PO Box 11618, Windhoek
Tel.: (+264)811460814
eben@isgnamibia.com

LAWS ON DATA PROTECTION, INTERCEPTION OF COMMUNICATION AND CYBER CRIME IN NAMIBIA:

ARE WE HEADING TOWARDS A SURVEILLANCE FUTURE?

An analysis of relevant bills and statutes. Namibia is in danger of becoming a surveillance state - in breach of Article 13 of the Namibian Constitution which guarantees privacy of a person's correspondence and communication and provides for protection against extra-judicial searches.

5 June 2023

This document was funded through voluntary contributions by members of EPRA.

TABLE OF CONTENTS **Page nr**

1. INTRODUCTION P. 4
2. METHODOLOGY P. 6
3. PART ONE: CURRENT AND PROPOSED LAWS P. 7
   - 3.1. The Data Protection Bill P. 7
     - 3.1.1. The Need for Data Protection in an Age of Increased Digital Surveillance P. 7
     - 3.1.2. The Illusion of Data Protection P. 8
     - 3.1.3. The Vulnerability and Role of Civil Society P. 9
     - 3.1.4. Concerns with the Data Protection Bill P. 12
       - 3.1.4.1. Input from IPPR P. 12
       - 3.1.4.2. Input from EPRA P. 22
       - 3.1.4.3. Is The Data Protection Supervisory Authority Truly Independent? P. 24
       - 3.1.4.4. Instances Where Protection Will Not Be Applicable P. 25
       - 3.1.4.5. Lack Of Protection Against State Surveillance of Individuals P. 25
       - 3.1.4.6. Transfer of Data to Foreign Countries and Entities P. 26
       - 3.1.4.7. Inspections by the DPSA P. 26
       - 3.1.4.8. Lack of Judicial Oversight P. 27
   - 3.2. The Cybercrime Bill P. 27
     - 3.2.1. Scope of the Cybercrime Bill P. 28
     - 3.2.2. Enforcement P. 28
     - 3.2.3. Funding of Csert? P. 30
     - 3.2.4. Effectivity, Full Access to All Data and Communications P. 30
     - 3.2.5. Obscuring Public Data P. 31
     - 3.2.6. Unauthorised Access P. 32
     - 3.2.7. Electronic Harassment (*vs* Freedom of Speech) P. 33
     - 3.2.8. Extra-territorial Effect P. 35
     - 3.2.9. Duty to Provide Evidence Against Oneself P. 36
     - 3.2.10. Provision of Data to Foreign Authorities P. 36
     - 3.2.11. Omnipotent Minister P. 37
     - 3.2.12. Conclusion on Cybercrime Bill P. 38
   - 3.3. Part 6 of the Communications Act (8 of 2009) P. 39
     - 3.3.1. Assessment by the LAC P. 39
       - 3.3.1.1. Introduction P. 39
         - 3.3.1.1.1. What is Data Retention? P. 39
       - 3.3.1.2. Namibia P. 39
         - 3.3.1.2.1. Legal Requirements P. 39

3.3.1.2.2. Jurisprudence on Namibia's Constitutional Right to Privacy P. 46
3.3.1.2.3. International Obligations P. 51
3.3.1.3. European Union (EU) P. 56
3.3.1.4. India P. 66
3.3.1.5. South Africa P. 69
3.3.1.6. Possible Constitutional Problems with the Namibian Regime P. 73
3.3.1.7. LAC's Conclusion P. 77
3.3.2. IPPR: Articles on SIM Card Registration and Service Disruption P. 77
3.3.3. Privacy International P. 92

4. PART TWO – BIG BROTHER IS WATCHING: WILL NAMIBIA BE A SURVEILLANCE STATE BY 2035? P.101
4.1. Introduction P.101
4.2. Methodology P.103
4.3. Scoping the Issues: The Global Context and the Rise of Big Brother P.103
4.4. China: A Totalitarian Blueprint for a Dystopian Future? P.104
4.5. India: Increased Surveillance in the World's Largest Democracy P.106
4.6. Namibia: What Will Determine its Surveillance Status in 2035? P.107
4.7. Case Study: The Patriot Newspaper P.107
4.7.1. Background P.107
4.7.2. The High Court of Namibia P.108
4.7.3. The Supreme Court of Namibia P.109
4.7.4. Commentary P.109
4.8. Quo Vadis Namibia? P.110
4.8.1. Scanning Namibia's Contextual Surveillance Environment P.110
4.8.2. Forecasting Namibia's Surveillance Future: Trend Analyses P.117
4.8.3. Futures Wheel P.117
4.8.4. Mapping Namibia's Baseline and Alternative Surveillance Futures: Scenario Development P.118
4.9. Conclusion P.120

1. INTRODUCTION

We live in an information age where we leave digital footprints every day. In fact, footprints are an understatement: our ubiquitous use of online services (particularly social media, platforms, and apps) means that we effectively display our personal information on a brightly lit neon billboard on the ever-expanding information superhighway. Every Tweet, every E-mail, every Google search, every Whatsapp / Signal message discloses something about who we are, what we think, and what we feel. It almost certainly discloses more than we want to reveal.

