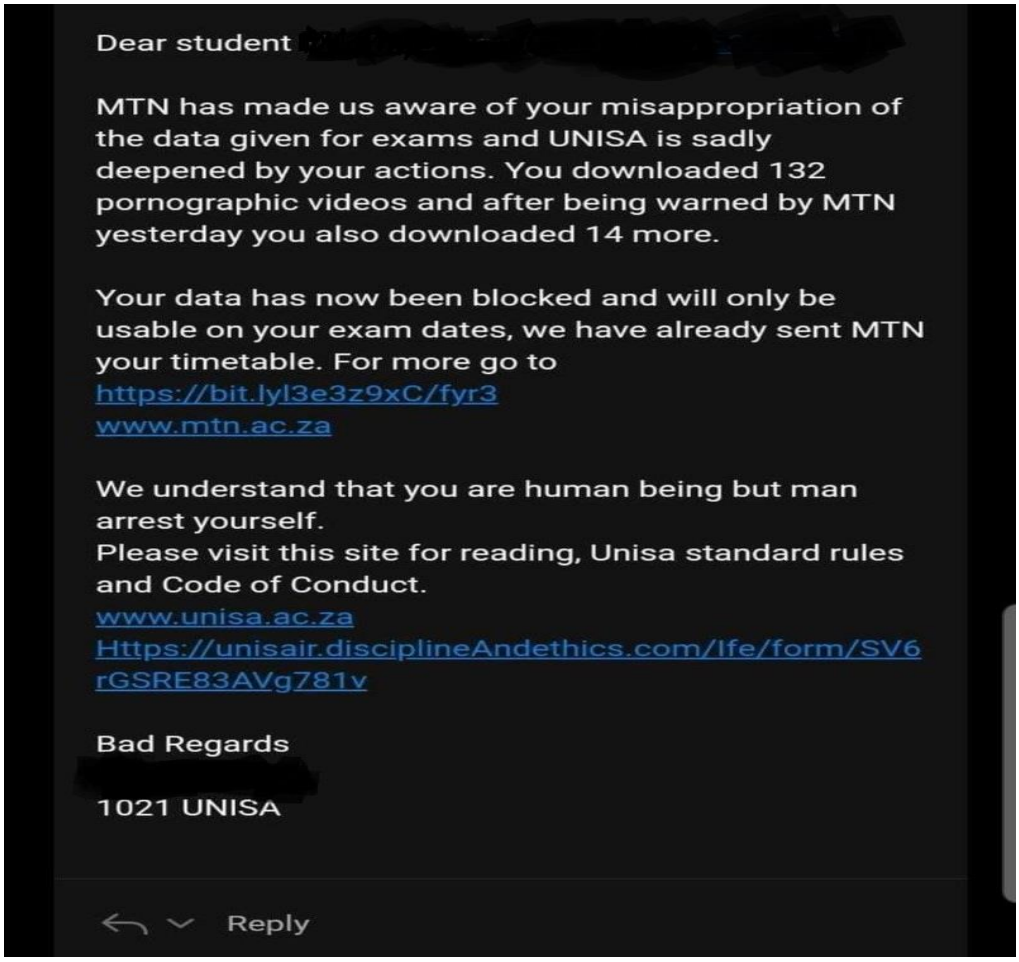
(Un)acceptable use of free data allocated to students by the Government during COVID-19

Masego Morige BCom (MGI)
Paralegal at Snail Attorneys @ Law inc
E-mail: masego@snailattorneys.com



1. INTRODUCTION

The above excerpt is a screenshot that has made the rounds on various social media platforms across the internet space in South Africa. While there may be a glaring question as to the legitimacy of the screenshot or the purpose of its dissemination on social media, this is not the subject of discussion in this article.

What is briefly interrogated here is the inherent concerns on the Right to Privacy – its application to the facts contained herein as well its limitations; the application of South African CyberLaws including the current Common

Law, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 200, and the Protection of Personal Information Act, 4 of 2013 (the POPIA); the relationship between the various stakeholders (the Government, academic institutions, students and telephony service providers); and the effect COVID-19 on all the aforementioned facets of the discussion.

2. COVID-19 AND THE FOURTH INDUSTRIAL REVOLUTION (4IR)

The transition of industry from the use machinery, electricity, electronics and internet is a dynamic process which may not unfold unaffected by nuances in life as experienced by ordinary people in everyday life. The worldwide pandemic known as COVID-19 is one such phenomenon. The reality for students across various institutions, since the national lockdown, is that online learning has become an integrated form of education (Ghilay, Y 'Online Learning in Higher Education' 2017). The usefulness of information technology in this age therefore extends beyond social interaction, maintaining familial relationships through online communication or securing personal information by means of features of artificial intelligence.

