

# Privacy and Personal Data Challenges and Trends in Malawi



---

September 2018



# Table of Contents

---

			
	1. Introduction		4
			
	2. Methodology		5
			
	3. Country context		6
	3.1 Political Economy		6
	3.2 ICT Status		6
	3.3 Political Environment		7
			
4. Laws and Policies Affecting Privacy and Personal Data Protection			8
	4.1 International Human Rights Instruments		8
	4.2 The Constitution of Malawi		8
	4.3 Recognition of Privacy and Personal Data Protection in Statutes		9
	4.3.1 Electronic Transactions and Cyber Security Act, 2016		9
	4.3.2 The Communications Act of 2016		10
	4.3.3 Access to Information Act, 2016		10
	4.3.4 National Statistics Act 2013		11

## 5. Results, Challenges and Trends12

5.1	Limited Understanding of Privacy	12
5.2	Weak Policy and Legal Frameworks	12
5.2.1	Absence of a Comprehensive Data Protection Framework	12
5.2.2	Fragmented Oversight Over Privacy and Data Protection	12
5.3	Data Collection Programmes by Governments	13
5.3.1	Mandatory SIM Card Registration	14
5.4	Enhanced State Surveillance Capacity	15
5.5	Legal Responsibility of Business Entities	15
5.6	Dispute Resolution and Remedies	16
5.6.1	Existing Frameworks for Redress	16
5.6.2	Notable Campaigns and Decisions	16

## 6. Conclusion and Recommendations17

6.1	Conclusions	17
6.2	Recommendations	18



# 1 Introduction and Background

Malawi, like many other African countries, is yet to enact a comprehensive law regulating citizens' right to privacy and personal data protection. This is challenging, especially since the government has been undertaking various data collection exercises including through the mandatory SIM card registration<sup>1</sup> and the nationwide mass registration of all Malawians aged 16 and above. The mass registration that started in May 2017 and ended in November 2017, is reported to have resulted in the registration of over 9.2 million people and the issuance of more than over 8.9 million National Identity Cards (NICs).<sup>2</sup>

Malawi has a number of laws that contain provisions on privacy and data protection, such as the 2016 Electronic Transaction and Cyber Security Act which in Part VII provides for the processing of personal data (Article 71); rights of data holders (Article 72); as well as security obligations to data controllers to ensure the safety of clients' data (Article 74). Other laws include the 2016 Access to Information law that provides for a framework to facilitate access to information held by information holders in compliance with any right to protected by the constitution and any other law. However, legislation such as the National Registration Act that mandated the creation of a National Registry and Identification System (NRIS), and the 2013 Business Registration Act that established the electronic Malawi Business Registration Database, which stores information for businesses, do not provide enough safeguards for clients' privacy and personal data.

The existing legislation does not offer appropriate regulatory mechanisms, thus posing a threat to privacy and data protection. For example, Article 29 of the 2016 Electronic Transactions and Cybersecurity Act requires service providers to hand over user information when presented with a court-issued warrant, though such legal safeguards have failed to prevent abuse in the past.<sup>3</sup> Under Article 52, this law requires providers of cryptography services or products to register with the regulator, Malawi Communications Regulatory Authority (MACRA) and provide the regulator with "the technical characteristics of the encryption means as well as the source code of the software used.

In addition to collecting clients' personal data, in January 2018, the government is reported to have implemented the technology called the Consolidated ICT Regulatory Management System (CIRMS),<sup>31</sup> that can conduct communication surveillance and is locally as the "spy machine."<sup>4</sup>

This study assesses the state of privacy and personal data protection in Malawi. It tracks key trends in the country over the past five years, analysing major risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy. The study identifies measures that can positively influence the right to privacy legislation in Malawi and should inform key actors, including government, the media, academia, civil society on the current legal, institutional and practice landscape as well as opportunities for advancing the right to privacy and data protection.

<sup>1</sup> Be Patriotic, Register Your SIM Card, <http://www.macra.org.mw/be-patriotic-register-your-sim-card/>

<sup>2</sup> Digital Identity Country Report: Malawi, <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf>

<sup>3</sup> Freedom on the Net 2018/Malawi available at: <https://freedomhouse.org/report/freedom-net/2018/malawi>

<sup>4</sup> Green Muheya, "Malawi roll out 'spy machine': Macra can now listen people's phone conversations," *Nyasa Times*, January 24, 2018, <https://www.nyasatimes.com/malawi-roll-spy-machine/>

## 2 Methodology

---

This study uses qualitative research methods. They include literature review, as a way of generating an understanding of the current debates and issues on privacy and data protection in Malawi. The study also analysed the country's policy and legal frameworks on privacy and personal data protection. This was to find how well, or not, the policy and legal frameworks support citizens' enjoyment of the right to privacy. The study also assessed the state of implementation of these laws and policies, including how state and non-state actors abuse them.

