Mapping the supply of surveillance technologies to Africa

Malawi country report

Jimmy Kainja

DOI: 10.19088/IDS.2023.027

1. Introduction

Malawians could be sleepwalking into a surveillance state. The government has implemented data collection and centralisation programmes, including a biometric national identification card for everyone over 16 years of age and mandatory SIM card registration; a data centre has been commissioned; and the country's telecommunications regulator has announced plans for a smart city.

This report shows that, in Malawi, state surveillance operates outside any adequate legal framework, violating citizens' constitutional rights. A data protection law has remained a draft bill since 2021, despite its pressing nature, and media coverage and academic research on the worrying expansion of digital surveillance in Malawi has been scant and hard to find to date. Despite these challenges, this report breaks new ground by providing the first landscape analysis of digital surveillance in Malawi. In doing so, it provides a platform upon which other researchers can build.

In July 2022, Malawi launched a data centre in the country's commercial city, Blantyre. The Malawian State President Lazarus Chakwera registered his excitement by saying the centre would guarantee information security to investors and make Malawi a location of choice for them. However, despite the president's optimism and assurance, the data centre project is just the latest to concern data collection without regard for data protection and privacy. The Government of Malawi's partner in the project, Huawei, has a chequered reputation over similar projects with the governments of Zambia and Uganda, where its employees helped ruling parties surveil the opposition political parties.

Though Section 21 of Malawi's constitution guarantees citizens' right to privacy of communication, Malawi lacks robust data protection laws. The Communications Act No. 34 of 2016[1] and the Electronic Transactions and Cyber Security Act No. 33 of 2016[2] have data protection sections criminalising electronic communication interception. However, this legislation does not provide for legal interception of data. Section 84(2) of the Electronic Transactions and Cyber Security Act mandates a responsible cabinet minister to identify a circumstance where authorised access to interception of, or interference with, data may be permitted in specific conditions in the regulations – a worrying mandate that is prone to abuse, as the minister is not a politically neutral person. Through the draft Data Protection Bill of

1 **Communications Act No. 34 (2016)**.
2 **Electronic Transactions and Cyber Security Act No. 33 (2016)**.

2021,[3] it is clear that the Government of Malawi is aware of legal gaps in the present provisions for data protection. The draft bill aims 'to make provision for the protection of personal data, for regulation of the processing of personal data, and matters connected therewith or incidental thereto'.[4]

Using desk research and a literature review, this report takes a historical approach to examine surveillance programmes and supply chains of surveillance technologies in Malawi. In particular, it examines companies supplying five types of surveillance technologies to Malawi and looks at whose rights are being violated and who is being (dis)advantaged the most. The report also provides case studies and offers possible solutions to the problems associated with surveillance technologies.

3 **Draft Data Protection Bill 2021**.
4 *Ibid.*

2. Background

Malawi is in southern Africa, bordering Zambia to the west, Tanzania to the north and northeast, and Mozambique to the east, south, and southwest. It became a British protectorate in 1891 as Nyasaland. It later formed part of the Federation of Nyasaland and Rhodesia, the other countries being Zambia and Zimbabwe. The country gained independence in 1964 and became a republic in 1966, with Kamuzu Banda as its founding president. Upon independence, Malawi returned to the Penal Code of 1936, with its vagrancy laws in sections 180 and 184 (Ó Drisceoil 2022) aimed at monitoring people's movements. Although sections 38 and 39 of the Constitution of the Republic of Malawi 1994[5] provide for freedoms of assembly and movement, respectively, the vagrancy laws were still in force until outlawed in 2017 by the High Court, when it was challenged by a citizen, Mayeso Gwanda.[6]

