biométrique. (2016, October 26). La Tribune. https://afrique.latribune.fr/politique/integration-regionale/2016-10-26/cedao-les-senegalais-premiers-beneficiaires-de-la-carte-d-identite-biometrique.html.

359 Paradigm Initiative (May 2022) Digital rights and inclusion in Africa Retrieved 20 October 2023 from https://paradigmhq.org/wp-content/uploads/2022/05/Londa-English-Report-real.pdf.

360 Jentzsch N, 'Implications of Mandatory Registration of Mobile Phone Users in Africa' [2012] SSRN Electronic Journal.

361 Statewatch | Senegal: Biometric populate database will facilitate deportations, restricted EU document confirms. (n.d.). Retrieved October 23, 2024, from https://www.statewatch.org/news/2021/april/senegal-biometric-population-database-will-facilitate-deportations-restricted-eu-document-confirms/.

362 Plans to send Frontex guards to Senegal illegitimate attempt to stop migrants, asylum seekers [EN/AR]—Senegal | ReliefWeb. (2022, February 25). https://reliefweb.int/report/senegal/plans-send-frontex-guards-senegal-illegitimate-attempt-stop-migrants-asylum-seekers.

drones, radar systems, and satellite imagery, to identify and prevent unauthorised border entry.[363] Senegal has built at least nine border crossings and four regional branches of the National Division for Combating Migrant Smuggling (DNLT), which are equipped with a large number of intrusive surveillance technologies.[364]

Like most West African countries, Senegal uses smart or safe city technologies to monitor public places.[365] A report by the African Centre for Strategic Studies confirms that Huawei's Safe City project serves about 100 countries, including Senegal.[366] In Dakar, surveillance cameras are strategically placed throughout the city's major streets, squares, and public areas.[367] These cameras are connected to a central monitoring system that allows law enforcement and city authorities to watch public spaces in real-time. This technology assists in deterring crime, responding quickly to emergencies, and ensuring the safety and security of residents and visitors. Additionally, the government has implemented number plate tracking cameras.[368]

Case Studies

Case Study 1: Telephone Tapping Receive Public Outcry in Senegal

In 2021, Senegalese citizens disclosed the government's "telephone tapping" surveillance, where their private conversations were being listened to. According to a sales agent who was interviewed by the press, he admitted that he was a victim of these practices and did not know the reasons or the basis.[369] He stated that:

> "I actually suspected that my phone calls were being intercepted for several months. Every time I made a call, I realised there was a beep coming in and a little jamming for the duration of the call"[370]

Another person, a lawyer who was also a victim of the telephone tapping, stated that although the tapping is possible on a mobile network, it is regulated under the Electronic Communications Code and that wiretapping without proper regulation constitutes mass surveillance and is thereby illegal, which

363 Comment l'Europe sous-traite à l'Afrique le contrôle des migrations (1/4): « Frontex menace la dignité humaine et l'identité africaine ». (2023, September 6). Le Monde.fr. https://www.lemonde.fr/afrique/article/2023/09/06/comment-l-europe-sous-traite-a-l-afrique-le-controle-des-migrations-1-4-frontex-menace-la-dignite-humaine-et-l-identite-africaine_6188169_3212.html

364 Ibid.

365 Sécurité au Sénégal: Le projet Safe City mis à contribution a déjà installé 473 caméras - CIOMAG. (2023, September 26). https://web.archive.org/web/20230926195053/https://cio-mag.com/securite-au-senegal-le-projet-safe-city-mis-a-contribution-a-deja-installe-473-cameras/

366 Jili, B. (n.d.). Surveillance tech in africa stirs security concerns – africa center. Africa Center for Strategic Studies. Retrieved October 23, 2024, from https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

367 FAAPA. (n.d.). Vidéo surveillance: Le gouvernement va poursuivre l'installation de caméras à dakar – faapa fr. Retrieved October 23, 2024, from https://www.faapa.info/blog/video-surveillance-le-gouvernement-va-poursuivre-linstallation-de-cameras-a-dakar/