The laws and policies include those that govern the telecommunications sector, the media, social media, access to information, interception of communications, security and intelligence agencies, and law enforcement in general. The study also reviewed the relevant international instruments the country is a party to and the relevant constitutional and statutory provisions on data protection.

Further, interviews were conducted with purposively selected key informants. The key informants included persons working with private companies, telecommunication firms, Internet Service Providers and government ministries responsible for ICT and security. Others included staff of semi-autonomous bodies such as the National Registration Bureau, the Electoral Commission, data telecommunication regulators, media institutions, social media users, human rights defenders and activists, consumers' associations, academics, lawyers, and select individuals drawn from the general public conversant with issues of privacy and personal data protection.

## 3 Country Context

### 3.1 Political Economy

Malawi remains among the least developed countries in the world, despite being politically stable. Currently, Malawi ranks 170 out of 188 countries on the United Nations Development Programme (UNDP) Human Development Index (HDI), which is “a summary measure of average achievement in key dimensions of human development.”<sup>5</sup> An estimated 71% were living in poverty as of 2017, “despite increased public spending on health and education, which are Malawi’s priority areas.”<sup>6</sup>

Agriculture is the mainstay of the economy and the primary economic activity for over 80% of the population.<sup>7</sup> It contributes 28% of the national GDP while manufacturing contributes 10.4% and industry contributes 15.9%.<sup>8</sup> Tobacco is the country’s chief export product, while cotton, tea, sugar and coffee being major export commodities too. Roughly 83% of Malawians live in rural areas.<sup>9</sup> The country’s GDP stands at USD 5.442 billion.<sup>10</sup>

### 3.2 ICT Status

Malawi has a long way to go in creating the kind of technology access and infrastructure needed to support a vibrant digital development sector despite being geographically located amongst some of the fastest-growing digital markets in the world.<sup>11</sup> Mobile phone penetration is at 38%<sup>12</sup> while Internet penetration stands at 9.5%.<sup>13</sup> The high internet tariffs hinder uptake for the majority of Malawians.<sup>14</sup>

The market remains a duopoly between TNM and Airtel Malawi.<sup>15</sup> The telecommunications’ sector is regulated by the Malawi Communications Regulatory Authority (MACRA), established by the Communications Act of 1998<sup>16</sup> as a result of telecommunication reforms. Among others, MACRA is mandated to make regulations and policies that govern the communications sector; issue licenses to communications services providers; enforce compliance with rules, regulations and policies; and protect the interests of consumers of communication services from unfair business practices, poor quality services and harmful or inferior products.<sup>17</sup>

<sup>5</sup> Human Index for Everyone, [http://hdr.undp.org/sites/all/themes/hdr\\_theme/country-notes/MWI.pdf](http://hdr.undp.org/sites/all/themes/hdr_theme/country-notes/MWI.pdf)

<sup>6</sup> Poverty Levels Extreme in Malawi, <http://mwnation.com/poverty-levels-extreme-in-malawi-unctad/>

<sup>7</sup> Malawi economy and industry, <http://www.our-africa.org/malawi/economy-industry>

<sup>8</sup> Agriculture, Value Added (% of GDP), <http://data.worldbank.org/indicator/NV.AGR.TOTL.ZS>

<sup>9</sup> Malawi: Rural Population (% of the Total Population);, <http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS?locations=MW>

<sup>10</sup> Malawi Gross Domestic Product, <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=MW>

<sup>11</sup> Malawi: A Challenging Tech Environment available at; <https://dai-global-digital.com/dfid-and-dai-host-malawis-first-digital-development-forum.html>

<sup>12</sup> Malawi – Telecommunications, <https://www.export.gov/article?id=Malawi-telecommunications>

<sup>13</sup> National Survey on Access to and Usage of ICT Services in Malawi,

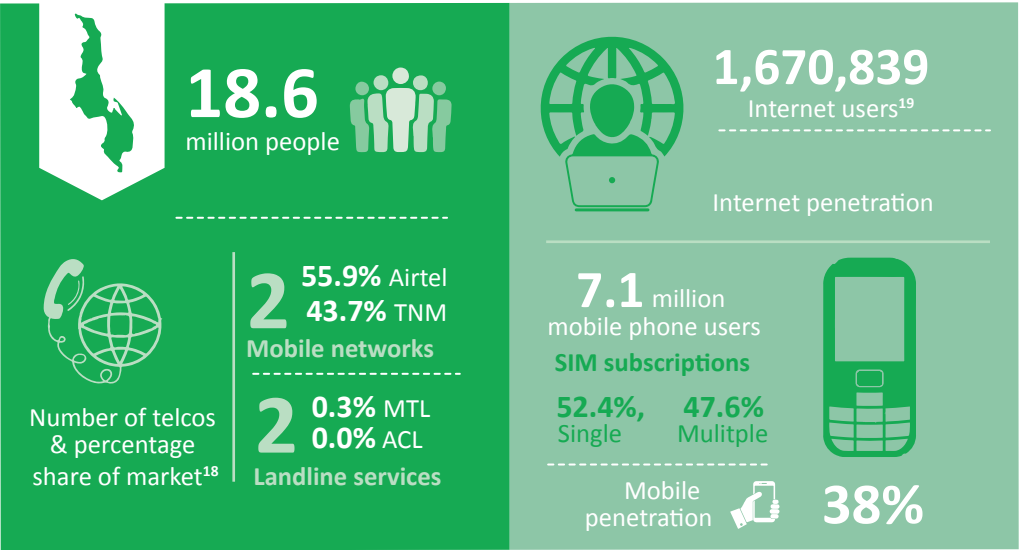
<http://www.macra.org.mw/wp-content/uploads/2016/01/MACRA-Survey-Report-National-Household-and-Individual-access-to-and-usage-of-ICT.pdf>