The legacy of such colonial legal frameworks meant independence did not guarantee human rights and civil liberties for Malawians. Instead, power shifted from white rule to Kamuzu Banda's dictatorship, whose regime outlawed all political parties other than his Malawi Congress Party (MCP). The state-controlled Malawi Broadcasting Corporation was the only broadcaster in the country; there was no television in Malawi for the 30 years that Kamuzu Banda was in power; and the only newspapers allowed to publish belonged to Banda's publishing company, with any other publications belonging to the missionary press, dedicated to the interests of missionaries. Malawi was a police state with heavy censorship, according to Human Rights Watch (1994), overseen by the Malawi Censorship Board established under the Censorship Act of 1968.[7]

Censorship typifies much of Kamuzu Banda's rule. The Malawi Censorship Board dealt with publishing and broadcast materials, overseeing heavy surveillance in the country. In his book *Political Prisoner 3/75* (Mpasu [1995] 2014), the former political prisoner Sam Mpasu narrates how the MCP, with its Youth League wing and the Malawian police's Special Branch, itself a carryover from the colonial administration, created a physical surveillance network through the use of informers, monitoring what people were saying about Kamuzu Banda and the MCP and compliance with MCP's four cornerstones: unity, loyalty, discipline, and obedience. Mpasu's account also shows how ordinary citizens were empowered to surveil one another. Anyone could be a spy: it was a panopticon, Big Brother society.

5 **Constitution of the Republic of Malawi 1994**.
6 **Gwanda v S (Constitutional Cause 5 of 2015) [2017] MWHC 23 (10 January 2017)**.
7 **Censorship and Control of Entertainments Act 1968**.

Data centre

In July 2022, Malawi became the latest African country to commission a data centre in partnership with the Chinese technology giant Huawei (Huaxia 2022). The data centre is part of the Government of Malawi's efforts to get a foothold in the 'fourth industrial revolution', to include embracing big data, artificial intelligence, and the internet of things. State President Lazarus Chakwera said the data centre would guarantee information security for investors, thus making Malawi a location of choice for them (RegTech Africa 2022). However, the specifications of Malawi's data centre were not shared, although it is known that similar projects in Zambia and other countries where the Chinese are funding and building data centres as part of their safe city model come as part of a wider package with hundreds of CCTV cameras enabled with facial recognition, and the new facility will host all government-wide systems (Swinhoe 2022).

The president may be right in his observation about the benefits of the data centre. However, as with Malawi's national digital ID project and SIM card registration, the authorities only pay attention to the benefits of the projects, overlooking safeguards required for the safety of citizens and human rights. Despite optimism for the data centre, the project is concerning for two reasons. First, Huawei, as the Malawi government, has a chequered reputation over surveillance. For example, *The Wall Street Journal* reported that Huawei employees embedded in cybersecurity forces helped ruling parties in Zambia and Uganda intercept encrypted communications and used cell data to track political opponents (Parkinson, Bariyo and Chin 2019). What happened in these countries can easily be replicated elsewhere; African countries are good at imitating each other.

Second, Malawi lacks robust data protection laws. This has complications. Contrary to the president's belief, the data centre is unlikely to attract investors when the country has no data protection laws; robust data protection legislation is a prerequisite to attract investors. Also, without data protection legislation, the data centre could make people's data vulnerable to abuse; without data protection legislation, there is no way this project can guarantee information security. Additionally, it is unclear if Huawei would have access to information at the data centre. The cases of communication interception in Zambia and Uganda mean that these fears are legitimate, more so that Malawi has no clear provisions for legal interception of data.

Hersey (2020) has documented how Malawi established the national ID system at 'breakneck speed'. Led by the United Nations Development Programme (UNDP), the project was touted as necessary because Malawi was the only country in sub-Saharan Africa without a fully implemented national registration system. The UNDP (2022) said the national ID would

enable Malawians to 'prove their identity and benefit from their rights'. In addition, Tariq Malik (2020: 6), who worked on the project as a UNDP consultant, said the ID would be critical in combating electoral fraud, and enhancing transparency in elections that enable 'one person, one identity, one vote'. Before the implementation of the ID programme, Malawians primarily relied on driver's licences and passports as forms of identification. Few people held these, making it easy for people to accept the IDs. By only emphasising the programme's positives and the lack of questions and critical oversight from civil society organisations (CSOs), it was not difficult to convince Malawians that the national ID was essential.