The need for online learning presents a few realities for students: Firstly that one must possess or have access to a computer or electronic device to access online course material, announcements and various communications with academic staff and fellow students. Secondly and more importantly, the said computer or electronic device must be capable of connectivity to the internet where various information and platforms are hosted. What would appear to be commonplace amongst students is, under circumstances where a student does not have access to these for any reason whatsoever, if they are within close proximity to the institution's premises it becomes easier for them to access the aforementioned materials. (Ghilay, Y 'Online Learning in Higher Education' 2017)

Students find alternative ways to access such materials if they find themselves unable to physically be present at the institution's premises, such as internet cafes, areas with free / open source wireless connections and various other means. With the spread of the corona virus in the wake of 2020 in South Africa, it became necessary for the government to issue Regulations in accordance with the provisions of the Disaster Management Act, 57 of 2002. Effectively this implied that movement became restricted for South African citizens, and consequentially access not only to basic services for all South Africans, but also for students to study materials. (Ghilay, Y 'Online Learning in Higher Education' 2017)

3. ALLOCATION OF MOBILE DATA TO STUDENTS DURING COVID-19 LOCKDOWN

The South African government during the course of May 2020, in order to meet some of the challenges experienced by students, commissioned various telephony / network service providers to allocate mobile data to students registered at institutions of higher learning who fell within the financial assistance of the National Student Financial Aid Scheme (NSFAS). (Pillay, V 'Blade Nzimande: 10GB data for NSFAS students for 3 months' *Independent Online* 23/5/20 accessed at https://www.iol.co.za/news/politics/blade-nzimande-10gb-data-for-nsfas-students-for-3-months-48430335 on 3rd June 2020).

The screenshot shown above demonstrates that the data allocated to students was possible of being used for purposes alternative to study. There are, however, legal questions that arise in relation to the message sent to the student apparently from an employee of the academic institution. The first question is, does the government's allocation of data to students justify monitoring activities occurring on students' personal devices? The second question is, to what extent has the government, in conjunction with the telephony / network service providers processed the students' personal information?

The third question flowing from this, is whether or not data protection and privacy laws have been observed by the government and the telephony / network service providers in processing the personal information? The fourth question is, what constitutes acceptable use of the data allocated by the government? In seeking clarity on these questions, this article takes a brief concise survey of the common law, the POPIA, the Promotion of Access to Information Act, 2 of 2000, the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 and the Constitution of the Republic of South Africa, 1994.

4. LAWFUL AND REASONABLE MONITORING OF ONLINE ACTIVITIES

The primary source of law on issues pertaining to the interception and monitoring of the activities of persons within the Republic of South Africa is the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002. The court in *Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others* (*Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019) highlighted the fact that controversy surrounding the Act is that its application entails a balancing of the following Constitutional rights:

- *The right to privacy as contained in terms of Section 14;*

- *The right to freedom of expression and media in terms of Section 16(1);*
- *The right of access to the courts in terms of Section 34; and*
- *The right to a fair trial in terms of Section 35(5).*

While the Court in the aforementioned case concerned itself, to some degree, with the Constitutionality of the Act, the present discussion requires an enquiry into what circumstances justify monitoring in terms of RICA. Section 2 of RICA creates a general prohibition on the monitoring of communications, however, as with any general rule or prohibition, there exist exceptions. These exceptions are contained in Sections 3 – 11 of the Act. The Act sets out that a prohibition on interception and monitoring of communications may be allowed under the following circumstances ("RICA: walking a fine line between crime prevention and protection of rights." De Rebus, Jan/Feb 2014:30 [2014] DEREBUS 6):

1. *a directive has been granted that permits the above prohibited activities;*
2. *the party protected by RICA gives requisite consent;*
3. *the entity engaging in the above activity was also a party to those communications;*
4. *intercepting, monitoring or disseminating information of an employee while carrying on a business;*
5. *interception to prevent serious bodily harm;*
6. *interception to determine a location during an emergency; or*
7. *when entitled to do so in terms of other legislation.*

When one considers the purpose for which the mobile data was provided to students, it can be expected that a level of accountability is required from the student. In other words, it would be unsurprising for the Government or the Fund to justify its monitoring of the activities of students online by articulating the reason that it may have sought to implement some measure of accounting to ensure that the data was indeed being used for the purposes of study.