368 Vers l'»immatriculation systématique» des deux-roues. (2017, February 28). SenePlus. https://www.seneplus.com/societe/vers-limmatriculation-systematique-des-deux-roues

369 Diop A., Senegal | global information society watch. (n.d.). Retrieved October 23, 2024, from https://www.giswatch.org/en/country-report/communications-surveillance/senegal

370 Ibid.

has been grounds for conviction in other countries like France.[371]

Case Study 2: Use of Surveillance Rechnology to Curb Migration

Cellebrite's Universal Forensic Extraction Device (UFED) is being used at the Rosso border station between Senegal and Mauritania.[372] UFED, traditionally used by global law enforcement for counter-terrorism and drug control, can pull extensive data from mobile devices, including encrypted messages.[373] In Rosso, a pivotal migration route to North Africa, its primary role is to track West Africans suspected of migrating to Europe. This is part of a broader EU-funded surveillance effort facilitated by the partnership between the EU and Senegal under the National Division for the Fight Against Migrant Trafficking and Related Practices (DNLT). Besides UFED, tools like biometric systems, drones, and night-vision equipment fortify several Senegalese border posts. While the EU only funds equipment and training, such advancements raise human rights concerns, especially for the rights and safety of those in transit. Additionally, there is an ongoing debate about the potential deployment of Frontex forces to Senegal, a move that has faced criticism from the public about its impact on the country's sovereignty.[374]

The EU has been criticised for funding the program and also failing to ensure that law enforcement does not misuse the technologies.[375] Surveillance tools, including biometric fingerprinting, facial recognition systems, drones, and night-vision equipment, now fortify multiple Senegalese border posts. While the EU's financial involvement is limited to provisioning equipment and training, the rapid technological escalation raises significant human rights concerns, particularly about the rights of individuals in transit and the broader implications of such surveillance on their freedom and safety.

This case study illustrates the complex and contentious issues surrounding the EU's approach to migration control in Africa, with potential ramifications for privacy rights, national sovereignty, and regional dynamics. It underscores the need for careful consideration of the human rights implications of such policies and the importance of ensuring that surveillance technology is used responsibly and transparently.

Regulatory Framework and Privacy Laws

Existing Laws and Regulations

Senegal is one of the African countries that have had uninterrupted democracy since its independence. The Constitution guarantees citizens' rights to privacy. However, there have been reports about cases of illegal surveillance in the country.[376] The country has a data protection law and a data protection authority to enforce the law. Senegal has signed and acceded to several international and regional

371 Ibid.

372 How Europe outsourced border enforcement to Africa. (2023, July 26). In These Times. https://inthesetimes.com/article/europe-militarize-africa-senegal-borders-anti-migration-surveillance.

373 Mass extraction. (n.d.). Upturn. Retrieved 24 March 2024, from https://upturn.org/work/mass-extraction/

374 Georgio, A. de. (2023, May 26). Au Sénégal, les desseins de Frontex se heurtent aux résistances locales—Enquête. Afrique XXI. https://afriquexxi.info/Au-Senegal-les-desseins-de-Frontex-se-heurtent-aux-resistances-locales.

375 Comment l'Europe sous-traite à l'Afrique le contrôle des migrations (1/4): « Frontex menace la dignité humaine et l'identité africaine ». (2023, September 6). Le Monde.fr. https://www.lemonde.fr/afrique/article/2023/09/06/comment-l-europe-sous-traite-a-l-afrique-le-controle-des-migrations-1-4-frontex-menace-la-dignite-humaine-et-l-identite-africaine_6188169_3212.html.

376 Diop R, (n 129).

human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the African Charter on Human and Peoples' Rights.[377] It is also one of the first countries to have signed and ratified the African Union Convention on Cybersecurity and Protection of Personal Data 2014 (Malabo Convention) and the ECOWAS Supplementary Act on Personal Data Protection 2010.