As with the national ID, SIM card registration was promoted on safety grounds: SIM card registration would reduce mobile phone-based crime, especially mobile money fraud. However, the country's telecommunication regulator has confirmed that mobile money fraud has actually increased since implementing SIM card registration (Gausi 2022). Unlike the surveillance during the colonial and one-party dictatorship eras, today's digital world means governments are dealing with considerable amounts of data that even the government can lose control of to external players.

Further, the involvement of the donor community in the conceptualisation and implementation of the digital ID brings awkward questions: how much input did the Malawi government have? Has the government got the will to address the legal gaps? What about the ownership of the programme? These questions may be the subject of further inquiry. Still, it is known that since its implementation, the Malawi government has struggled to replace expired IDs and issue IDs to new applicants (Chitsulo 2021). This defeats the reasons given for the importance of the card. For example, the hiccups in issuing new IDs and replacing expired ones could affect people's right to vote. In their study, Kunyenje and Chigona (2019) established that one problem with policy implementation in most African countries is that policies are mostly initiated and funded by donors, while African governments, which may not fully appreciate the policies, have to implement them. This could explain why the Zambian and Ugandan governments had to have Huawei employees embedded in their systems.

3. Supply of surveillance technology

Internet interception

There is no evidence that the Malawi government has ever unlawfully intercepted internet traffic in ways that violate citizens' rights.

Mobile interception

Evidence shows that the Malawi government monitors citizens' private mobile phone communications and the state has used mobile phone communications as evidence in court. Any surveillance of mobile phone communication violates citizens' constitutional right to privacy. No statute allows the state to violate a citizen's rights in this way.

In 2010, the Malawi Communications Regulatory Authority (MACRA) procured a Consolidated ICT Regulatory Management System (CIRMS). According to MACRA, the system would help the regulator verify telecommunication companies' service quality, and revenue and tax levels (Chitsulo 2020). CIRMS equipment was purchased from US firm Agilis International in 2010 at US$6m (MWK6.2bn), and an additional US$20m (≈MWK21.1bn) had been paid to the company in subsequent contracts (Priezkalns 2022). Although MACRA said the equipment would be used for lawful interception, there are no details on which law provides for lawful interception. However, a court order stopped the implementation of the system after the High Court agreed with a petition by private citizens, arguing that despite MACRA's assurances, the technology could be used to eavesdrop on people's communication, contravening section 21 of the constitution, which guarantees privacy. The court ruling shows that MACRA procured CIRMS for lawful interception of communication, internet interception, and equipment identity registry (Kainja 2021).

The High Court ruling was overturned on appeal in 2017, paving the way for MACRA to implement CIRMS. However, the CIRMS is not in use because, as Chimjeka (2016) reported, the ruling came a year after MACRA had terminated its contract with CIRMS supplier Agilis International, preferring to give the contract to Global Voice Group, a South African company. Priezkalns (2022) recently reported that the country's anti-corruption body had halted attempts to procure a new CIRMS system through an unnamed supplier because of suspected offences under the country's procurement laws. It is unclear if this unnamed supplier is a South African company, as reported by Chimjeka. MACRA reportedly said that one motivation for replacing CIRMS with a new system was to surveil mobile money transactions. There are

8 million mobile money users in Malawi out of a total population of 19 million (*ibid.*).