Furthermore, it appears that the last of the exceptions listed above is applicable in this matter in that the accessing the cellphone records and specifically engaging the student on the personal use of his mobile or other technological device entails the processing of personal information. This is a scenario falling within purview of the right to privacy, and as such it falls with the ambit of the provisions of the POPIA.

5. THE PURPOSE AND EXTENT OF PROCESSING STUDENTS' PERSONAL INFORMATION

Prior to the provision of funding by the NSFAS, students, their legal guardians or spouse enter into a written agreement with the Fund in terms whereof they *inter alia* provide their consent for the processing of their personal information (FN: NSFAS BURSAY AGREEMENT TERMS AND CONDITIONS available at https://www.nsfas.org.za/content/downloads/NSFAS%20Bursary%20Terms%20and%20Conditions.pdf, accessed on 3/6/20). In particular, clause 7.1.3.1 provides the following

> *"the processing of the student's personal information as may be required to enforce or otherwise give effect to the Bursary Agreement and any other agreement or arrangement concluded between the student, NSFAS or any other third party contemplated herein or required to give effect to the matters contemplated in the 'Bursary Agreement', including but not limited to the processing of personal information by NSFAS and by a third party NSFAS-Wallet vendor and other participants under NSFAS-Wallet payment platform, where applicable …"*

The agreement itself is a document indicating express, written consent by the student for his/her personal information to be processed by Fund and third parties, such as the University or the telephony company. The legal backdrop against which such an agreement ought to be read is the POPIA. This Act's purpose entails giving effect to the right to privacy by safeguarding personal information when it is processed by certain persons.

The POPIA provides some important guiding definitions on parties that may be involved in the processing of personal information. For all intents and purposes the important stakeholders identified in this scenario are data subject, a person, a responsible party and an operator. Considering that the specific wording used in the agreement between the Fund and students, it is equally important to understand what the POPIA envisaged in making reference to 'processing'. The relevance hereof lies in that essentially, data subjects (students), by entering into the said agreement are allowing a responsibility party (the Fund), as well as operators (the academic institutions and telephony networks) to process their personal information.

The technical definitions provided by the POPIA in relation to the aforementioned actors are important due to the fact that while there may not exist much casuistry in relation to privacy concerns with the direct influence or application of the POPIA, South Africa has nevertheless entered into the realm of potential disputes and litigation on the protection of the right to privacy. This is so because sections 38, sections 55 – 109, section 111 and section

114(1), (2) and (3) commenced on the 1st July 2020.

Of potential relevance to the set of facts visible upon the above extract are the sections relating to the enforcement of the Act, which entail the lodging of complaints to the Information Regulator as well as civil remedies that may be brought before the Courts. Suffice it to say that for responsible parties what is worth noting as of the 1st July 2020 is that a one-year grace period for compliance with the Act is extended and that in processing personal information, responsible parties and operators must observe the principles for the lawful processing of personal information, namely accountability, processing limitation, specific purpose, further processing limitation, information quality, openness, security safeguards and data subject participation.

Section 1 of the POPIA defines a data subject "as a person to whom personal information relates – who in the above image is the student-"; a responsible party is defined "as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information – who in relations to the article is the government institution "UNISA-""; and an operator is defined "as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party – who in the above image is MTN- ". The POPIA defines the act of processing as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.

From the above it becomes clear to appreciate who the different stakeholders are in the context of the above screenshot. Furthermore, it becomes possible to glean that the definition of what processing constitutes is a wide definition that encompasses the collection of personal information by the Fund (the responsible party), the transmission of same to the operators (the academic institution and telephony network operators), or the converse retrieval by such operators prior to the communication being sent to the student (data subject) with regards to his apparent unreasonable use of the mobile data provided by the Fund for the purpose of study. The extent of the processing therefore seems reasonable in this context.