The Protection of Personal Data Law 2008 and the Decree Concerning Law Enforcement 2008 regulate the processing of personal data in Senegal. It creates a data protection commission that oversees compliance with the law. The commission ensures that citizens' privacy rights are respected and their data is processed according to the law. The law provides safeguards to protect data subjects' rights, subject to certain derogations. Although the law provides for a comprehensive legal framework for the protection of citizen's data and privacy, writers have suggested that the law needs to be updated to address emerging technology issues and concerns.[378]

Article 13 of Senegal's Constitution 2001 provides further that "the secrecy of correspondence and postal, telegraphic, telephonic and electronic communications shall be inviolable, subject only to restrictions imposed by law." The restriction on the application of this provision aligns with the recommendations under the International Principles on the Application of Human Rights to Communications Surveillance, which provide that any surveillance that interferes with the right to privacy must be expressly allowed and specified under applicable laws.[379]

Article 12 of the Telecommunications Code 2011 establishes that only a judge or police officer, under specific circumstances related to prosecution, investigation, or judicial rulings, has the legal authority to request telecommunications operators and service providers to provide stored information from computer systems they administer. This provision ensures that the inviolability of private communications can only be restricted when authorised by a competent judicial authority, aligning with the principles of legality and the requirement for a publicly available legislative act to limit the right to privacy—additionally, Article 7 mandates service providers to protect consumers' privacy and personal data under the law.

The Cybercrime Law of 2008 empowers officials investigating to use appropriate technical means to record communications in real-time. It also permits service providers to assist investigation officers in intercepting communication data that is relevant to the investigation. The law provides checks for exercising the powers under this section. It limits access to data that is relevant to the investigations and also subjects it to judicial supervision.[380]

The Intelligence Services Law 2016 provides for the legitimate purposes of every surveillance.[381] It allows surveillance to address a threat only where there are no other ways. Thus, surveillance in Senegal under this law is regulated and limited only when necessary for public safety and security.

377 Diop A, (n 143).

378 Paradigm Initiative (n 133)

379 Electronic Frontier Foundation (2013) International principles on the application of human rights to communication surveillance. Retrieved October 21 from https://www.eff.org/files/necessaryandproportionatefinal.pdf.

380 See Articles 667-38 and 667-36.

381 Article 10.

The Code of Criminal Procedure Law 2016, like the Intelligence Services Law, provides for legitimate purposes for surveillance. It provides that combating terrorism is a valid ground for conducting surveillance. It allows an investigating authority to search computers for any information useful to the investigation.[382] Although under judicial authorisation and supervision, it also allows for the decryption of encrypted data for investigation.

Article 27 of the 2018 Code of Electronic Communications, broadens government surveillance capabilities to include intermediaries, raising privacy concerns. Yet, Article 36 compels service providers to prioritise user privacy and data protection. The 2008 Law on Cryptography recognises the right to encryption but imposes quality restrictions. Article 12 permits private encryption, but limitations set by Article 16 and oversight by the National Cryptology Commission may infringe on constitutionally protected communications privacy.

Challenges and Concerns of Surveillance Technology in West Africa

There is a growing trend of governments significantly investing in advanced surveillance technologies across the sub-region. This investment is often accompanied by the enactment of laws that bolster state surveillance powers. Yet, even with these new powers, reports of unauthorised surveillance targeting journalists, judges, human rights activists, and opposition members are common. Other challenges include undermining encryption, vague legal definitions in surveillance legislation, introducing invasive technologies enabling unchecked surveillance, and a lack of accountability for illicit surveillance activities. Moreover, mandates such as the compulsory installation of trackers on telecom devices and obligatory SIM card registration further intensify these concerns.