Malawi also implemented mandatory SIM card registration in 2018, enabled under the Communications Act No. 34 of 2016. Compulsory registration means that all SIM cards must be registered on a central database and the customer requires their national ID to be verified when purchasing, replacing, or swapping a SIM (Sangala 2018). Although the policy is that SIMs can be registered using identification documents such as a passport or driver's licence, in practice only the national ID is allowed; some agents only accept the national biometric digital ID. SIM card registration is against the Human Rights Council's Special Rapporteur (2015) assertion that countries should refrain from identifying users as a condition for access to digital communications and online services and requiring SIM card registration for mobile users.

The MACRA has provided justification for why it is essential to have SIM card registration. However, the reasons involve policing functions. The police use the Criminal Procedure and Evidence Code (Act No. 36 of 1967)[8] to obtain search warrants and this law was made with a physical search of persons and property in mind. However, its use remains in the digital era to access phone call logs, and telecommunication service providers are requested to appear in court as expert witnesses to telecommunication activities.

The MACRA has provided the following justifications for SIM card registration (MACRA n.d.):

- To prevent SIM boxing. SIM boxing allows individuals to set up a device that can take more than one SIM card (a SIM box). This can be used to make international calls received as voice calls over the internet and, in turn, serve them to in-country mobile network subscribers as local traffic;
- To help recover stolen phones;
- To provide protection from hate texts, threats, and incitement of violence;
- To create a conducive environment for all phone users and 'instil discipline' in those that 'abuse phones'. (Note: the language used here is subjective and without clear definition of what 'discipline' and 'abuse phones' mean. It is itself open to abuse);

8 **Criminal Procedure and Evidence Code (Act No. 36 of 1967)**.

- To help law enforcers track down criminals who use phones for illegal activities;
- To curb fraud and theft through the use of phones.

As noted by Kainja (2021), while CIRMS implementation faced resistance, the mandatory SIM card registration, implemented in June 2017, did not face notable resistance. There are two possible reasons for this: first, citizens may have been content with the justifications for its implementation; second, CSOs may have failed to see and articulate the potential of SIM card registration to violate human rights. Wanyama (2018) asserts that it is essential that governments carefully reconcile the state's interests, personal data, and privacy rights – which has not been the case in Malawi.

Social media monitoring

Security agents still use physical ways of monitoring people's communications, including on social media networks. For example, Kainja (2022) has documented that several people in the past two years have been arrested for WhatsApp conversations, allegedly for insulting the state president, although WhatsApp has end-to-end encryption. Likewise, in 2016, two members of parliament were charged with sedition for their WhatsApp conversation (Gwede 2016).

Smart city/safe city

Malawi does not have a smart city, or facial recognition CCTV for surveillance. However, MACRA's director general, Daud Suleman, recently told the Parliamentary Committee on Public Accounts that the telecommunications regulator had identified a piece of land to establish a smart city in Dowa District, about 50km from Malawi's capital, Lilongwe. Without disclosing the source of funding and supplier of the technologies, the local media cited the director general as having told the committee that 'this is a place where the digital economy and technologies will be built up. For all the technologies the country intends to have, there is a need for this smart city to coordinate all the works of technology' (Gausi 2023).

Biometric ID

In 2016, the Government of Malawi hired a French company specialising in scratch cards, SELP (SELP Group n.d.), to supply, deliver, instal, and commission training of National Registration Bureau (NRB) staff to implement a biometric digital ID programme (National Registration Bureau n.d.). The Government of Malawi paid US$1.27m (≈MWK1.4bn) for these services. SELP is also active in Senegal, Spain, France, the United Arab Emirates, and India.

The NRB programme is governed by the Malawi National Registration Act, No. 13 of 2010 (World Bank 2017).

The total cost of the national biometric ID could not be found. However, the Government of Malawi contributed 40 per cent of the biometric digital ID project costs. The remaining 60 per cent was funded by the UK's former Department for International Development (DFID), the European Union, Irish Aid, the Government of Norway, the United States Agency for International Development, and UNDP (Citizens Rights in Africa Initiative 2017). The national ID registration targets those aged 16 and over. As of May 2020, the biometric digital ID programme had registered 9.9 million Malawians, representing over 98 per cent of the target population (Chenjezi 2020).