Our digital data is inseparable from our right to privacy. In an age of increasing artificial intelligence, rising mass surveillance, and formidable machine learning, the real power is no longer knowledge, it is data. What happens to this data - who collects it, who controls it, who owns it, and most importantly, how and for what purpose it is used - should concern all of us.

Most democratic societies recognize the importance of protecting individual freedoms, including the right to privacy. Article 13 of the Namibian Constitution states:

"No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others."

Article 13 can easily lull us into a false sense of security that our privacy is protected. Many citizens are probably unaware that Namibia already promulgated several laws that give Government (through several agencies) access to private communications and privately owned data. For example, Part 6 of the Communications Act (6 of 2009) was enacted on 1 January 2023. This part enables Government to intercept private communications and data. It also requires all users of mobile communication devices to 'register' SIM cards and creates a system of mandatory data retention (and access thereto by Government).

Namibia does not have dedicated data protection laws. This is about to change. In October 2022, the Ministry of Information and Communication Technology (MICT) circulated a draft Data Protection Bill ("the Data Protection Bill") for public comment.

History teaches us that it is naïve to think that public power will never be abused by corrupt actors. In fact, state apparatus has on several occasions been used in Namibia and in South Africa to commit and cover up grand corruption. In South Africa, several law enforcement institutions were captured to enable state capture. In Namibia, large scale looting took place at several institutions with little to no action taken by the relevant law enforcement agencies.

SME Bank and the looting of GIPF, are but two examples. After more than N$600 million was looted at GIPF, the Prosecutor General concluded that "The money is gone, but there is no evidence". Would the looting (and lack of criminal prosecution) in over a decade be possible if all the law enforcement agencies and prosecuting authorities acted with absolute integrity? Is it possible that one or more government agencies were involved in this incredible coverup? The CEO at NAMFISA at the time reported to relevant institutions that several suspicious events (and further investigations) at NAMFISA suggested that government agents may have been involved in the GIPF coverup. Nothing came of this.

For any major coverup to be effective, those tasked with the coverup must be one step ahead of the several (honest) investigators that are involved. To be a step ahead, it is certainly helpful to have the ability to intercept communications, privileged data / and documents. No private Namibian citizen has access to the technology and expertise required to conduct complex interceptions over several years of multiple public and private institutions and persons. However, Government does.

Recently reported events at NAMCOR do not exactly instill public confidence that law enforcement agencies are always acting *bona fide*. Six years after the liquidation of SME Bank began (in 2017), the liquidators stated that many hundreds of millions were stolen, no arrests have been made, and the public is still kept in the dark. Even the proceedings of the Commission of Inquiry are kept a secret. Despite numerous media reports implicating politically connected actors, government officials and reported conflict of interest at the highest level in NAMPOL[1], no arrests have been made. Conjecture has it that at least one person in the know has gone into hiding after experiencing several highly suspicious breaches of security events and fearing for his life. Is there again a major effort to cover up this crime, perhaps spearheaded by

[1] https://investigations.namibian.com.na/top-cops-sme-bank-loan-revealed/

Government agents? If so, will Namibians ever know? Unlikely, because Government has the means to surveil, civil society does not, and is in fact prohibit by law to conduct any surveillance.[2]

Civil society should sound the alarm bells and take all reasonable steps to prevent abuse of public power. Abuse takes many forms, but it can also come in the form of laws enabling public power to sidestep the spirit of freedoms and rights enshrined in our Constitution. Even though there might be no visible abuse at first, it is almost always the potential for abuse which opens the door to actual abuse at a later stage. For this reason, laws should be carefully drafted, balancing personal rights enshrined in our constitution with legitimate interests of the state in a free and fair, functioning democracy. This paper will examine how the abovementioned laws, read together with a compendium of other relevant laws and policies/bills, advance the power and potential of a surveillance state. It can easily be abused by public power for sinister motives, and poses a substantial threat to the right to privacy of current and future generations of Namibians.

