RESILIENCE TECHNOLOGIES

SPYWARE GOVERNANCE IN AFRICA AND THE IMPACT OF SPYWARE ON CIVIL LIBERTIES

RESEARCH BY:

SHOREFUNMI BOLA-SALIU

RT Spyware Fellow 2024

Author:
Shorefunmi Bola-Saliu

Design &Layout:
Ihuoma Ndu-Eluwa

This is an output project of the RT
Spyware Fellowship 2024

TABLE OF CONTENT

0.0 Executive Summary Page 1

1.0 Introduction Page 2

2.0 Understanding Spyware Page 4

3.0 Case Studies Page 13

4.0 Impact of Spyware on Civil Liberties Page 25

5.0 Conclusion Page 28

0.0 EXECUTIVE SUMMARY

This research explores the growing use of spyware by governments in Africa and its profound impact on civil liberties, including privacy, freedom of expression, and abuse of power. Spyware, often marketed for legitimate uses such as national security and law enforcement, is increasingly being deployed in ways that undermine democratic governance and infringe on human rights.

The legal frameworks regulating spyware in Africa are largely inadequate, with many countries lacking specific laws to govern its use. Existing regulations are often ambiguous, allowing governments to exploit legal loopholes to justify surveillance and suppress dissidents. This has led to widespread extrajudicial surveillance, where spyware is used to monitor journalists, activists, opposition figures, and ordinary citizens without proper oversight or accountability.

This research looks into weak regulations and calls for stronger and more direct regulatory frameworks, greater transparency, and accountability to prevent the abuse of spyware and protect civil liberties in Africa.

1.0 INTRODUCTION

The practice of mass surveillance exists in direct tension with the fundamental human right to privacy. Universally, the right to privacy is based on the belief that individuals have reason to value freedom from unwarranted monitoring by the state, corporations, or other actors. While states claim that their use of surveillance tools, such as spyware, is for legitimate crime-fighting purposes, it has however been observed that many exceed the regulatory scope and in doing so, violate the trust citizens have in them to protect and uphold their fundamental human rights.

In Africa, where the governments of various countries are comfortable with authoritarian rule and bypassing democratic principles, the use of spyware technologies to illegally monitor, manipulate, censor, and control the citizens, is becoming the unregulated order of the day. Spyware is used to target both individuals and groups, especially journalists and dissidents, for abuse, false accusation, incarceration, and torture, especially when they express opposing opinions.

1.0 Introduction

Spyware tools take advantage of technical weaknesses on a target's device to gather a wide array of data, such as text messages, emails, media files, audio, video, passwords, voice calls, location information, call records, contact details, and all communications and interactions with the target.

Due to advanced capabilities and effectiveness in surveillance and intelligence gathering, governments—especially authoritarian regimes—continue to rely on it for monitoring not only criminals but prominent politicians, journalists, lawyers, and dissidents. Its advanced surveillance capabilities include comprehensive access to data, real-time monitoring, persistent device infiltration, geographic flexibility, effective intelligence gathering, and various strategic advantages.

This research takes a look at 5 case study countries across the five regions in Africa; Morocco, Nigeria, Rwanda, Equatorial Guinea, and Zambia. These countries are known for their notorious use of spyware and their governments' exorbitant expenses incurred on surveillance tools.

2.0 UNDERSTANDING SPYWARE

Spyware is a malicious software that gathers data from a targeted device and user and sends it to third parties without their consent. A commonly accepted spyware definition is that it is a strand of malware designed to access and damage a device without the user's consent.

It collects personal and sensitive information, transmitting it to advertisers, data collection firms, state actors, or malicious entities. The collected data can be used for surveillance for the sake of national security and law enforcement, and in some cases, for several malicious activities, including identity theft, corporate espionage, and profit gain.

2.1 TYPES OF SPYWARE

ROOTKITS

This spyware is the most dangerous as it is designed to hide the presence of certain processes or programs that aid surveillance from normal methods of detection, allowing the attacker to maintain control over the system stealthily.

ADWARE

This type of spyware carries out its tactics through targeted ads on an infected device. It is usually bundled with free and legitimate software. Once installed, the spyware tracks the browsing activities to display targeted ads.

TROJAN

This is a type of spyware that disguises itself as legitimate software to trick users into installing it. Once installed, it can perform malicious activities, such as data theft or creating backdoors for other malware.