The NRB uses Malawi's National Registration and Identification System, also used by several government agencies, replacing previously siloed ID programmes within a brief period (Malik 2020). According to the NRB, the system was introduced to address the lack of identification in Malawi associated with the lack of universal and compulsory registration in the national register. Since 2019, the Electoral Commission has used biometric digital IDs to register voters. The Malawi Revenue Authority uses it to record taxpayers; it is used to pay public and civil servants; and the immigration department uses it to verify applicants for travel documents. The finance ministry also uses the digital ID to consider households for inclusion in social protection programmes. Government ministries, departments, and agencies have integrated digital ID into financial development and inclusion programmes, farm subsidies, health care, and other social protection services (*ibid.*).

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Malawi kwacha (MWK)	US$
Internet interception			
No evidence of surveillance technology			
Mobile interception			
Agilis International (USA)	Consolidated ICT Regulatory Management System equipment at US$6m (2010, MACRA). A further US$20m paid in subsequent contracts	27bn	26m
Social media monitoring			
No evidence of surveillance technology			
Safe cities			
No evidence of surveillance technology			
Biometric ID			
SELP Group (France)	Supply, delivery, installation, and training of NRB staff to implement the biometric digital ID programme (2016, Government of Malawi)	1.4bn	1.3m
	Total	**28.4bn**	**27.3m**

Source Authors' own. Created using data from Priezkalns (2022).

4. Impacts – the chilling effect of surveillance

Through the National Registration and Identification System, the state has built a centralised identification registry containing the biometrically verified digital ID of 10 million registered Malawians. As the digital biometric ID is linked to the registration of the SIM card, which is mandatory, the government has the potential to surveil its citizens. This is more so than in other cases as most Malawians access the internet and social media platforms, use mobile phones, and have mobile money accounts and electronic banking services attached to their mobile phones. Most smart mobile phone users have their GPS switched on, which makes monitoring mobiles possible, potentially providing the state and telecommunication companies with real-time surveillance of citizens' communications, including calls, text messages, financial transactions, location, and interaction.

Thus, data centralisation paves the way for surveillance, and in the absence of data protection law, the state and non-state actors can abuse personal information. Privacy International (2019) says compulsory SIM card registration undermines citizens' ability to 'organise and associate with others; it infringes their rights to privacy and freedom of expression'. Registering a SIM card makes it 'easier for law enforcement authorities to track and monitor people; these laws threaten vulnerable groups and facilitate generalised surveillance'. A good example is the case of investigative journalist Gregory Gondwe (see section 6 of this report). Glenn Greenwald says:

> *It's really in the private realm where dissent, creativity and personal exploration lie. When we think we're being watched, we make behaviour choices that we believe other people want us to make… it's a natural human desire to avoid societal condemnation. That's why every state loves surveillance – it breeds a conformist population.*
> (Miles 2014)

Surveillance has a chilling effect on investigative journalists, dissidents, CSOs, and political opposition, among others.

5. Solutions – data protection and citizen action

There is a clear need for the Malawian government to take a human rights-based approach to implement legislation and ICT policies. In the current case, the country needed data protection legislation before embarking on personal data collection programmes such as the digital biometric ID. The government must ensure the enactment and implementation of data protection laws.

In addition, the country needs to have clear provisions for lawful communication interception. The Criminal Procedure and Evidence Code (Act No. 36 of 1967) must be amended to align with technological changes and follow good practices concerning human rights.

There is a shortage of research in this area. Malawian academics and researchers must undertake more research and provide intellectual leadership on digital and communication surveillance, which is not fully understood in the country. This has become evident in this research. There is now a digital rights coalition in the country lobbying for digital rights legislation – a move in the right direction because local CSOs have to date largely been absent on digital rights, despite being vibrant on other issues. Thus, CSOs must lobby and demand urgent enactment and implementation of data protection law.