While technology can undoubtedly boost national security and administrative efficiency, the absence of clear safeguards can lead to many problematic outcomes. Instruments such as the African Declaration on Principles on Freedom of Expression and Access to Information,[383] and the International Principles on the Application of Human Rights to Communication Surveillance[384] by the Electronic Frontier Foundation (EFF) provide clear safeguards to ensure transparency and strong accountability mechanisms for surveillance by law enforcement. Surveillance technologies are presented as a panacea in the face of rising security threats and administrative needs. However, as seen through some of the cases highlighted, the motive sometimes transcends keeping the public safe. The government has shown a propensity to abuse these technologies to clamp down on civic space, arrest critics, and monitor political opponents. However, the rapid embrace of these tools without robust regulatory oversight has raised significant concerns, particularly from the digital rights perspective.

Some of the challenges and concerns that emerge from the use of surveillance technologies include the following:

Privacy Violations

The widespread use of surveillance technologies, including phone tapping and spyware like Pegasus, has led to significant invasions of privacy. Citizens' communications, locations, and activities are monitored without their knowledge or obligation to notify them, eroding trust in governance and

382 Article 90-2.

383 Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019. (2020, April 17). African Commission on Human and Peoples' Rights. https://achpr.au.int/en/node/902.

384 See (n 153).

violating fundamental rights. Activating devices' microphones and cameras without the owner's knowledge further risks personal safety, creating an environment of fear and suspicion. Also, deploying surveillance technologies introduces cybersecurity vulnerabilities, exposing citizens' data to potential exploitation by malicious actors.[385]

There have been reports of unauthorised surveillance of journalists and activists in Nigeria, which has led to the violation of their rights to privacy and human dignity. The trailing of journalists physically and digitally by intercepting communications is privacy-invasive and negatively impacts their rights to freedom of expression, which ordinarily defeats the purpose of a democratic society. In many cases, these surveillance activities have led to harassment from law enforcement agents and the loss of lives of journalists. The violation extends to the breaking of encryption. For example, mobile operators in Nigeria can be ordered to decrypt encrypted communication without judicial oversight. This was more evident when the government approved a supplementary budget to acquire tools to intercept end-to-end encrypted communication tools.

Potential for Misuse and Abuse

Without adequate checks or supervision, surveillance tools can be susceptible to misuse by those in power, be it for political vendettas, personal gains, or other non-sanctioned purposes, as already seen in the case studies discussed. In Nigeria, opposition figures and journalists have claimed to be at the receiving end of targeted surveillance aimed more at political repression than any genuine security concern, and governors of states have bought surveillance tools to monitor opposition members. Without robust checks and balances, the tools meant for protection could easily become weapons of political repression.

Lack of Transparency

Surveillance equipment's source, capabilities, and deployment details, such as those acquired from foreign entities, often remain shrouded in secrecy. In Senegal, questions about a deal for surveillance tools from a firm were raised, but details remain scant. Without transparency, it is difficult for the public to trust that these tools are being used for their stated purposes. Also, there is no legal requirement in countries to notify persons subject to surveillance or the mandatory requirement to publish a transparency report on the use of surveillance technology by law enforcement authorities.

Insufficient Redress Mechanisms

In these countries, the law does not mandate the notification of individuals post-surveillance or allow judicial review. There is no way to seek effective legal addresses when people are in the dark about being surveilled. Another challenge is the lack of understanding from the judiciary. For instance, the court's decision in the Eagle Eyes case in Nigeria shows the absence of sufficient understanding of the subject. It was clear from the outcome that the courts lacked a proper understanding of the implications of the trackers embedded in the app and how they affected the privacy rights of users. The court erroneously held that data gathered through online behavioural profiling does not constitute personal data and, as such, cannot be seen as a breach of privacy. In another case brought before the Human Rights Court in Ghana, the court held that the applicants failed to prove how the monitoring platform created by the government violated their privacy rights without assessing the actual functionality of the platform.

Economic Implications

385 Miller, G., & Parsons, C. (2023). Finding you: The network effect of telecommunications vulnerabilities for location disclosure. Citizen Lab, University of Toronto. https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/.