2. METHODOLOGY

This paper consists of two parts. Part One deals with different aspects of current and proposed laws which give rise to a surveyance state, and the consequences of each. Part Two is a futures exercise and will take a deep dive into Namibia's possible, plausible, and probable surveillance future outcomes in 2035. [3] Apart from EPRA's own assessment, a substantial portion of this report contains research conducted by other institutions, most notably the Institute for Public Policy Research (IPPR) and the Legal Assistance Centre (LAC). EPRA sincerely expresses gratitude to these institutions for their permission to include their research in this report. Nothing in this report should be taken to mean that the IPPR and the LAC necessarily agree or disagree with the analyses and conclusions reached by EPRA.

[2] See for instance the Protection of Information Act (1982)
[3] Part 2 is based on a 2019 futures assignment of Muthow, Erik to the University of Stellenbosch Business School in fulfilment of a Post Graduate Diploma in Futures Studies (PGDip Futures Studies).

3. PART ONE: CURRENT AND PROPOSED LAWS

3.1. The Data Protection Bill

The Data Protection Bill can be a much-needed step in the right direction. It is however far from adequate and has some serious deficiencies. We will highlight them below. Before doing so, it is worthwhile briefly reminding ourselves why data protection is important and how mass surveillance (and the accompanying loss of privacy) can with ease contribute predominantly to a dystopian future.

3.1.1. The Need for Data Protection in an Age of Increased Digital Surveillance

The collection of digital data and mass surveillance go hand in hand. One cannot effectively exist without the other.

George Orwell's seminal dystopian novel, *Nineteen Eighty-Four*, was published in 1949. Seventy-four years later, it continues to serve as a frightening reminder of the dangers of living under the watchful eyes and ears of a totalitarian mass surveillance regime. We all suspect that "*Big Brother*" (a fictional Orwellian term that can mean anyone in a position of authority, influence, or power) is harvesting our personal data, using it, and watching us. But what does it mean in practice? Why is the protection of our personal data, particularly our biometric data, so important? A good starting explanation is provided by the UN High Commissioner for Human Rights who reported in 2018 as follow.

"The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data."

Clearly, our personal data is worth protecting. It is inseparable from our right to privacy and closely associated with our right to freedom.

It is not only Namibians who are concerned about data protection and mass surveillance. In Europe, the European Union ("EU") recently enacted its General Data Protection Regulation ("GDPR") to give greater protection to individual rights and to harmonize the patchwork of EU-wide laws dealing with data protection. The GDPR is widely regarded as a set of model data protection laws – something others can only emulate and hope to aspire to. It clarifies the rights and obligations of companies and public bodies in what is essentially a digital single market. The GDPR entered into force on 24 May 2016 and applies since 25 May 2018.

3.1.2. The Illusion of Data Protection

A 2021 report by European Digital Rights (the largest European network defending rights and freedom online) considered the rise of biometric mass surveillance in the EU. Notably, the report was compiled after the adoption of the GDPR. It is beyond the scope of this paper to dive into the report in any detail. Suffice to say that its authors found disturbing evidence to suggest that unlawful biometric mass surveillance continues at pace in the sample EU countries selected (Germany, Netherland and Poland). It appears that, despite public assurances to the contrary, EU is increasing unlawful and often arbitrary mass surveillance occur for various purposes.

The report warns that digital surveillance is *"deployed less in response to specific and evidentiary threats but rather indiscriminately as a precautionary or deterrent measure"*, and *"this research further demonstrates the lacuna between a true ban – in which such harmful and rights - violating uses could not be deployed in the first place – and today's biometric mass surveillance Wild West, where private companies, profit, and the state impulse to monitor, surveil, and control people at all times prevail.*

The harvesting of personal data and mass surveillance is usually predicated on "noble" causes, such as reducing crime, combatting terrorism, or increasing efficiency. As we will see, these tools can, however easily be appropriated for more nefarious purposes.

Most of Western Europe has a strong history of resistance to mass surveillance and the invasion of privacy. If the EU, with all its executive organs and after the adoption of the GDPR, struggles to curtail mass surveillance and to effectively protect its citizens from the arbitrary and unlawful collection of personal data, then it stands to reason that smaller and much less resourced countries (like Namibia) have their work cut out for them.

It should by now be obvious that loss of privacy (and freedom) doesn't necessarily require a “Big Brother” taking it from us by force. We are perfectly capable of relinquishing it ourselves. To paraphrase Dorian Lynsey (who wrote a biography on Orwell’s 1984), many of us are happy to barter privacy for pleasure, convenience, and attention.