The involvement of CSOs will also help with mapping surveillance technologies and their supply chains in Malawi. This will help researchers with critical information about surveillance programmes. Information currently is scant and not written from a human rights perspective. For example, much remains unknown about the Malawi data centre, in part because CSOs did not demand the information when the centre was being launched.

CIPESA (2023) noted that among key issues identified by digital rights activists at the Forum on Internet Freedom in Africa, held in Lusaka, Zambia in 2022, was that CSOs are often absent when legislation is being made, only to cry foul when flawed legislation is made. Thus, CSOs must be present and influential when legislation is being drafted. At best, CSOs must demand that they are both consulted and their proposal considered. This will ensure that there is human rights-based legislation. The evidence from this study is that there is too much at stake to leave lawmaking to the lawmakers only. That is why the 1967 Criminal Procedure and Evidence Code law is used in the digital age.

6. Surveillance stories – exercising power via interception

There have been several cases in Malawi that indicate the government's willingness to surveil its citizens. People have been arrested for their posts on Facebook and encrypted, closed WhatsApp groups. Those detained have one thing in common: they are accused of insulting influential people or powerful institutions. This shows that surveillance always involves exercising power – and it invariably serves the interests of vested power groups. Kainja (2022) captured the following cases:

Chidawawa Mainje was arrested on 1 May 2022 over a WhatsApp conversation in which Mainje allegedly insulted the state president. WhatsApp is an encrypted service, but it is believed that security agents used old-fashioned spies to monitor conversations and take screenshots. Screenshots have been used as evidence to prosecute people. Mainje was charged under section 86 of the Electronic Transactions and Cyber Security Act No. 33 of 2016, which prohibits cyber-harassment. So the president is said to have been harassed even if he was unaware of the conversation. Arresting someone for a discussion in a closed space shows the state's intent and capacity to use people to monitor conversations on social media.

Gregory Gondwe, a renowned investigative journalist in Malawi, was arrested in April 2022. According to Gondwe's account of events surrounding his arrest, the police had been tracking his phone conversations. The police were aware that Gondwe had been talking to his sister on a mobile phone and they knew his exact location. There is no known technology that the police use to track or eavesdrop on people's phone calls, but it could have been aided by his registered SIM card as SIM registration is mandatory in the country and linked to national digital ID. The police also confiscated his mobile phone, suggesting a clear surveillance case. A few weeks later, the Platform for Investigative Journalism website, where Gondwe's work is published, was hacked, which MISA Malawi (2022) believe was connected to Gondwe's arrest.

References

Chenjezi, T. (2020) '**Malawi Reaping Fruits of Digital Identification**', *The Nation*, 16 May (accessed 25 April 2023)

Chimjeka, R. (2016) '**MACRA to Terminate CIRMS Supplier Deal**', *The Nation*, 28 May (accessed 25 April 2023)

Chitsulo, L. (2021) '**NRB Explains National ID Renewal Delays**', *The Nation*, 9 October (accessed 25 April 2023)

Chitsulo, L. (2020) '**MACRA Speaks on CIRMS**', *The Nation*, 27 July (accessed 25 April 2023)

CIPESA (2023) ***Move Fast and Fix Policy: African Digital Rights Advocacy in an Era of Rapid Policy Change***, CIPESA blog, 2 January (accessed 25 April 2023)

Citizens Rights in Africa Initiative (2017) ***Public Statement: Mass Registration of Malawian Citizens for National Identity Cards***, 25 April (accessed 25 April 2023)

Gausi, W. (2023) '**MACRA Identifies Smart City Land**', *The Daily Times*, 9 January (accessed 25 April 2023)

Gausi, W. (2022) '**Malawians Duped K120 Million Monthly through E-Cash Transfers**', *The Daily Times*, 4 November (accessed 25 April 2023)