In a globalised world, international businesses might hesitate to operate in or partner with countries where surveillance practices are not transparent and safeguarded, fearing corporate espionage or the absence of a relief mechanism. Many countries, like Togo, have allocated significant portions of their budget to acquire state-of-the-art surveillance equipment. Yet, the benefits in terms of crime prevention and detection remain ambiguous. This raises questions about economic prudence, especially when other sectors might be underfunded. Despite significant investments in mandatory SIM registration for security purposes, the persistent insecurity in the sub-region underscores that biometric surveillance is not the magic wand governments tout it to be. These programs entail substantial costs for governments. Moreover, the extensive expenditure on high-end surveillance tools has not improved public safety. These funds could be more effectively directed towards addressing the underlying causes of insecurity.

Erosion of Trust in Government and Suppression of Rights

Without clear safeguards, citizens may view surveillance as an intrusion into their personal lives. This suspicion can erode trust in government institutions, increasing social friction and decreasing civic participation. Without strict regulations, surveillance can easily become a tool to monitor and intimidate journalists, activists, and opposition figures. This has had a chilling effect on democracy, affecting the political climate and electoral processes by creating a sense of apprehension among citizens and discouraging open discourse and fair political competition. Such practices violate individual rights and weaken the democratic fabric by stifling essential voices. In addition, minority groups, especially those that might already face discrimination or bias, can be disproportionately targeted. This can further marginalise these communities, leading to increased social tensions.

Erosion of National Sovereignty

External pressures and funding, notably from entities like the EU, have influenced African countries to adopt surveillance policies potentially misaligned with their interests, eroding national sovereignty. Additionally, the overreach of surveillance capabilities without proper legal oversight and disregard for existing regulations raises legal and ethical concerns, potentially rendering such actions unlawful.

Legal Ambiguities

The dispersion of surveillance laws across multiple sources poses a significant challenge, leading to legal ambiguities and uncertainties without clear safeguards and guidelines. Such fragmentation can leave citizens, law enforcement, and the judiciary uncertain about the limits of permissible actions. Additionally, the lack of precise definitions for terms like “public interest” and “public safety” in some of these scattered laws can pave the way for potential abuse by investigative authorities. Surveillance laws are distributed across various laws and regulations in the countries analysed, deviating from global best practices that advocate for a consolidated legal framework.

Inadequate Safeguards

Internationally recognised standards dictate that specific safeguards should be embedded in national frameworks for surveillance to be conducted safely and responsibly. These include having consolidated surveillance laws, clearly defining legitimate surveillance objectives, and ensuring an independent judiciary authorises surveillance operations. Additionally, there should be regular reviews by impartial oversight bodies and clear stipulations regarding legality. Reasonable grounds should support surveillance activities, have a defined purpose like evidence gathering, and be proportionate in their scope. Notifying the surveillance subjects is crucial, allowing them a chance for recourse and appeal. Transparency in these operations is essential, as evidenced by the need for annual public reports detailing surveillance requests and authorisations. Before deploying surveillance tools, a comprehensive human rights impact assessment is recommended. Observations from the three focus countries and many others in the sub-region indicate a stark deviation from these guidelines in legislative frameworks and practice.

Recommendations

For Governments

1. Data protection: Implement stringent rules aligning with global best practices, ensuring citizens' data is securely stored and not misused. Judicial review should be available when permission is not sought for surveillance and should be conditional upon the state's respect for privacy rights contained under the laws.

2. Budgetary transparency: Ensure surveillance technology acquisition and deployment budgets are transparent and justifiable.

3. Ensuring the safety of journalists, civil society actors, and protesters: The report shows that journalists have had to bear the brunt of the adverse effects of government surveillance. The government should establish security measures that ensure that internet or social media interception does not affect the rights of journalists, civil society actors, and protesters or curtail free speech.

4. Judicial independence: The independence of the judiciary is essential to ensuring accountability in using surveillance technologies. This is important because most of the surveillance laws in West Africa make judicial approval a precondition for the interception of communications. As such, the independence of the judiciary will be important to enforce this particular provision against the government.