<sup>14</sup> Malawi’s Expensive Mobile Habit, <http://www.bbc.com/news/world-africa-31533397>

<sup>15</sup> Malawi – Telecoms, Mobile and Broadband Statistics and Analyses, <https://www.budde.com.au/Research/Malawi-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses>

<sup>16</sup> Memorandum on the Malawi Communication Act, 1998: <https://www.article19.org/data/files/pdfs/analysis/malawi.bro.03.pdf>

<sup>17</sup> Internet Usage and Population Statistics for Africa: <https://www.internetworldstats.com/africa.htm#mw>



### 3.3 Political Environment

Malawi is a landlocked country in Southern Africa, bordering Zambia, Tanzania, and Mozambique, with an estimated population of 18.6 million people.<sup>20</sup> Since the 1994 ouster of the country's founding president, Hastings Kamuzu Banda who held power for 31 years, Malawi has held multi-party presidential and parliamentary elections every five years. The next general elections will be in May 2019 and President Peter Mutharika, who was first elected in 2014, is expected to stand for re-election. The country remains peaceful and politically stable, although the government has been widely criticised for not sufficiently fighting corruption.

Many Malawians do not feel comfortable criticising the government and thus engage in self-censorship. The government has specifically targeted online activities, including arresting three opposition members in February 2016 based on a private WhatsApp group chat and charging them with treason in October 2016, over an alleged scheme to unseat president Mutharika.<sup>21</sup> The charges were dropped in March 2017 after failure by the state to bring them to court a year after the arrests.<sup>22</sup>

<sup>18</sup> List of Mobile Network Operators in Malawi, <http://www.telcomatraining.com/list-of-mobile-network-operators-of-malawi/>

<sup>19</sup> <http://www.internetworldstats.com/africa.htm#mw>

<sup>20</sup> United Nations Population Division: <http://data.worldbank.org/indicator/SP.POP.TOTL?locations=MW>

<sup>21</sup> Freedom of the Net, Malawi 2016 <https://freedomhouse.org/report/freedom-net/2016/malawi>

<sup>22</sup> Treason charges dropped against Kabwila, two others <https://malawi24.com/2017/03/29/treason-charges-dropped-kabwila-two-others/>

## 4. Laws and Policies Affecting Privacy and Personal Data Protection

This section provides an overview of international and regional human rights instruments as well as national laws and policies relevant to privacy and data protection. It highlights sections of these laws and how they define and limit the right to privacy.

### 4.1 International Human Rights Instruments

Malawi has ratified two key United Nations instruments - the Universal Declaration of Human Rights (UDHR), and the International Convention on Civil and Political Rights (ICCPR). It has also ratified the African Charter on Human and Peoples' Rights (ACHPR) and Protocol on the Establishment of African Court on Human and Peoples at the continental level.

However, Malawi is yet to sign the African Union Convention on Cyber Security and Personal Data Protection.<sup>23</sup> While it has been taking part in Universal Periodic Review (UPR) process, which also involves local CSOs and the Malawi Human Rights Commission, no submissions on data protection have been made. The last review in 2015 covered broad topics such as women's rights, gender and child rights; civil and political rights; cooperation with the UN treaties bodies and special procedures; national institutions; refugees and stateless persons; and economic, social and cultural rights.<sup>24</sup>

### 4.2 The Constitution of Malawi

The right to privacy is provided for in the Malawi constitution (as amended), specifically, Article 21 states that:

“Every person shall have the right to personal privacy, which shall include the right not to be subject to –

- a. searches of his or her person, home or property;
- b. the seizure of private possessions; or c. interference with private communications, including mail and all forms of telecommunications.

There are also constitutional guarantees for the right to freedom of expression (Article 35); freedom of the press to report and publish freely, and to be accorded the fullest possible facilities for access to public information (Article 36); as well as the right of access to information held by the State or any of its organs at any level of Government in so far as such information is required for the exercise of his rights (Article 37).