6. CONDITIONS FOR THE LAWFULNESS PROCESSING OF PERSONAL INFORMATION

During the processing of personal information of a data subject, the responsible party must ensure that the processing complies with the 8 (Eight) Conditions for lawful processing of personal information which are provided for from Sections 8 – Section 25;

- **Accountability** – The Government Institution must ensure that it processes personal information lawfully and in good faith.
- **Process Limitation** – The Government Institution must ensure that it processes the personal information in a lawful and reasonable manner, in that it does not infringe on the privacy and dignity of the data subject, therefore a data subject may at any time object to the processing of his or her personal information should it be used *mala fide*.
- **Purpose specification** – The Government Institution may only process the personal information for the purposes directly related to the object and purpose of the students mandate at the Institution.
- **Further processing limitation** – Any further processing of the personal information of the student must be compatible with the purpose for which it was originally obtained for, which was for academic purposes
- **Information quality** – Any Institution must take practical and reasonable steps to ensure that personal information it processes is correct, up to date and complete.
- **Openness** – A student must be notified that his or her personal information is being processed by the Institution and the Network Provider in a way that will infringe on his or her dignity.
- **Security safeguards** – The Government Institution must ensure that they have adequate security measures and controls put in place to safeguard the personal information of voters against loss, damage and misuse, in case of a breach the Government Institution must notify the Information Regulator (IR) and an the affected student of any security breach.
- **Data subject participation** – The Government Institution must, upon request by a student confirm whether it is processing the personal information of a student correctly, and the information about the identities of all third parties, who have and have had access to the information.

The Government Institution did not make use of the personal information for the initial purpose it was specified for which was for academic purposes, there was a lack of Openness from the side of the institution as the student ahd no knowledge that this his privacy was being monitored in a way that the institution did, lastly the students information was not safeguarded.

7. ACCEPTABLE USE OF DATA ALLOCATED BY THE GOVERNMENT FOR ACADEMIC ACTIVITY

The practice of publishing an 'Acceptable Use Policy' is commonplace in academic as well as various other types of organizations. The general rule that can be drawn from such policies is that pornographic material is prohibited. This general rule, however, appears to have an important *caveat*, namely that the academic institution or organization generally prohibits the accessing, dissemination or otherwise use of pornographic material on its platforms, facilities and equipment such as the institution's computers or wireless networks.

According to Schmerler, one of the factors to consider when creating an 'Acceptable Use Policy' (7 THINGS TO CONSIDER WHEN CREATING AN ACCEPTABLE USE POLICY, Available at; https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/7-things-consider-creating-acceptable-use-policy/ Accessed; 08/07/20) is the purpose for which the resources are intended. It is accepted, however, that technical definitions present uncertainty. By way of example, below are direct quotes of the preamble of the University of South Africa's 'Internet, Electronic Communication and Web Management Policy' (https://www.unisa.ac.za/static/corporate_web/Content/Library/Documents/InternetElectronicCommunicationPolicy_apprvManCom_240209.pdf accessed on 14/7/20) , as well as key concepts contained in the definition section thereof:

PREAMBLE

"This policy applies to all users who have access to and/or use UNISA's communication facilities or equipment. It provides rules, standards and guidelines on the use of UNISA's communication facilities and equipment to ensure the value and integrity of UNISA's equipment and network(s)."

"COMMUNICATIONS"

"Communication facilities include internet access, email access and the use of any equipment made available by UNISA for purposes of:

a) accessing, creating, copying, distributing, sharing and deleting records

b) initiating, creating, receiving or storing communications;"

"Communications include

a) written text and verbal utterances of a user in or during a meeting where the business of UNISA or related matters are discussed,

b) the transfer of any information whether speech, data, text or images in any format through communication facilities,

c) *access to or use of the services available on the internet, including email, websites, file transfer, video conferencing, voice over Internet Protocol, chat rooms and bulletin boards by users*
through the equipment;"

This policy by UNISA becomes applicable to any data subject who makes use of the facilities provided for by the institution whether within the campus or outside of the campus, this thus limits the institution to the accessing or limiting of use of private facilities by a data subject/student. In this case this now raises a question of whether the institution can use the Acceptable Use Policy as grounds for justification for accessing the students personal information on that the data provided was resources from the Government or not?

8. PORNOGRAPHIC

"Pornographic means all the content and actions, simulated or real, graphic or written detailed in Schedules 1, 2, 6, 7 and 11 of the Films and Publications Act 65 of 1996;"

In light of the above it is, on the one hand, clear that academic institutions deem it necessary to prohibit the use of pornographic materials on their facilities and networks. On the other hand, there is an inherent uncertainty created by the fact that in the scenario depicted by the screenshot above, the student allegedly 'misappropriated data', seemingly without making use of the institution's networks, equipment or facilities. With the valid assumption that the student accessed pornographic material on a personal device, or rather on a device or network that cannot be classified as belonging to the institution, a few other legal questions arise, namely:-

1. Does accessing pornographic materials constitute the right to freedom of expression?
2. If so, is such a right absolute?