5. Annual transparency reporting: Governments should foster trust and ensure accountability by publishing an annual transparency report. This report should detail the surveillance tools used, the number of surveillances authorised, their outcomes, and measures taken in response to any detected abuses. Regularly publishing such reports would enhance government accountability, allowing the public and civil society organisations to debate the balance between surveillance and human rights.

For Policymakers and Lawmakers

1. Draft comprehensive surveillance laws: Prioritise the creation of comprehensive legislation that balances security concerns with individual privacy and other human rights. A recurrent theme across the sub-region is that surveillance laws are scattered across some laws, rules and regulations, which creates ambiguities and uncertainties for law enforcement, the judiciary, and the citizens.

2. Information provisions: The surveillance legislation should require investigating authorities to inform individuals under surveillance and grant them the right to challenge or appeal the decision in court. Furthermore, if surveillance is carried out without judicial oversight, a prompt review system should be established to assess the surveillance's legality.

3. Regulation of the importation of surveillance technology: The government and regulators should consider specific regulations that regulate the importation of surveillance technology into the country. The regulation should specify the federal government agencies with authority to import surveillance technology and for what purposes. In addition, there should be a mandatory requirement to conduct a risk assessment before deployment. All countries should mandate the conduct of a comprehensive Human Rights Impact Assessment before any surveillance tool is deployed. This Human Rights Impact Assessment (HRIA) should evaluate the potential adverse impacts of the surveillance tool on individuals' fundamental rights and freedoms and propose measures to mitigate the identified risks. The current practice in the sub-region is that there is no legal requirement to conduct an HRIA, leaving room for unforeseen human rights violations. Incorporating an HRIA would provide a structured approach to anticipate, identify, and address these concerns.

4. Establishment of an independent oversight body: Countries should establish an independent oversight body with the authority and capacity to periodically review surveillance technologies, ensuring they are used in line with human rights standards. The oversight body should be endowed with the power to halt the use of any surveillance tool found to be infringing upon human rights, pending necessary adjustments. Currently, the lack of such oversight bodies in the studied countries means there is little to no check on the potential misuse of surveillance technologies.

5. Public involvement: Before passing any surveillance-related laws, ensure public consultations, incorporating citizens' voices and concerns. Also, engage in regional and global conversations about surveillance best practices and consider harmonising policies with international standards.

For Civil Society

1. Raise awareness: Engage in campaigns to educate the public about the implications of surveillance technologies, ensuring that citizens are informed and can make their voices heard. In addition, educating the public about the need for self-protection against spyware through appropriate technology, such as anti-spyware solutions, can help ensure individual privacy and protection.

2. Engage in constructive dialogue: Foster spaces for dialogue between governments, technology providers, and the public to ensure all perspectives are considered.

3. Legal support: Support people who believe unauthorised surveillance violates their digital and privacy rights. In addition to supporting victims, civil society organisations may advocate for creating regulations restricting the authority to import surveillance technology to specific government agencies and support bills that protect civil liberties. In addition, civil society organisations should leverage strategic litigation to challenge and clarify the scope of

surveillance laws. By bringing cases highlighting potential abuses or ambiguities in the legal framework, they can help ensure surveillance practices comply with human rights standards and promote transparency and accountability in the state's surveillance activities.

For Technology Providers

1. Ethical sales: Refrain from selling surveillance technology to governments or entities with a track record of human rights violations or without precise oversight mechanisms.
2. Training and guidelines: Offer training sessions for government and regulatory bodies on the ethical use of surveillance tools and provide clear guidelines on their intended use.
3. Transparency: Be transparent about the capabilities of the tools being sold and ensure that clients (countries) understand the implications of their use.

For Journalists

1. Raising public awareness: Journalists should raise public awareness about the use of surveillance technologies by the government and their effects on the rights of data subjects. Such reports to create awareness should be informed and well-researched for accuracy.
2. Whistleblower protection: Protect sources and whistleblowers who provide information on the misuse of surveillance technologies, ensuring they can safely expose malpractices.
3. Adopting self-protective strategies: Journalists should adopt self-protective measures to ensure the security of their information online, such as encrypting data or anti-spyware tools.