Data collection (and digital mass surveillance) is not necessarily bad provided it is applied narrowly and upholds our fundamental human rights (including our right to privacy). Having said that, history teaches us that the indiscriminate collection of personal data coupled with mass surveillance is almost always a harbinger of future evil. Even if it serves a seemingly benign purpose today, it can easily be abused by bad actors tomorrow, with devastating consequences. Trusting the authorities to do “the right thing” without proper checks and balances and without holding them to account is extremely naïve. The bottom line is that data collection and surveillance should never be unnecessarily broad and disproportionate to what is reasonably necessary for the proper functioning of a free and fair democratic society, because broad and unchecked power shall be abused.

3.1.3. The Vulnerability and Role of Civil Society

Namibia has a small population and does not have a very active (and crucially, well-funded) civil society. Namibians, therefore, place substantial trust in the structured legislative system whereby laws are created. A substantial portion of Namibians rely on the oversight opposition parties supposedly provide to curtail the creation and expansion of institutions of extraction.[4] This creates a false sense of security. The use of political power for self-enrichment and means other than to serve the electorate, especially through the legislative process, is now well known as “state capture”, following the disastrous looting of public assets in South Africa by politically deployed cadres, in partnership with corrupt private sector actors / handlers. Also, from the South African experience, we have witnessed the capture, and outright destruction of institutions that would traditionally be tasked with the protection of public interests and assets and the prosecution of looters of public assets. In Namibia, one example is the grand looting of the GIPF, which ended in the Prosecutor General concluding that “*the money is gone, but there is no evidence*”.

[4] As defined by Acemuglo and Robinson in their book *Why Nations Fail*.

Civil society played a significant role in exposing state capture in South Africa. Some argue that, if it was not for civil society, state capture would never have been exposed. What is clear is that, left to their own devices, the ruling ANC would have never exposed this rot, and the looting would have continued unabated. The ANC continued to deny the existence of this cancerous system and only after public pressure was forced to establish the Zondo Commission. A mountain of evidence was presented, proving conclusively the existence and the magnitude of state capture. There was simply no denying it anymore, and the ANC had to change its narrative from "it does not exist" to a promise that "we will fight it". Only time will tell if the citizens of South Africa believe the ANC's promise. It is however naïve to think that those who created the corrupt system (and gained massive material wealth in the process) can be entrusted to dismantle the corrupt system.

There is increasing concern that Namibia is following in the footsteps of South Africa's state capture methodologies, especially through the legislative process, and through the capturing of institutions. For this reason, EPRA resolved to become more active in assessing newly proposed national policies (which include proposed laws and proposed amendments to existing statutes). Sadly, unlike in South Africa, Namibia's civil society is weak, and underfunded. Civil society in Namibia today is simply not capable of exposing state capture to the degree that it has been exposed in South Africa. Even if public pressure (mostly through the media) does result in some action being taken, the actions often result in a report withheld from the public in any event. Numerous reports on 'Presidential Inquiries' were never made public. There are many examples: The Walvis Bay Municipality refuses to publish a recent report on corruption. TransNamib (and the Government) continues to refuse a forensic report on alleged corruption. The SME Bank Commission of Inquiry is held in secret, and it is unlikely that the public will ever know what transpired. The list goes on and on. On the rare occasions that the reports do reach the public domain, they are almost always leaked by an internal source, and the public institutions almost always take (often draconian) disciplinary action against those responsible for the leak; as if these persons are the villains for having acted in public interest by leaking information evidencing corruption in the public sector and looting of public assets.

Whistle-blowers in Namibia are not protected, and they are not safe. We have seen this in the case of Johannes Stefansson, the whistle-blower in the 'Fishrot' case. The biggest fear is the use of the state apparatus to silence whistle-blowers and conceal evidence

to protect corrupt, politically connected individuals. What chance does a single whistle-blower stand if the entire state surveillance system and security apparatus is turned against him or her? We all like to believe this will never happen, but that will be very naïve, especially given the mysterious 'vanishing' of so many cases of high-level corruption cases we witnessed before. So, for instance, the ACC already received evidence of 'Fishrot' in 2014. It claims that it was investigating and intended to act. But it only did so five years later, once Al Jazeera exposed the rot in a daring investigation which opened the eyes of the public and left the ACC with no choice but to act. Many feel, probably rightly so, that no action would have been taken in the 'Fishrot' matter if it was not for the exposure by Al Jazeera. This leaves a major question mark on the credibility of the ACC, not only in this matter, but all other matters possibly involving high level corruption. A recent High Court judgement which in no certain terms found that the Prime Minster acted outside of her powers in interfering with appointments at the ACC further confirms the suspicion that the ACC is a politically captured institution.