KEYLOGGERS

This spyware records keystrokes made by the user, capturing sensitive information like usernames, passwords, and credit card numbers.

2.2 COMMON TARGETS OF SPYWARE IN AFRICA

Citizens

Ensuring national security is a responsibility of the state to its citizens, however, some governments abuse this legal right and use it to monitor, manipulate, and control their citizens with 'national security' often cited as a justification for these infringements.

Journalists

More often than not, governments use spyware to monitor and intercept communications among journalists illegally. They gather information utilising this tool and use it as an intimidation weapon, especially for those investigating corruption and human rights abuses.

Political Opponents and Activists

Governments use spyware to monitor and suppress opposition groups, dissidents, activists, and human rights defenders.

Business Leaders and Corporations

Corporate espionage targets business leaders and companies to steal trade secrets, financial information, or strategic plans.

Government Officials

Rival political factions or foreign governments may target officials for intelligence gathering or to gain political leverage.

2.3 USES OF SPYWARE

Surveillance and Monitoring

Governments and other entities use spyware to monitor communications, track movements, and gather information on targets' activities. Authoritarian governments also use spyware to track and suppress political opposition, human rights activists, and other dissidents. Authoritarian regimes continue to rely on it for monitoring not only criminals but prominent politicians, journalists, lawyers, and dissidents

Data Collection and Profiling

Due to the weak enforcement of regulatory fines, some “Big Tech” companies use spyware as a means of collecting vast amounts of data on individuals for profiling, to sell for a profit to data brokers who often use this data in targeted advertising. According to a study, an idle Android phone sent Google 900 data points over 24 hours, including location data. Facebook also tracks users on Android through its apps, logging people’s calls and SMS history.

Cybercrime

Cyber criminals and sophisticated criminal organisations use spyware to steal personal and financial information for illegal activities, especially for identity theft and fraud.

Corporate Espionage

Gaining competitive advantages by stealing intellectual property, trade secrets, and business strategies from rival companies is also one of the ways spyware is used. Meta, one of the tech giants, was alleged in 2023 to engage in anticompetitive practices and exploited user data by using Onavo’s software to spy on competitors, including Snapchat.

Intimidation and Coercion

This involves gathering compromising information on individuals to blackmail or coerce them into specific actions. Dissident journalists and former soldiers are among dozens of potential targets, earning the country a place among the “top ten perpetrators of transnational repression,” according to the NGO Freedom House.

3.0 CASE STUDIES

3.1 SURVEILLANCE IN NORTHERN AFRICA: MOROCCO

The use of sophisticated surveillance tools like the Pegasus spyware has been a particularly controversial issue in Morocco, similar to other countries in Northern Africa. High-profile targets who were arrested by the government reportedly included journalist Omar Radi, and historian and human rights activist Maati Monjib, who were known for critical reporting on government corruption and human rights abuses, and activism against the government. In 2014, Mansouri, a freelance investigative journalist, was beaten by two unknown assailants after leaving a meeting with human rights defenders, including historian Maati Monjib. A year later, armed intelligence agents raided his home at 9 a.m., finding him and a female friend in his bedroom together. They stripped him naked and arrested him for “adultery,” which is a crime in Morocco. He spent 10 months in a Rabat prison (a previous version of this article stated that Mansouri was imprisoned in Casablanca), in a cell reserved for the most serious criminals that inmates had nicknamed “La Poubelle,” or “The Trash Bin.”

In its 2018 “Hide and Seek” report, digital rights organization Citizen Lab identified operators of NSO’s Pegasus in some countries of which Morocco is a part, with records of arbitrarily detaining journalists and human rights defenders.

In 2021, Morocco was alleged to have spied on Algeria’s officials and citizens, where the Ministry of Foreign Affairs in Algiers condemned this “systematic attack on human rights and fundamental freedoms”.

Morocco's legal framework regulating spyware governance is typified by expansive and often vaguely defined powers granted to the state under laws related to national security, cybercrime, and public order. Some key legal instruments that indirectly regulate spyware governance in Morocco are: Penal Code of Morocco, Law on the Prevention and Combating of Cybercrime, Law on the Protection of Information and Communication Systems.