Gwede, W. (2016) '**Kabwila Arrested: Malawi Police May Arrest More "WhatsApp Coup Plotters"** ', *Nyasa Times*, 22 February (accessed 25 April 2023)

Hersey, F. (2020) '**How Malawi Established a Biometric National ID System at Breakneck Speed**', *Biometric Update*, 12 October (accessed 25 April 2023)

Huaxia (2022) '**Malawi Government, Huawei Commission National Data Center**', *Xinhua*, 22 July (accessed 15 May 2023)

Human Rights Council (2015) '**Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye**', Human Rights Council, Twenty-ninth Session, Agenda Item 3, 22 May (accessed 25 April 2023)

Human Rights Watch (1994) ***Human Rights Watch World Report 1994 – Malawi***, 1 January (accessed 25 April 2023)

Kainja, J. (2022) '**Arrests Mar Malawi's Digital Rights Landscape**', *Southern Africa Digital Rights 1* (accessed 25 April 2023)

Kainja, J. (2021) ***Mapping Digital Surveillance and Privacy Concerns in Malawi***, Media Policy and Democracy Project (accessed 25 April 2023)

Kunyenje, G. and Chigona, W. (2019) '**External Actors in Forming National ICT Policy in Malawi: A Cause for Concern in Low-Income Countries?**', *African Journal of Information Systems* 11.1: 2 (accessed 25 April 2023)

MACRA (n.d.) ***Frequently Asked Questions*** (accessed 25 April 2023)

Malik, T. (2020) ***Malawi's Journey Towards Transformation: Lessons from its National ID Project***, Washington DC: Center for Global Development (accessed 25 April 2023)

Miles, K. (2014) '**Glenn Greenwald on Why Privacy is Vital, Even if You "Have Nothing to Hide"** ', *HuffPost*, 20 June (accessed 25 April 2023)

MISA Malawi (2022) '**Hacking of Platform for Investigative Journalism Website Not a Mere Coincidence**', 15 April (accessed 25 April 2023)

Mpasu, S. (1995) *Political Prisoner 3/75 of Dr. H. Kamuzu Banda of Malawi*, rev. ed. (2014), Balaka: Montfort Media

National Registration Bureau (n.d.) ***Articles*** (accessed 26 April 2023)

Ó Drisceoil, M. (2022) '**Post-Colonial Theory**', *Law Society Gazette*, 8 June (accessed 26 April 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019) '**Huawei Technicians Helped African Governments Spy on Political Opponents**', *The Wall Street Journal*, 15 August (accessed 26 April 2023)

Priezkalns, E. (2022) '**Anti Corruption Bureau Halts Purchase of National Revenue Assurance System in Malawi**', *Comms Risk*, 3 August (accessed 26 April 2023)

Privacy International (2019) ***Timeline of SIM Card Registration Laws***, 11 June (accessed 26 April 2023)

RegTech Africa (2022) '**Malawi: Malawi Opens First National Data Centre in Blantyre**', RegTech Africa, 2 August (accessed 26 April 2023)

Sangala, T. (2018) '**MACRA Sets New SIM Card Registration Deadlines**', *The Times Group*, 4 June (accessed 26 April 2023)

SELP Group (n.d.) ***About Us*** (accessed 26 April 2023)

Swinhoe, D. (2022) '**Malawi Launches National Data Center: African Country Partners with Huawei for New Facility**', *DCD*, 28 July (accessed 26 April 2023)

UNDP (2022) ***Malawi's Foundational Legal Identity System Sets the Stage for a More Efficient and Responsible Digital Future***, *United Nations Development Programme, 20 May* (accessed 26 April 2023)

Wanyama, E. (2018) ***The Stampede for SIM Card Registration: A Major Question for Africa***, CIPESA blog, 18 April (accessed 26 April 2023)

World Bank (2017) ***The State of Identification Systems in Africa: Country Briefs***, Washington DC: World Bank (accessed 23 May 2023)