Note that a former employee of the Namibia Central Intelligence Service was appointed at the ACC.[5] Although widely reported on, and despite several civil societies raising the alarm, no action was taken by Government to reverse this undesirable appointment and to restore the institutional integrity of the ACC. Also, during this time Commissioner Nelius Becker, investigator on the 'Fishrot' matter, was moved from the ACC to the Police. He continued investigating the 'Fishrot'" matter, until he was moved to the Police's Forensics Institute, effectively removing one of the ACC's most capable investigators from the 'Fishrot' investigation.

Can we confidently state that our institutions of law enforcement and prosecution are not politically captured? If they are politically captured, what does it mean for our society if these institutions will obtain even more powers to increase surveillance and harvest data and communications of all citizens?

In the latest national planning document, the Harambee Prosperity Plan II, Goal One is Accountability and Prosperity, to be achieved, *inter alia* through activities which will see the "*adoption and enactment of key policies and legislation*". These include, *inter alia*, the Data Protection Bill and the Cyber Crime Bill. The two bills cannot be read in isolation since there is substantial overlap.

[5] https://www.namibiansun.com/news/moving-spy-to-acc-sinister2020-07-31

Our assessment focuses on constitutionality, possible derogation of the Rule of Law, and possible adverse effects on the enabling environment needed for investment and private sector growth. Our assessment accounts that several experts have in the past warned that state control is becoming a substantial obstacle to investment and economic growth and where appropriate we report on possible unreasonable and/or undesirable expansion of state control through these bills.

3.1.4. Concerns with the Data Protection Bill

The 2021 (latest known) version of the Data Protection Bill follows a previous 2020 version.

3.1.4.1. Input from IPPR

The IPPR published an analysis of the latest bill in November 2022, and in that raised numerous concerns as follow.

"*The present iteration of the Bill is of concern and, in multiple instances, removes or amends necessary and important sections from the 2020 version of the Bill, including, among others:*

- *Removing Part III of the 2020 Bill which affirms the rights of data subjects.*
- *Removing Parts VII and VIII, which relate to recourse to the judicial authority and offences and penalties.*
- *Substantially reducing the institutional independence of the Data Protection Supervisory Authority ("Supervisory Authority") by reducing parliamentary involvement in the appointment, removal, and remuneration of board members.*

While the reason for these sweeping changes remains unclear, they are addressed, in part, in these submissions. However, as a result of these changes, the Bill should be further developed following this public participation process and further opportunities to provide written submissions on future versions of the Bill should be provided to all stakeholders, including civil society."

The IPPR further provided a detailed analysis of certain sections of the bill, which is quoted hereunder, with credit to the IPPR.

"*Overview of Submissions*

On the face of it, the Bill appears to include several essential components of a data protection framework but, distinct from the 2020 Bill, it removes some key sections and seeks to include some essential elements in a piecemeal fashion. We are pleased by the establishment of the Supervisory Authority (although concerned by its institutional independence); provisions dealing with authorisation prior to the collection of special personal information; the provision prohibiting the processing of children's personal information; and provisions pertaining to transborder data flows. However, the Bill should, among others, more explicitly detail and affirm the rights of data subjects, establish offences, penalties, and administrative fines, and better equip and empower the Supervisory Authority to issue sanctions.

We also note that certain aspects of the Bill still require further development to align with best practices, which we detail below, and in some instances the provisions of the Bill should be more clearly drafted. Accordingly, we have identified the following seven areas which, among others, warrant further consideration by the MICT:

First, prior consent should be required for the processing of personal data.

Second, the rights of data subjects must be expressly detailed and affirmed.

Third, the institutional independence of the Supervisory Authority must be guaranteed, its powers, duties, and functions need to be further clarified, and offences, penalties, and fines must be expressly included in the Bill.

Fourth, the exceptions are overbroad and insufficiently detailed.

Fifth, there is a lack of clarity regarding exemption applications.

Sixth, there is a lack of clarity regarding the interaction with the Office of the Information Commissioner established in terms of the Access to Information Bill.

Finally, we list additional practical matters for further consideration. These are dealt with in turn below.

<u>Prior Consent</u>

In its present definition of "consent" in section 1, the Bill provides that "'consent" means any freely given, specific, informed, and unambiguous indication of the data subject's

wishes'. While this accords with comparable legislation, the Bill may benefit from the insertion of the word "prior" after "informed". Adding the element of prior consent to all data subjects strengthens the definition of "consent" in section 1 of the Bill and ensures that data subjects must consent to the processing of their personal data prior to processing. Notably, in section 42 of the Bill, it is only the processing of the personal information of children which is currently subject to "prior consent" requirements.