While these laws provide a basis for surveillance activities, they lack specific provisions regulating the use of spyware, leading to potential overreach and abuses of power, which is usually the case. The lack of detailed and direct regulations makes it hard to adequately protect the civil liberties of its citizens in the face of growing state surveillance capabilities.

3.2 SURVEILLANCE IN EAST AFRICA: RWANDA

The surveillance menace in Rwanda is well known in the digital rights community. The government has been accused of using extensive surveillance technology to monitor citizens, both domestically and internationally. Several cases prove that these surveillance practices extend beyond Rwanda's borders, targeting Rwandans living abroad.

The US advocacy group Freedom House cited Rwanda as one of the world's most prolific practitioners of "transnational repression", ranking alongside Saudi Arabia, China, Russia, and Turkey. "The commitment to controlling Rwandans abroad and the resources devoted to the effort are stunning when considering that Rwanda is a country of 13 million people, where roughly a third of the population lives below the poverty line," it states.

High-profile targets of surveillance spyware include Anne Rwigara, the sister of an opposition figure of the Rwandan government, who faced numerous challenges, including accusations of tax evasion and election misconduct, which led to Anne and her mother Adeline Rwigara being imprisoned for a year. Carine Kanimba, the daughter of Paul Rusesabagina, a Hotel Rwanda hero, was also targeted with NSO Group's Pegasus spyware.

Rwanda has made significant efforts to regulate spyware, and these legal frameworks are closely linked with its broader national security and cybercrime prevention strategies. While there are laws in place to combat cybercrime and regulate ICT use, these frameworks often grant the government broad powers to conduct surveillance, including the potential use of spyware, and these powers are with limited oversight. The lack of specific and direct legislation addressing spyware, coupled with the expansive powers of intelligence and security agencies, raises concerns about the potential for abuse and the impact on civil liberties.

No doubt, Rwanda has made impressive achievements in developing its digital infrastructure, but this has also led to increased government control over digital spaces, typically at the expense of privacy and civil liberties. Some key legal frameworks governing spyware in Rwanda are: Penal Code of Rwanda, Law Governing Information and Communication Technologies , Law Relating to the Prevention and Punishment of Cybercrimes, National Cyber Security Policy (2015), and Law determining the Powers, Mission, Organisation and Functioning of the National Intelligence and Security Service Law 73 of 2013.

3.3 SURVEILLANCE IN WEST AFRICA: NIGERIA

According to research done by the Institute of Development Studies and the African Digital Rights Network, Nigeria has been revealed as Africa's largest customer of surveillance technology contracts, spending hundreds of millions of dollars annually, and at least US$2.7bn on known contracts between 2013–2022. This is the equivalent of $12 per Nigerian citizen. For instance, in 2013, the Nigerian government under the administration of President Goodluck Ebele Jonathan awarded a US$40m contract to an Israeli arms manufacturing company, Elbit Systems, to secure a sophisticated cyber-defence tool, Wise Intelligence Technology (WiT). This system is believed to be capable of monitoring internet communications (Johnson 2013). The following year, 2014, in preparation for the 2015 general election, the Nigerian government engaged Romix Technologies, a Cyprus-registered company, and Packets Technologies, an Israeli company, on a US$2m contract to supply and install cyber-intelligence system software. The spyware was expected to conduct distributed denial of service (DDoS) on websites critical to the then president's political ambitions (Emmanuel 2016).

Researchers of the Institute of Development Studies and the African Digital Rights Network reveal that Nigeria is a leading customer of every major surveillance technology they studied, including internet and mobile and internet interception, social media monitoring, biometric ID data, and the so-called 'safe city' monitoring of citizens in public spaces. They also found that the Nigerian state permits far more government agencies to conduct surveillance than the other countries studied and has contracts with each of the leading surveillance technology suppliers based in the US, China, EU, UK, and Israel.

On the 2nd of April 2020, Solomon Akuma, a pharmacist, was arrested and detained for three months without trial, for allegedly making a tweet critical of President Buhari and his late Chief of Staff, Abba Kyari. He was eventually charged with terrorism, sedition, criminal intimidation of the president, and threat to the life of the president.

Eti-Inyene Akpan, a freelance photojournalist, who was one of the EndSars protesters in 2020 had to flee the country because he was a target of the government who had used surveillance tools to track him down due to the photos of the EndSars massacre he posted on his Instagram.