For International Bodies and Donors

1. Funding and support: It is recommended that financial and technical assistance be offered to nations aiming to adopt ethical surveillance practices that align with their sovereign rights. This support should prioritise respecting each country's sovereignty, ensuring that collaboration or partnership is grounded in mutual respect for local and national priorities.
2. Capacity building: Offer training sessions to regulators, policymakers, judges and civil society on global best practices related to surveillance and digital rights.
3. Conditional engagements: Make engagements and aid conditional on respect for human rights, especially when surveillance technologies are involved.

Conclusion

While surveillance technologies can potentially enhance security in West Africa, their deployment brings significant challenges and concerns. The sub-region requires the establishment of rights-respecting regulatory frameworks and practices and the strengthening of existing institutions. Without adequate safeguards, these technologies risk undermining the societal fabric in the sub-region. The rapid advancement of surveillance technology necessitates a unified and informed approach from all stakeholders. Collaboration and inclusive dialogue can lead to a balanced surveillance ecosystem that upholds national security and individual freedoms. The lack of sufficient safeguards, highlighted in international instruments, poses ethical and practical challenges. For sustained stability and growth, a deepened commitment to democratic values and human rights must match technological advancements in the sub-region.

Conclusions

This report looks at the state of surveillance across Africa, focusing specifically on Central, East, Southern, and West Africa. It agrees that technologies has facilitated development, enhanced information access, dissemination, and consumption, and helped grow democracy around the continent. Moreover, arguments abound that technology is essential to the advancement of national security, crime prevention and investigation, law enforcement, economic stability and well-being, public emergency, and safety.

Granted, as this report states, the potential benefits of technologies for governance, security, and development are undeniable. For example, surveillance cameras are now commonplace in several cities and towns across Africa and these are seen as legitimate given the rising criminality, terrorism, and violent extremism in those cities and towns.

However, as this report contends, the same technologies are increasingly used by State actors to violate fundamental liberties and rights. These actions have in turn undermined democracy, constitutionalism, the rule of law, and human rights.

In West Africa, for example, the increasing political instability, conflict, and the rise of extremist groups have necessitated the deployment of surveillance, and while those technologies may have helped the fight against terror groups, offering states the tools and strategies to fight violent extremism and criminality. Yet, authoritarian regimes use such excuses to deploy and misuse technology, monitor or surveil, manipulate, censor, and control their populace thus violating fundamental rights and freedoms as evidenced from the numerous countries reveal. Besides, as the West African section of this report shows, there is little improvement in the sub-region's security landscape.

The conclusions drawn from the four regional studies are telling with regard to the state of surveillance. Overall, there are concerns that surveillance is worsening due to the use of various technologies such as spyware, internet interception, communication surveillance, biometric ID data gathering, social media monitoring, facial recognition, and car number plate identification, which are sometimes used for illegitimate reasons, violating privacy and other rights and liberties in the process.

The use of Pegasus, Circles, and Finfisher has been flagged as examples of extrajudicial use of surveillance technologies by state actors. Their deployment has raised legitimate concerns about individual rights, especially in the absence of comprehensive and modern privacy frameworks.

For example, the report holds that the legal and regulatory framework governing surveillance technologies in Southern Africa varies from one country to another. Evidence shows that some of the countries studied have implemented comprehensive laws regulating surveillance practices. However, some lack such regulations, leading to a fragmented landscape of standards. These disparities can result in uncertainty and breed a potential for misuse of these technologies, further exacerbating concerns about privacy violations, and thus rising concerns about the misuse of technologies particularly by State security apparatuses.

Consequently, as the report argues, there is an important need to strike a balance between national security and other interests and individual privacy rights.

Crucially, the introduction of oversight and accountability as well as impact assessments before adoption and mass deployment of technologies would be critical to the protection and promotion of human rights and fundamental freedoms.

@ParadigmHQ

www.paradigmhq.org