The Rights of Data Subjects

Dissimilar to the 2020 version of the Bill, the Bill does not clearly and cogently identify the rights of data subjects and removes Part III of the 2020 version of the Bill in its entirety. On a full reading of the Bill, which only addresses the rights of data subjects in a limited and piecemeal fashion, the rationale for removing Part III of the 2020 version of the Bill is unclear.

Cognisant that the nature of data protection legislation is the protection and promotion of the right to privacy, and a balancing of how privacy intersects with other rights, including freedom of expression and access to information, ***the Bill should be approached from a rights-based lens. Accordingly, the Bill should reintroduce Part III of the 2020 version of the Bill as a new Part 2 in the present Bill, with the "Data Protection Supervisory Authority" part becoming a new Part 3. This will correctly give prominence to the primary rights holders in the Bill: data subjects****.*

Independence, Duties, And Functions of The Supervisory Authority

As a point of departure, the IPPR acknowledges the utility in the establishment of the Supervisory Authority. The importance of this office, which is primarily tasked with monitoring and enforcing compliance with data protection legislation, cannot be gainsaid. The General Data Protection Regulation ("GDPR"), which is largely regarded as the model data protection law[6] includes the establishment of properly resourced supervisory authorities composed of suitably qualified data protection experts. Similarly, comparative legislation in other comparable jurisdictions, such as South Africa and Kenya, have followed a similar approach.

[6] While the GDPR is recognised as a model data protection law, national data protection frameworks should be developed cognisant of domestic and cultural contexts, customs, and practices.

Independence of the Supervisory Authority

Despite the important need for the establishment of a Supervisory Authority, the Bill regresses from the 2020 version of the Bill in terms of the institutional independence of the Supervisory Authority, which is considered best practice in contemporary data protection frameworks. The 2020 version of the Bill provides that, among others, the Supervisory Authority is operationally and financially independent from the Executive; that it must report annually to Parliament and its decisions may be reviewed by the courts; and that it is led by a board of five members, who are appointed by Parliament from a pool of ten candidates nominated by the Minister through a "transparent meritocratic recruitment procedure".[7] Notably, the 2020 version of the Bill provides some security of tenure[8] and states that the members of the Supervisory Authority should be remunerated "to guarantee financial independence".[9]

Comparatively, sections 6 and 10 of the Bill provide that board members, including the chairperson and vice-chairperson, are appointed by — and may be removed by — the Minister. Additionally, section 12 provides that the remuneration of the board is to be determined by the Minister, without mention of financial independence, and there are no provisions detailing and safeguarding the security of tenure of board members or specifying timeframes in office. The need for an institutionally independent Supervisory Authority is of paramount importance and it is essential to the proper functioning of a data protection framework. The present Bill substantially reduces this independence, compared to the 2020 version of the Bill, and vests the Minister with ultimate power over the Supervisory Authority as opposed to Parliament.

As a result, Part 2 of the Bill needs to be substantially redrafted in line with the 2020 version of the Bill to ensure that appointments, removals, and the remuneration of board members of the Supervisory Authority are determined by Parliament as opposed to the Minister, and that board members, including the chairperson and the vice-chairperson, are afforded security of tenure and are shielded from undue political influence. Additionally, in appointing board members, Parliament should be directed to seek public nominations before initiating any appointment processes.

[7] See section 28(1) of the 2020 version of the Bill.
[8] Id at section 29.
[9] Id at section 31

The Power to Sanction

The Bill provides insufficient information on precisely how compliance will be monitored and enforced by the Supervisory Authority. More specifically, sections 4 and 5 detail the Supervisory Authority's powers, duties, and functions which non-exhaustively include: being responsible for investigating contraventions of the Act; consulting with interested parties on the protection of personal data; handling complaints by various stakeholders; monitoring and enforcing compliance through a number of actions; and conducting research and reporting it to the MICT.

While these duties and functions are legitimate, the IPPR is concerned that vague and imprecise language has been used particularly with respect to monitoring and enforcement. Although the reality is that monitoring and enforcement will be a case-by-case exercise, the Bill, as it currently stands, does not provide sufficient guidance on how the Supervisory Authority will proactively monitor and enforce compliance. This is not an issue that is unique to Namibia's proposed framework. In South Africa,[10] there has been concern over the Information Regulator (which is South Africa's equivalent of the Supervisory Authority) only intervening where there has been non-compliance.