Nigeria has relatively adequate legal frameworks for regulating spyware governance and these are primarily focused on national security, cybercrime prevention, and data protection. However, the implementation and enforcement of these laws have been the drawback in the regulation of spyware. Like the other countries previously stated, the limitless powers granted to the government without effective regulation raise concerns about the infringement on civil liberties, especially of groups considered to oppose the government in power.

Some Laws regulating spyware in Nigeria include: Cybercrimes (Prohibition, Prevention, Etc.) Act, 2024, National Security Agencies Act, 1986C, Nigerian Communications Commission (NCC) Act, 2003, Nigeria Data Protection Act (NDPA), 2023, Constitution of the Federal Republic of Nigeria, 1999, Lawful Interception of Communications Regulation 2019 (LICR) (FRN 2019), a subsidiary legislation of the Nigerian Communications Act 2003 (FRN 2003).

3.4 SURVEILLANCE IN CENTRAL AFRICA: EQUATORIAL GUINEA

Surveillance and the use of spyware in Equatorial Guinea have been significant tools of political repression under the long-standing rule of the current government. The government has maintained tight control over the population through a combination of surveillance, censorship, and intimidation. The country has one of the most horrible human rights records in Africa, with the government frequently accused of using surveillance to stifle dissidents and maintain its grip on power.

In 2017, the vice president of Guinea's leading opposition party, the Union of Democratic Forces of Guinea (UFDG) was arrested. More than 100 other people – mainly activists – were also caught in the police dragnet. These arrests were part of a broader crackdown on dissidents, with many of those detained reporting that their communications had been monitored leading up to their arrests.

The legal framework for regulating spyware governance in Equatorial Guinea is notably opaque, underdeveloped, and often used to justify the repression of dissidents rather than to protect individual rights.

Examples are Constitution of the Equatorial Guinea, Penal Code (consolidated text of 1963), Equatorial Guinea Criminal Procedure Code 1967, Law-1-2.016 On Data Protection

As usual, the government states that it is primarily concerned with national security, cybercrime prevention, and the oversight of electronic communications. While these frameworks provide the government with significant powers to conduct surveillance and monitor communications, they typically lack specific provisions regulating the use of spyware and offer limited oversight mechanisms. Like other African countries, the vague and broad discretionary powers granted to government agencies have given rise to abuses, particularly in the context of targeting political opponents, activists, and journalists.

3.5 SURVEILLANCE IN SOUTHERN AFRICA: ZAMBIA

According to the Institute of Development Studies and the African Digital Rights Network, Zambia is one of Africa's countries to have made a huge investment in a Chinese 'safe city' surveillance system; a massive upgrade of its surveillance capabilities. The government can lawfully intercept communications under certain circumstances, particularly for reasons of national security, crime prevention, and public safety.

A Wall Street Journal report in 2019 states, 'In Zambia, Huawei technicians reportedly helped the government access the phones and Facebook pages belonging to bloggers who oppose Zambian President Edgar Lungu's regime. This allowed the Zambian cyber-surveillance unit to locate the bloggers' locations, which led to their arrest.'

In 2017, the government shut down The Post, a popular independent newspaper, under the pretext of tax evasion. Nonetheless, it was widely held that the closure was motivated by political motives and aimed at suppressing a vocal critic of the government. Journalists associated with the newspaper reported being under surveillance, with their communications monitored and movements tracked.

Civil society organisations (CSOs) and activists in Zambia, particularly those involved in human rights advocacy, have also been targets of state surveillance. The government has justified these actions under the guise of maintaining national security and public order.

Zambia's legal frameworks for regulating spyware governance involve a complex interplay of laws addressing interception, cybercrime, and data protection. These include The Constitution, The Cyber Security and Cyber Crimes Act, 2021, Electronic Communications and Transactions Act (2009).

Although there are provisions for judicial oversight and data protection, concerns remain regarding potential abuses and the balance between national security and individual privacy.

The issue lies not in the laws themselves, but in their misuse to justify abuses of power. This highlights the urgent need for strict accountability measures to ensure proper enforcement and prevent abuse.