<sup>23</sup> African Convention on Cyber Security and Personal Data Protection, [https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

<sup>24</sup> Malawi Accepts 132, Rejects 41 Human Rights Recommendations – 2015 UPR Review, <http://www.mw.one.un.org/malawi-accepts-132-rejects-41-human-rights-recommendations-2015-upr/>



### 4.3 Recognition of Privacy and Personal Data Protection in Statutes

Despite having a constitutional provision on privacy, Malawi does not have a data protection law. In March 2018, the Minister of Information and Communication Technology, Nicholas Dausi, announced the government's plans to enact a data protection law, though he did not indicate when the law was likely to be introduced.<sup>25</sup> The minister stated that this would be in response to the changing media and technological landscape. Nonetheless, Malawi has a number of laws that contain provisions on privacy and data protection.

#### 4.3.1 Electronic Transactions and Cyber Security Act, 2016

This Act<sup>26</sup> is the closest that Malawi has to a data protection law. It defines personal data as "any information relating to an individual who\_\_ (a) may be directly identified; or (b) if not directly identified, may be identifiable by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social, or economic identity;" this law defines a data subject as "a person from whom data relating to that person is collected, processed or stored by a data controller."

According to Section 3(c), one of the objectives of the Act is "to put in place mechanisms that safeguard information and communication technology users from fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of information and communication technology."

Under Part VII, the act provides for the processing of personal data (Section 71); and the rights of data subjects including rectification of complete erasure of personal data held by the data controller (Section 72). Section 73 requires data

controllers to provide a data subject from whom data relating to himself is collected with (a) the identity of the data controller and of his representative, if any; (b) the purposes of the processing for which the data is intended; (c) the existence of the right of access to and the right to rectify the data concerning him; and (d) the existence of the right to object to the processing of the data concerning him.

Additionally, Section 74 requires data controllers to ensure that clients' data is secure and is protected against accidents or unlawful destruction of accidental loss, alteration, unauthorised disclosure or access by third parties, especially if the processing involves the transmission of data over a network..." Under Section 83, the Act criminalises unauthorised access to, or interception (Section 84(3), or interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, with conviction attracting fines of K2,000,000 (USD 2,680) and to imprisonment for five years.

<sup>25</sup> Data Protection Law on the Cards, <https://www.mbc.mw/index.php/news/sports/item/6016-data-protection-law-on-the-cards>

<sup>26</sup> The Malawi Gazette Supplement, dated 4th November, 2016, containing Acts, <http://www.maca.org.mw/wp-content/uploads/2014/07/E-Transactions-Act-2016.pdf>

### 4.3.2 The Communications Act of 2016 <sup>27</sup>

Under section 176(1), the Act criminalises unlawful interception or interference by service providers, noting that, “A licensee operating an electronic communications network or providing an electronic communications service who, other than in the course of its duty, intercepts, interferes with the contents of, or modifies, any message sent as part of the electronic communications service, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 (USD 6,500) and imprisonment for five years.”

Section 176(2) further states that, “A person who, without lawful authority under this Act or any other written law\_\_\_

- a) intercepts, attempts to intercept, or causes any other person to intercept or to attempt to intercept, any communications;
- b) discloses or attempts to disclose to any person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this Act; or
- c) uses or attempts to use the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this Act, commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and imprisonment for five years.

### 4.3.3 Access to Information Act, 2016 <sup>28</sup>

This Act provides for the right of access to information in the custody of public bodies and relevant private bodies as well as the processes and procedures for obtaining such information. Section 20(1) requires an information holder to notify third parties, if he considers that the information being requested relates to confidential or commercial interest, in writing with details of the request. Third parties are required to respond in writing within 10 working days from the date of receipt of the notice and indicate whether they consider the information to be confidential and give reasons why the information should not be disclosed.

The Act also prohibits information holders from disclosing information whose disclosure would result in the unreasonable disclosure of personal information about a third party (Section 29) or which is likely to result in endangering the life, health or safety of a person (Section 31). On the other hand, information holders are prohibited from disclosing legally privileged information unless the data subject (patient, client, source or person entitled to the privilege), consents to the release of the information or has waived the privilege or a court order is made to that effect (Section 32).

<sup>27</sup> Malawi Communications Act 2016, <http://www.macra.org.mw/wp-content/uploads/2014/07/Communications-Act-2016.pdf>

<sup>28</sup> Malawi Access to Information Law, <https://www.right2info.org/laws/malawiaccessinfo.pdf>

#### 4.3.4 National Statistics Act 2013 <sup>29</sup>

Section 10 of the National Statistics Act, 2013 empowers the National Statistics Organisation (NSO) to collect all types of information, including personal information, nationwide on behalf of the government. Under section 10(3) “a person, on being required to give information ... shall, to the best of his knowledge, information and belief, complete forms, make returns, answer questions and give all necessary information, in the manner and within the time prescribed or as the Commissioner may direct.

Section 12(11) of the Act states that the Commissioner or any authorised officer may, for any purpose connected to collecting statistical information, enter and inspect any land, building or other premises, vehicle, vessel or aircraft. But they can only enter such areas with the consent of property owners or the backing of a warrant; and they are enjoined to maintain decency and order, including the protection of a person’s right to dignity, freedom and privacy, under section 12(5).