Further, the provisions in the Bill dealing with monitoring and enforcement do not impose any time periods for the Supervisory Authority to fulfil its duties. Notably, the Bill also does not require the Supervisory Authority to educate and empower members of the public on their rights under the Bill.

Resultantly, and at the very least, section 4(h) should be amended to read: "be responsible for investigating contraventions of, and enforcing compliance with, this Act . . .". Additionally, the MICT may consider defining, or providing further clarity on, "the Court" in section 5(1)(h) and including additional enforcement-related provisions within sections 4 and 5 which explicitly empower the Supervisory Authority to issue sanctions, in the form of fines and other administrative penalties, for non-compliance with the Act.

Offences, Penalties, And Administrative Fines

Read with the above, sections 54 to 71 pertain to enforcement and empower the Supervisory Authority to investigate and "settle" complaints and apply for warrants.

[10] See AfricanLii, 'POPIA: Progress and Problems', 9 June 2021, accessible here.

However, dissimilar to the 2020 version of the Bill,[11] the Bill is largely silent on explicit criminal and administrative sanctions, including offences, penalties, and administrative fines for non-compliance, save for brief references in, among others, section 52 and in section 73(2)(l) on "matters incidental to the imposition of administrative fines". This is a notable omission from the Bill, which renders its application limited and is unlikely to lead to compliance with it by data controllers.

As a result, a new Part or Chapter — based on Part VIII of the 2020 version of the Bill but developed as necessary — should be included in the Bill which refers directly to offences, penalties, and administrative fines. This Chapter should consolidate the offences and administrative fines referenced in the Bill and:

- *Expressly create an offence for any person who hinders, obstructs, or unlawfully influences the Supervisory Authority; who fails to comply with an assessment or enforcement notice; or who obstructs the execution of a warrant, among others.*
- *Establish criminal penalties for offences which may include fines or imprisonment, or both.*
- *Create administrative penalties, in the form of fines, which may be issued by the Supervisory Authority for non-compliance with the Act.*

These offences, penalties, and administrative fines should be comprehensively and precisely detailed to avoid ambiguity, and should detail the responsible authorities, including the Supervisory Authority.

Civil Liability

Another notable omission from the Bill pertains to civil liability. As has been noted:

> *'One of the most important accountability mechanisms available to a data subject is civil liability. This allows a data subject to institute legal proceedings against a data controller if the controller violates the law and causes the data subject harm or loss. The data subject can use this legal action to claim a monetary amount from the data controller in damages for the harm or loss they suffered. Such a court*

[11] See Part VIII of the 2020 version of the Bill.

action is time-consuming and expensive, and will likely carry significant reputational harm for a data controller."[12]

While civil liability may be accommodated elsewhere in Namibian law, contemporary data protection frameworks, including in South Africa, often include reference to civil liability and civil remedies in their data protection legislation, both for the Supervisory Authority and for individuals. As a result, either in sections 4 and 5 or ina new Part or Chapter, the power of the Supervisory Authority, or an individual, to institute civil action should be prescribed.

Overbroad "Exceptions"

General exceptions:

Section 43(1) of the Bill contains nine "exceptions" to the processing of personal data. These exceptions (which must pursue a legitimate purpose and be necessary and proportionate) may relate to the protection of: (a) national security; (b) defence; (c) public safety; (d) important economic and financial interests of the State; (f) the impartiality and independence of the judiciary of Namibia; (g) the prevention, investigation, and prosecution of criminal offences; (h) the execution of criminal penalties; (i) other essential objectives of general public interest; or (j) the protection of the data subject or the rights and fundamental freedoms of others. Notably, section 43(1) does not contain a subsection (e) and section 43(2) refers to a "regulation" in section 43(1), which is unclear and unspecified. The Bill should be amended accordingly.

The IPPR does not contend that exceptions, on the whole, are inherently problematic. However, the IPPR is concerned about the broadness of the exceptions contained in the Bill. In particular, the exceptions listed in sections 43(1)(a), (c), (d), and (i) are inherently vague, open to a wide interpretation, and may potentially be misused. Notably, none of the exceptions are defined in the Bill, which may lead to diminished and inconsistent application of the law.

The IPPR recommends that sufficiently detailed regulations should be published in terms of section 43(1) providing clear and precise definitions, objective and adequate

[12] Tara Davis, 'Data Protection in Africa: A Look at OGP Member Progress,' August 2021, at page 44, accessible here.

safeguards, and further general guidance on the application of the exceptions contained in section 43(1) of the Bill, particularly sections 43(1)(a), (c), (d), and (i). Alternatively and preferably, the Bill itself should be developed to provide further guidance on the exceptions. Through developing these regulations or developing the Bill, the IPPR takes the view that any exceptions which cannot be reasonably justified should be removed. Ultimately, exceptions should apply in narrowly circumscribed instances and in a manner that promotes progressive democratic constitutionalism.