4.0 IMPACT OF SPYWARE ON CIVIL LIBERTIES

A society where individuals are compelled to alter their behaviour due to the pervasive fear of surveillance is one where leadership has failed to uphold the fundamental human rights of its people. Even more troubling is a society where civil society organisations—those who champion and defend civil liberties—cannot operate freely because they are under constant scrutiny. In such an environment, the very voices that are meant to hold power accountable are stifled. When those who are supposed to protect the rights of the citizens are themselves oppressed, who then will stand up to safeguard the freedoms of the people from the very leaders they elected in trust?

There is no debate that surveillance technologies have the potential to improve public safety and national security, however, there remains a struggle with balancing state and citizen interests. The right to privacy has come under growing siege, which is in turn negatively impacting the enjoyment of other rights, including freedom of expression, association, and access to information online.

Extensive and illegal surveillance can infringe on personal privacy. Oftentimes, spyware technology is used on innocent citizens and no standard of risk assessment is carried out before launching this targeted activity.

There is no debate that surveillance technologies have the potential to improve public safety and national security, however, there remains a struggle with balancing state and citizen interests. The right to privacy has come under growing siege, which is in turn negatively impacting the enjoyment of other rights, including freedom of expression, association, and access to information online. Extensive and illegal surveillance can infringe on personal privacy. Oftentimes, spyware technology is used on innocent citizens and no standard of risk assessment is carried out before launching this targeted activity.

Civil Society Organisations (CSOs) play a vital role as watchdogs, protecting the rights of citizens against abusive surveillance. However, this same government surveillance is targeted at CSOs and threatens the work, and sometimes lives, of CSOs.

The biggest impacts of surveillance on civil liberties in Africa include:

Impact On Freedom of Expression

As a fundamental human right to be protected, spyware surveillance has stifled the freedom of certain groups of people. This tool is used to censor and, oftentimes, intimidate journalists, CSOs, political opponents, and citizens.

Abuse of Power

Government, enforcement agencies, and Intelligence agencies have practically unlimited and vague powers due to the inadequacies of the law and minimal judicial oversight. This has led to abusing of this power and backing it up with the Law.

Privacy Violations

Cases of privacy infringement with the use of spyware are not new to the Nigerian ecosystem. Both governments and private entities spy on the citizens and because effective implementation and enforcement is a big concern to upholding the right to privacy, violations are inevitable.

5.0 CONCLUSION

Sophisticated spyware tools are primarily marketed and sold to state actors, such as government agencies, intelligence services, and law enforcement organisations under the justification that they will be used for legitimate purposes, such as national security, counterterrorism, and crime prevention. There is evidence that these tools can sometimes be obtained by non-state actors through illicit markets, corrupt officials, or black market channels. This can include private corporations, criminal organisations, or even wealthy individuals. However, when it comes to a significant impact on civil liberties, the governments take the lead.

Pegasus, Circles, and Finfisher are examples of extrajudicial use of surveillance technologies by state actors mentioned in this research.

What, then, is the purpose of laws governing spyware when these very laws are used to justify abuse and blatant disregard for human rights? Ideally, the law should serve as a safeguard, holding both leaders and citizens accountable. However, in the context of surveillance, the law has often been weaponized to suppress individual freedoms and grant unchecked power to those in authority.

5.0 Conclusion

While the use of surveillance technologies by the government may be legal under current laws, it undermines the core principles of democracy and disregards the values that citizens expect their government to uphold. There is a pressing need to re-examine the laws that govern surveillance spyware, both directly and indirectly, and to refine these regulations with clear, specific guidelines rather than vague and ambiguous provisions. Accountability and transparency must be central components in the revision of these laws to ensure that the fundamental human rights of citizens are protected. It is the government's responsibility to strike a careful balance between safeguarding national security and upholding the civil liberties of its people.