<sup>29</sup> National Statistics Act, 2013, [http://www.nsomalawi.mw/images/stories/data\\_on\\_line/general/National%20Statistics%20Act%202013.pdf](http://www.nsomalawi.mw/images/stories/data_on_line/general/National%20Statistics%20Act%202013.pdf)

## 5. Results, Challenges and Trends

### 5.1 Limited Understanding of Privacy

The study found that there is limited understanding of the concept of privacy among several Malawians. This is because the concept of privacy does not carry the same meaning in local languages as it does in English. For example, translating “privacy” into one of Malawi’s main languages, Chichewa, which is spoken by over 57%<sup>30</sup> of Malawians, the term tends to have negative connotations. In Chichewa privacy could literally be translated as kuchita zinthu mchibisibisi (which means doing things in secrecy), which is generally frowned upon in Malawian culture.

Additionally, the concept of privacy is considered elitist, as exemplified by a respondent from the Media Institute of Southern Africa (MISA), who noted that “only those who are knowledgeable and literate would care about such issues. I am convinced that most people who do not know about data protection would not care at all.” A research participant at mHub Malawi similarly observed that “very few Malawians care about issues of privacy and data protection”, adding that this could be seen from how freely and carelessly they share sensitive data on social media platforms.

### 5.2 Weak Policy and Legal Frameworks

#### 5.2.1 Absence of a Comprehensive Data Protection Framework

The major weakness of the current legal and policy framework is the lack of a stand-alone privacy and data protection law. This is especially problematic at a time when there has been an escalation of personal data collection in the country, such as the on-going mandatory SIM card registration as well as biometric national identity cards registration exercises, which are also a key to electoral voter registration. Similarly, national and multinational companies such as banks and telecommunication companies are allowed to collect data of their own.

#### 5.2.2 Fragmented Oversight Over Privacy and Data Protection

Due to lack of a comprehensive data protection law, Malawi does not have a single body that regulates the collection of personal data in the country. MACRA is responsible for the implementation of the Electronic Transactions Act, which is the de-facto law on privacy and data protection.

<sup>30</sup> Malawi, <https://en.wikipedia.org/wiki/Malawi>

Unfortunately, the current setup of data protection laws does not provide enough safeguards for users' personal data. This is because the Electronic Transactions and Cybersecurity Act which provides for data protection was drafted specifically for electronic communication and commerce. Section 6(1) of the Act establishes the Malawi Computer Emergency Response Team (CERT) as a unit under MACRA. Section 6(2) provides that the "Malawi CERT shall take charge of its information infrastructure protection actions and serve as a base for national coordination to respond to information and communication technology threats." Section 4 of the Act stipulates that it is the duty of MACRA to ensure that the Malawi CERT executes several services. However, almost two years since the Act came into force, the Malawi CERT is not yet operational. In March 2018, MACRA Director of Finance, Ben Chitsonga told the local media<sup>31</sup> that the communications regulator had engaged experts from the International Telecommunication Union (ITU) to help get Malawi CERT off the ground.

Some organisations, businesses, as well as government departments have their own internal policies which guide data handling and cater for privacy issues. For instance, a research participant working with Standard Bank pointed to the privacy and security statement on their website.<sup>32</sup> The statement includes measures such as third party policies; mail, email or SMS promotions; cookies; storing personal information; when disclosing personal information without consent; and the right to amend the privacy and security statement. Other big businesses and companies such as Airtel,<sup>33</sup> TNM,<sup>34</sup> MTL,<sup>35</sup> EcoBank<sup>36</sup> and insurance companies such as Old Mutual<sup>37</sup> have similar privacy and data policies.

These privacy policies are provided at the local level but what is not clear is how international companies and business such as South African owned NedBank,<sup>38</sup> Eco Bank,<sup>39</sup> Standard Bank,<sup>40</sup> and Airtel Malawi owned by Bharti Airtel<sup>41</sup> handle locally collected data given that these companies are headquartered elsewhere. There is a need to have clear policy guidelines on this.

### 5.3 Data Collection Programmes by Governments

Government departments such as the National Statistics Organisation (NSO), Immigration, Road Traffic Directorate and service providing institutions such as hospitals and educational centres, as well as banks traditionally collect vast amounts of personal data. Recently, telcos have been collecting a lot of personal data, more so with the introduction of the mandatory SIM card registration. the Communications Act of 2016, which requires all SIM cards in Malawi to be registered on a central database a customer's national identity number needs to be verified when purchasing, replacing, or swapping a SIM card. However, there is no readily available data on how much information each of these bodies collects, or how well they are complying with existing laws on the collection, processing and sharing of personal information.