The attitude of the Courts with regards to pornography as a form of expression can be briefly demonstrated by a finding in *Case and Another v Minister of Safety and Security and Others, Curtis v Minister of Safety and Security and Others* (CCT20/95, CCT21/95) [1996] ZACC 7; 1996 (3) SA 617; 1996 (5) BCLR 608 (9 May 1996):

While I agree that one's right to privacy should be respected, this, in my view, does not mean that all pornographic or similar material warrants protection under that right or even under the wing of free expression. There seems to be considerable consensus, both here and abroad, that some forms of

> *pornography and obscene matter should not enjoy constitutional protection. In my view, children should not be exposed to or participate in the production of pornography, and that, therefore, possession by them and exposure to pornographic material should be prohibited. However, possession by adults, in the privacy of their homes for personal viewing of sexually explicit erotica, portraying nudity, sexual interaction between consenting adults, without aggression, force, violence or abuse, may not be prohibited, for the benefit of those who derive pleasure in viewing such material*.

While there are various debates around the use of pornography in various settings, it should be noted that while freedom of expression, even in the context of using, viewing, downloading or accessing pornographic material at one's own home is a consideration the Courts make as an aspect of the right to privacy. Furthermore, it is trite that the rights contained in the Bill of Rights are not absolute and as such they may be limited in terms of Section 36 of the Constitution. The nature and extent of limitation of the right to freedom of expression through downloading pornographic material using mobile data provided by a public fund intended for the purposes of study is not the strictly legal enquiry of this article, but rather an academic analysis.

9. CONCLUSION

It is therefore opined that there may be a legally justified limitation of the student's right to view or download pornography on the MTN network, which is an operator having been acquired to provide a service to the NSFAS, which is a responsible party extending a grant to students who are data subjects making use of such a service for the intended purpose of study at academic institutions, who are operators, regardless of the fact that the students did so in the privacy of their own homes and on their personal devices. The rights at play in this scenario include the right of access to information, the right to freedom of expression as well as the right to privacy and the protection of personal information. A holistic view of the application of available legal instruments to these rights entails a balancing act in light of the Constitution of the Republic of South Africa.

When a student or the member of any organization signs over consent to his or her personal information being processed by a responsible party, it is important for them to understand the implications and extent of such processing in terms of the POPIA. This is crucial in that what unfolds thereafter is an interplay between the individual's rights to privacy, freedom of expression and the rights of a responsible party and/or operator in terms of RICA, PAIA and the limitation clause contained in the Constitution of the Republic of South Africa.

REFERENCES

ACTS OF PARLIAMENT & THE CONSTITUTION

Constitution of the Republic of South Africa, 1994

Disaster Management Act, 57 of 2002

Personal Information Act, 4 of 2013

Promotion of Access to Information Act, 2 of 2000,

Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002

CASE LAW

Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP) (16 September 2019)

Case and Another v Minister of Safety and Security and Others, Curtis v Minister of Safety and Security and Others (CCT20/95, CCT21/95) [1996] ZACC 7; 1996 (3) SA 617; 1996 (5) BCLR 608 (9 May 1996)

ONLINE SOURCES

Schmerler, B '7 THINGS TO CONSIDER WHEN CREATING AN ACCEPTABLE USE POLICY', available at; https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/7-things-consider-creating-acceptable-use-policy/

Ghilay, Y 'Online Learning in Higher Education' 2017 available at

https://www.researchgate.net/publication/313030748_Online_Learning_in_Higher_Education

NSFAS BURSAY AGREEMENT TERMS AND CONDITIONS available at https://www.nsfas.org.za/content/downloads/NSFAS%20Bursary%20Terms%20and%20Conditions.pdf

Pillay, V 'Blade Nzimande: 10GB data for NSFAS students for 3 months' Independent Online 23/5/20 accessed at https://www.iol.co.za/news/politics/blade-nzimande-10gb-data-for-nsfas-students-for-3-months-48430335

Luck, R "RICA: walking a fine line between crime prevention and protection of rights." De Rebus, Jan/Feb 2014:30 [2014] DEREBUS 6, available at http://www.saflii.org/za/journals/DEREBUS/2014/6.html

University of South Africa's 'Internet, Electronic Communication and Web Management Policy' (https://www.unisa.ac.za/static/corporate_web/Content/Library/Documents/InternetElectronicCommunicationPolicy_apprvManCom_240209.pdf