6.0 REFERENCES

Institute of Development Studies. (n.d.). Surveillance legislation in Africa. Retrieved from https://www.ids.ac.uk/projects/surveillance-legislation-in-africa/

Encyclopaedia Britannica. (n.d.). Pegasus spyware https://www.britannica.com/topic/Pegasus-spyware

Institute of Development Studies. Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia. Institute of Development Studies website. Accessed July 6, 2024.

https://opendocs.ids.ac.uk/articles/online_resource/Mapping_the_Supply_of_Surveillance_Technologies_to_Africa_Case_Studies_from_Nigeria_Ghana_Morocco_Malawi_and_Zambia/26431414?file=48182842

Encyclopaedia Britannica. (n.d.). Pegasus spyware https://www.britannica.com/topic/Pegasus-spyware

Observer. Meta used spyware to monitor Snapchat, Amazon, and YouTube from 2016 to 2018. Observer website. https://observer.com/2024/03/meta-facebook-compete-snapchat-class-action-document/:~:text=Meta%20used%20a%20spyware%20to,from%20a%20class%20action%20suit.&text=How%20did%20Meta%20(META)%20become,cutthroat%20industry%20of%20social%20media%3F Accessed July 6, 2024.

Digital Content Next. Google data collection. Digital Content Next website. https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf Accessed July 6, 2024.

Forbidden Stories. Espionage, threats, suspicious deaths: Rwanda tries to silence its opponents abroad. Forbidden Stories website. https://forbiddenstories.org/espionage-threats-suspicious-deaths-rwanda-tries-to-silence-its-opponents-abroad/ Accessed July 6, 2024.

Forbidden Stories. Pegasus: The new global weapon for silencing journalists. Forbidden Stories website. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ Accessed July 6, 2024.

Citizen Lab. Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. Citizen Lab website. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ Accessed July 6, 2024.

Middle East Monitor. Algeria concerned over Morocco's alleged use of Pegasus spyware. Middle East Monitor website. https://www.middleeastmonitor.com/20210723-algeria-concerned-over-moroccos-alleged-use-of-pegasus-spyware/ Accessed July 6, 2024.

Morocco. Penal Code of Morocco [Arabic]. Dropbox. Accessed July 6, 2024. https://www.dropbox.com/scl/fi/84r3tjn42g3bqbrxs78o2/Penal-Code-of-Morocco_Arabic.pdf?rlkey=tgwxnkzqntllt33bxawfytzco&e=1&dl=0

Journal Officiel de la République Algérienne Démocratique et Populaire. Journal Officiel de la République Algérienne Démocratique et Populaire. Published August 16, 2009. Accessed July 6, 2024. https://www.wipo.int/wipolex/en/legislation/details/14778

LPA-CGR. SmartNews Algeria: Law on the post and electronic communications, law on e-commerce. LPA-CGR website. https://www.lpalaw.com/en/news/smartnews-algerie-loi-poste-communications-electroniques-loi-e-commerce/ Accessed July 6, 2024

Human Rights Watch. Transnational repression: Rwanda. Human Rights Watch website. https://www.hrw.org/news/2024/02/15/transnational-repression-rwanda Accessed July 6, 2024

The Guardian. (2021, July 23). Rwanda's Pegasus surveillance: The inside story. Retrieved from https://www.theguardian.com/commentisfree/2021/jul/23/rwanda-pegasus-surveillance

Rwanda Penal Code. University of Nottingham; 2019. Accessed August 8, 2024. https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Rwanda-Penal-Code.pdf

Law Governing Information and Communication Technology. Ministry of ICT and Innovation, Republic of Rwanda; 2016. Accessed August 8, 2024. https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Laws/ICT_LAW.pdf

Law Relating to the Prevention, Suppression, and Punishment of Trafficking in Persons and Exploitation of Others. Rwanda Legal Information Institute; 2018. Accessed August 8, 2024. https://rwandalii.org/akn/rw/act/law/2018/60/eng@2018-09-25/source

National Cyber Security Policy. Ministry of ICT and Innovation, Republic of Rwanda; 2015. Accessed August 8, 2024.

https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/National_Cyber_Security_Policy_Rwanda.pdf

6.0 References

Law Determining the Powers, Mission, Organisation, and Functioning of the National Intelligence and Security Service; 2013. Accessed August 8, 2024.

Institute of Development Studies. Nigeria spending billions of dollars on harmful surveillance of citizens. Institute of Development Studies website. https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/ Accessed July 6, 2024.

Institute of Development Studies. Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia. Institute of Development Studies website. Accessed July 6, 2024.

https://opendocs.ids.ac.uk/articles/online_resource/Mapping_the_Supply_of_Surveillance_Technologies_to_Africa_Case_Studies_from_Nigeria_Ghana_Morocco_Malawi_and_Zambia/26431414?file=48182842

Institute of Development Studies. Nigeria spending billions of dollars on harmful surveillance of citizens. Institute of Development Studies website. https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/ Accessed July 6, 2024.
HumAngle Media. How digital surveillance threatens press freedom in West Africa. HumAngle Media website. https://humanglemedia.com/how-digital-surveillance-threatens-press-freedom-in-west-africa/ Accessed July 6, 2024.