<sup>31</sup> Malawi Moves to Secure its Cyber Space, <https://mwntation.com/malawi-moves-secure-cyber-space/>

<sup>32</sup> Privacy and Security Statement, <https://www.standardbank.co.mw/Malawi/About--Us/Footer/Privacy-and-security-statement>

<sup>33</sup> Airtel Terms and Conditions, <http://www.africa.airtel.com/wps/wcm/connect/africaRevamp/malawi/home/terms>

<sup>34</sup> TNM Privacy Policy, <http://www.tnm.co.mw/privacy-policy>

<sup>35</sup> Privacy Policy for Malawi Telecommunication Limited (MTL) <http://www.mtl.mw/index.php?page=privacy>

<sup>36</sup> EcoBank Privacy Policy, <https://ecobank.com/mw/personal-banking/privacy-policy>

<sup>37</sup> Old Mutual Privacy Policy, <https://www.oldmutual.com/privacy-notice>

<sup>38</sup> NedBank Group Business Summary, <http://www.4-traders.com/NEDBANK-GROUP-LTD-1413393/company/>

<sup>39</sup> EcoBank History, <https://ecobank.com/group/about-us>

<sup>40</sup> Standard Bank Group Limited, <http://www.4-traders.com/STANDARD-BANK-GROUP-LTD-1413410/company/>

<sup>41</sup> Bharti Airtel, <https://www.airtel.in/about-bharti/about-bharti-airtel>

The National Registration Bureau (NRB) is mandated by National Registration Bureau Act of 2010 to implement, coordinate, manage and maintain the National Registration and Identification System (NRIS) in Malawi. The bureau collects data for Birth Certificates; National Identity Cards for Malawians; Identity Cards for foreigners; Certificate of Registration of Marriage and Death Certificates.<sup>42</sup> There is also Malawi Electoral Commission (MEC), which i conducts voter registration and manage the voters' registration roll."

The (NSO)<sup>43</sup> collects mandatory data on behalf of the government, for all the types of national statistics. Meanwhile, the Department of Road Traffic (Road Traffic Directorate)<sup>44</sup> and Department of Immigration<sup>45</sup> are mandated to issue various documents, such as driving licenses, passports and other travel documents.

In 2017 the government started the National Registration and Identification System (NRIS) for all citizens aged 16 years and over. The government introduced NRIS in order "to address problems associated with lack of universal and compulsory registration." The Government said this would be achieved through "the registration of births, adults, marriages, resident foreigners and deaths."<sup>46</sup>

Even though these programmes have seen a huge amount of personal data being collected, the initiatives have not met notable resistance or questions on data protection, despite their large-scale implementation and possible impacts.

### 5.3.1 Mandatory SIM Card Registration

The mandatory SIM card registration is provided for under Section of 92(1) of the Electronic Transaction Act. It provides that:

***a person who uses a generic number or owns or intends to use a SIM card for voice telephony services shall register that generic number or SIM card with any electronic communications licensee or with the distributor, agent or dealer of the electronic communications licensee, authorised to provide or sell generic numbers or SIM cards.***

The exercise which was announced in June 2017<sup>47</sup> was suspended in February 2018, over what the Minister of Information said was lack of civic education, but the suspension was lifted two weeks later.<sup>48</sup> Unlike the minister's explanation, the broader issue to the suspension was to address the rumours that government surveillance was the aim of the registration exercise.<sup>49</sup> Many saw the SIM card registration process as part of the government's efforts to control electronic crimes, which had increased given the number of phone-based money platforms.

<sup>42</sup> National Registration Bureau: Mandate and Vision, <http://www.nrb.gov.mw/index.php/about-us/mandate-vision>

<sup>43</sup> National Statistics Office, [http://www.nsomalawi.mw/index.php?option=com\\_content&view=article&id=34&Itemid=5](http://www.nsomalawi.mw/index.php?option=com_content&view=article&id=34&Itemid=5)

<sup>44</sup> Department of Road Traffic (Road Traffic Directorate), <http://www.motpwh.gov.mw/index.php/roads/road-traffic/79-departments>

<sup>45</sup> Department of Immigration, Republic of Malawi, <http://www.immigration.gov.mw/about-us/main-functions/>

<sup>46</sup> National Registration and Identification System (NRIS), <http://www.nrb.gov.mw/index.php/about-us/strategic-plan/item/3-the-national-registration-identification-system-nris-for-malawi>

<sup>47</sup> Malawi Start Mandatory SIM Card Registration, <https://www.mbc.mw/index.php/news/sports/item/4597-malawi-starts-mandatory-sim-card-registration>

<sup>48</sup> Malawi Government Lifts Suspension on SIM Card Registration,, :

<https://www.capitalradiomalawi.com/index.php/blog/local-news/capital-news/item/9083-malawi-government-lifts-suspension-of-sim-card-registration>

<sup>49</sup> Malawi suspends SIM card registrations citing "state spying" concerns, <https://www.iafrikan.com/2018/02/16/malawi-sim-card-registration-spying/>