Cybercrime (Prohibition, Prevention, etc.) Act, 2024. Nigeria Computer Emergency Response Team; 2024. Accessed August 8, 2024. https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf

National Security Agencies Act, 1986. Federal Republic of Nigeria. Accessed August 8, 2024 https://lawsofnigeria.placng.org/print.php?sn=336
Nigerian Communications Commission (NCC) Act, 2003. Laws of the Federation of Nigeria. Accessed August 8, 2024. http://www.commonlii.org/ng/legis/num_act/ncca364/
Nigeria Data Protection Act, 2023. Public and Private Development Centre; 2023. Accessed August 8, 2024. https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

Constitution of the Federal Republic of Nigeria. National Human Rights Commission; 1999. Accessed August 8, 2024. https://nigeriarights.gov.ng/files/constitution.pdf
Nigerian Communications Commission. Lawful Interception of Communications Regulations, 2019. Nigerian Communications Commission website. https://www.ncc.gov.ng/documents/839-lawful-interception-of-comunications-regulations-1/file Accessed July 6, 2024.

U.S. Department of State. 2022 Country Reports on Human Rights Practices: Equatorial Guinea. U.S. Department of State website. https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/equatorial-guinea Accessed July 6, 2024.

Al Jazeera. Guinea arrests opposition figures after contested vote. Al Jazeera website. Published November 12, 2020. Accessed July 6, 2024. https://www.aljazeera.com/news/2020/11/12/guinea-arrests-opposition-figures-after-contested-vote

Equatorial Guinea. Constitution of the Republic of Equatorial Guinea. ConstitutionNet website. Accessed July 6, 2024. https://constitutionnet.org/sites/default/files/Equatorial%20Guinea%20Constitution.pdf

Equatorial Guinea. Ley No. 1/2016 de Protección de Datos. Accessed July 6, 2024. https://www.afapdp.org/wp-content/uploads/2022/02/Guinee-equatoriale-ley-1-2.016-de-proteccion-de-datos.pdf

Institute of Development Studies. Nigeria spending billions of dollars on harmful surveillance of citizens. Institute of Development Studies website. https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/ Accessed July 6, 2024.

Business Insider. Huawei technicians have been helping governments in Uganda and Zambia spy on their political opponents. Business Insider Africa website. https://africa.businessinsider.com/tech/huawei-technicians-have-been-helping-governments-in-uganda-and-zambia-spy-on-their/hy35bwd Accessed July 6, 2024.

The Zambian Observer. Tax evasion, propaganda, and lies on the closure of The Post Newspaper – Fred M'membe. The Zambian Observer website. Accessed July 6, 2024. https://zambianobserver.com/tax-evasion-propaganda-and-lies-onthe-closure-of-the-post-newspaper-fred-mmembe/

Zambian Parliament. Constitution Amendment Bill Summary. Zambian Parliament website. Accessed July 6, 2024. https://www.parliament.gov.zm/node/8067
The Zambian Observer. Tax evasion, propaganda, and lies on the closure of The Post Newspaper – Fred M'membe. The Zambian Observer website. Accessed July 6, 2024. https://zambianobserver.com/tax-evasion-propaganda-and-lies-onthe-closure-of-the-post-newspaper-fred-mmembe/

https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%204%20of%202021%2C%20The%20Electronic%20Communications%20and%20Transactions_0.pdf

Lirri, E. Privacy imperilled: Analysis of surveillance, encryption, and data localisation laws in Africa. Collaboration on International ICT Policy for East and Southern Africa (CIPESA) website. https://cipesa.org/2022/08/privacy-imperilled-analysis-of-surveillance-encryption-and-data-localisation-laws-in-africa/ Accessed July 6, 2024.
Citizen Lab. Running in circles: Uncovering the clients of cyberespionage firm Circles. Citizen Lab website. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/ Accessed July 6, 2024.

Published by:

RESILIENCE
TECHNOLOGIES

www.rtafrica.org