## 5.4 Enhanced State Surveillance Capacity

In 2011, the Malawian regulator, MACRA, procured the Consolidated ICT Regulatory Management System (CIRMS) to enable the regulator monitor service providers for quality of service and fair pricing.<sup>50</sup> The implementation of the CIRMS, locally known as the “Spy Machine”, faced a challenge in court from telecom operators and Civil Society Organisations (CSOs), who feared that it would be used by state organs to eavesdrop on private communications, compromise the telcos’ obligations of ensuring privacy of subscribers, and violate article 21 of Malawi’s constitution.<sup>51</sup>

In October 2011, the High Court ruled in favour of the applicants, but on appeal the decision was overturned in favour of MACRA in September 2014. In April 2015, an application for review of MACRA’s decision to start using the machine was made at the High Court by Telekom Networks Malawi Limited (TNM), arguing that there was no framework to protect customer confidentiality and that it should not therefore implement the machine. In June 2017, the Supreme Court of Appeal ruled in favour of MACRA with a proviso that the system should not be connected to access content.<sup>52</sup> Following the decision, MACRA installed the system which has been operational since September 2017.<sup>53</sup>

## 5.5 Legal Responsibility of Business Entities

Under section 29(1) of the Electronic Transactions and Cybersecurity Act, an intermediary service provider is mandated to maintain and preserve the data that permits the identification of any person who contributed to the creation of all or part of the content relating to the services rendered by such intermediary service provider. Section 29(2) states that the High Court may require from the intermediary service provider communication of this data.

Section 30(1) of the Act requires that an intermediary service provider offering access to online publication communication services provide and inform its subscribers of the existence of any technical means that permit restriction of access to certain services. Section 30(2) states that an intermediary service provider shall set up an easily accessible and visible system to enable any person to inform the intermediary service of any content which is unlawful or infringes, or may infringe, on such person’s rights.

Section 31(1) provides that an online content provider shall display in a conspicuous manner, the following information on its webpage:

- (a) in case of a natural person, full name, domicile, telephone number, and email address, of the editor;
- (b) in case of a legal entity, corporate name, postal and physical address of the registered office, telephone number, email address, authorised share capital, and registration number, of the editor;
- (c) where applicable, the name of the corporate officer appointed as director of the publication of the online public communication and the editor in chief; and,
- (d) the name, title, corporate name, postal and physical address and telephone number, email address of the intermediary service provider prescribed in this section.

<sup>50</sup> ‘Spy machine’ roll out in September, says Malawi regulator, <https://www.nyasatimes.com/spy-machine-roll-september-says-malawi-regulator/>

<sup>51</sup> “Spy Machine” Brings Telecoms Fears: <http://www.biztechafrika.com/article/spy-machine-brings-telecoms-fears/1437/>

<sup>52</sup> Court Nods to Macra’s “Spy Machine”: <http://mw-nation.com/court-nods-to-macra-spy-machine/>

<sup>53</sup> Macra Unleashes Spy Machine: <http://zodiakmalawi.com/top-stories/macra-unleashes-spy-machine>

On the other hand, however, under Section 67(1) service providers of encryption services shall declare to the Authority the technical characteristics of the encryption means as well as the source code of the software used.

Should data breaches occur, a convicted person would be fined K2,000,000 and imprisoned for five years, as provided for under Section 84 of the Electronic Transactions and Cyber Security Act. " Section 84(4) provides that, "Any person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, commits an offence and shall, upon conviction, be liable to a fine of K2,000,000 and to imprisonment for five years."

Targeted and indiscriminate communication is not widespread in Malawi, mobile phone companies tend to send promotions and other unsolicited messages to their subscribers in the name of updating their customers on new services.

## 5.6 Dispute Resolution and Remedies

### 5.6.1 Existing Frameworks for Redress

According to Section 96, any person or any interested organisations whose members are affected by a criminal offence defined under this Act may lodge a complaint to the Authority which shall direct a cyber inspector to assess the relevance of the complaint and, if the complaint is considered relevant and reasonable, proceed with investigations.

### 5.6.2 Notable Campaigns and Decisions

There has been a case where an unlikely alliance of CSOs and telcos emerged to raise concerns on privacy issues. This was when the Malawi government through the telecoms regulator MACRA, wanted to introduce the Consolidated ICT Regulatory Management System (CIRMS)<sup>54</sup> to help the regulator to monitor the quality of service, among other things. The CSOs argued that CIRMS would enable the government to eavesdrop on people's personal communication and that it represented an infringement on people's privacy, contrary to article 21 of the Constitution.

The telecommunication companies opposed installation of the system as it was aimed at monitoring their services and would give the regulator important information on their operations.<sup>55</sup> The case of the CSOs was mostly informed by the lots of tension between CSOs and the government,<sup>56</sup> which raised suspicion that by introducing the CIRMS, the government was keen to improve surveillance capacity which it could use against the political opposition and critical activists and the media. Ultimately, the courts of law ruled in favour of installing the system. The positive experience of CSOs working with telecom companies has not been seen again.

In a separate incident, in March 2017 nude photos of a trainee police woman were leaked on Facebook before going viral on other social media networks.<sup>57</sup> The pictures were taken for her personal use at a police-training base. The woman was fired from the police, but she won a case for a right to appeal against the dismissal after seeking redress from Malawi Human Rights Commission (MHRC).<sup>58</sup>

<sup>54</sup> MACRA Courts Media on "Spy Machine", <http://www.bizcommunity.com/Article/129/78/66853.html>

<sup>55</sup> Malawi Telecom Operators Fight Regulator on CIRMS, <http://www.communicationsafrica.com/security/malawi-telecom-operators-fight-regulator-on-cirms>

<sup>56</sup> Malawi: Confusion and Uncertainty Over August 17 Vigil, <https://globalvoices.org/2011/08/16/malawi-confusion-and-uncertainty-over-august-17th-vigil/>

<sup>57</sup> Nude Photos of Malawi Police Woman Cause Stir, Fired, <https://www.nyasatimes.com/nude-photos-malawi-police-woman-causes-stir-fired/>

<sup>58</sup> MHRC Faults the Firing of a Woman Who had Her Photos Leaked, <http://www.maravipost.com/mhrc-report-faults-firing-police-woman-nude-pics-leaked/>



## 6 Conclusion and Recommendations

---

### 6.1 Conclusion

The major issue in Malawi currently is the lack of a specific law on privacy and personal data protection. The findings show that despite the constitutional guarantees for the right to privacy, the country is yet to enact a comprehensive law to operationalise this right. Findings further show that because of these fragmented provisions in the different laws, there is no single body within the country that is mandated with regulating the collection of personal data. Additionally, many Malawians do not fully understand the concept of privacy and are often not keen on protecting their data. The lack of the law has been a keener concern over the past two years as there has been a huge increase in personal data collection through the introduction of mandatory SIM card registration and biometric national identity registration for Malawians who are 16 years or older.

While it is true that processes such as SIM card registration could help curb certain forms of criminal activity, this should not come at the expense of protecting other human rights. The government needed to have a robust data protection law in place before embarking on such mandatory data collection exercises. New technologies come with new challenges and in order to protect citizens, the government has the duty to ensure an appropriate legal framework is in place. Also, it is very important for the country to ensure that security service personnel are fully aware of the existing laws on privacy and personal data protection. It is also imperative to ensure that such laws are operational and are implemented as expected.

## 6.2 Recommendations

### Government should:

- Progressively adopt and implement policies and legislation aimed at achieving essential goals in society as provided under the constitution's Article 21 (privacy), Article 35 (freedom of expression) and Article 37 (access to information).
- Ensure that new laws do not create new problems. Laws must be made to protect public and private interests and not just the interests of the state.
- Put in place a data protection law because such a law is important for protecting other fundamental rights and freedoms as enshrined in the Malawi constitution's Bill of Rights. It is also important to protect citizens from unscrupulous business people and criminals, who might want to steal people's money and identity.
- Ensure that laws are updated regularly to keep up with changing technologies. and that they promote the uptake of new technologies.
- Government must be a party to progressive international agreements and treaties aimed at protecting people's rights and freedoms, including the right to privacy and personal data protection.

### Business should:

- In the absence of data protection laws, companies must take steps to have their own in-house policies to protect people's data and privacy.
- Companies must make their privacy and data handling procedures open and publicly available.
- Companies should support consumers to make informed decisions about their data and information.

### Media

- Given that many Malawians do not fully appreciate the importance of privacy and data protection laws, the media has a huge role in civic education and awareness on issues of data protection.
- The media must not themselves encourage sharing and dissemination of information comprising people's personal and private information. This has often been the case, especially with online publications.
- The media must realise that publishing online does not mean disregarding ethical considerations, which are hallmarks of good media practice, online and offline.

### Academia

- Academics have the responsibility of intellectual leadership and guidance in society. Through research and outreach, academics are well equipped to point out the dangers of ignoring important issues such as that of privacy even though these issues may seem as unimportant to for populist stakeholders and politicians whose main goal is to win popularity.

### Civil Society

- The CSOs should be vigilant in protecting people's basic freedoms and rights, online and offline, including government about the need to enact a progressive law to protect privacy and personal data.
- The CSOs should actively demand that the Malawi government sign ups to progressive international instruments on freedom of expression, privacy and personal data protection, and ensure that the government lives up to its obligations in line with these instruments.
- Civil society should also take a leading role in creating awareness among different stakeholder groups, including policy makers, businesses, and ordinary citizens, of the need to protect privacy and personal data.



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.

Tel: +256 414 289 502 | Mobile: +256 790 860 084, +256 712 204 335

Email: [programmes@cipesa.org](mailto:programmes@cipesa.org)

Twitter: [@cipesaug](https://twitter.com/cipesaug)

Facebook: [facebook.com/cipesaug](https://facebook.com/cipesaug)

[www.cipesa.org](http://www.cipesa.org)