Exemption of Journalistic, Literary, or Artistic Purposes:

While referencing an exception for communications between legal advisers and clients in section 67 and general authorisations specified in section 34, the Bill does not contain an express exemption, exclusion, or authorization for journalistic, literary, or artistic purposes, contrary to contemporary trends in data protection legislation which seek to balance and reconcile the right to privacy with the right to freedom of expression.

As a result, an express exemption for journalistic, literary, or artistic purposes should be recognised in the Bill, either in section 34(1)(f) or section 43, and should provide that "The Act does not apply to the processing of personal data solely for the purpose of journalistic, literary, or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression, including press freedom." (Additionally, an express exemption for processing personal data for academic purposes, with sufficient safeguards, should be considered by MICT.)

<u>Exemption Applications</u>

Section 43 does not empower the Supervisory Authority to grant additional "exclusions" or exemptions for the processing of personal data. While this may perceivably fall within the remit of "Codes of Conduct" in sections 44 to 52, an express enabling provision should be included in the Bill within section 43, alternatively a new section 44, to enable the Supervisory Authority to grant an exemption to a responsible party to process personal information if it is in the public interest to do so, and there is a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

Given the fast-moving and unforeseen nature of data protection, the Supervisory Authority should be permitted to grant exemptions, on application from an individual or a data controller, where it is in the public interest to do and where unforeseen instances arise. This may include, for example, retaining (for an extended period) educational and employment data of children (who are permitted to work from age 14 onwards) to assist them in seeking additional educational or employment opportunities.

Interaction with the Information Commissioner

A potential lack of alignment and harmonisation exists, or may be created, between the mandate of the Supervisory Authority and the mandate of the Office of the Information Commissioner established in terms of the Access to Information Bill.[13] *The Information Commissioner is mandated to enforce the right of access to information in general contexts, which may include evaluating whether a request for information relating to personal information or data was properly decided. The Supervisory Authority is mandated to enforce data subjects' rights in the context of processing personal data, which may include enforcing the right of a data subject to access personal data about themselves that is held by another partner or to access information about how their personal information has been or is being processed.*

As a result, sections should be expressly included in both the Bill and the Access to Information Bill to delineate how the mandates of the Supervisory Authority and the Information Commissioner will interact to ensure that both oversight bodies are able to function cohesively and effectively.

Additional Matters for Consideration

Breach notifications:

Section 1 defines a "personal data breach" as a "breach of security leading to the accidental or unlawful use, destruction, loss, alteration, disclosure of, or access to, personal data transmitted, stored, or otherwise processed". However, outside of this section, it does not again appear in the text of the Bill. Section 30, which presumably deals with personal data breaches, is titled "Notification of security compromises", a term which is not defined in section 1. To ensure consistency in the Bill, section 30

[13] Section 9 of the Access to Information Bill B4-2020.

should be re-titled or renamed "Personal data breach notifications" to align with the definition of a "personal data breach" in section 1.

Additionally, a new subsection in section 30 should provide for offences, penalties, and/or administrative fines if a data controller does not provide the required notification of a personal data breach. Alternatively, the suggested new Part or Chapter on offences, penalties, and administrative fines should expressly list a failure to notify a data subject of a personal data breach as an offence warranting a penalty or administrative fine.

Direct marketing:

The Bill makes limited reference to direct marketing in section 20(6) stating that "A data subject may object, at any time, to the processing of personal data for the purposes of direct marketing other than direct marketing by means of unsolicited electronic communication." However, the Bill goes no further. Unsolicited direct marketing — by any means or form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail — should be expressly prohibited in the Bill due to its intrusive, unwanted, and non-consensual nature. As a result, a new section should be introduced in the Bill which expressly prohibits unsolicited direct marketing, without consent, and enables the Supervisory Authority to issue administrative fines against responsible parties.

Terms of service icons:

In order to foster greater transparency and participation of data subjects, information about the processing of personal data may be disseminated to data subjects through a combination of text and icons, particularly in online spaces such as websites. The effective use of terms of service icons depends on their standardisation and identifiability. Generally, terms of service icons will appear on a website and enable ease of access to terms and conditions, particularly in relation to the processing of personal information.

To foster transparency, section 5(1)(c) of the Bill could include a further subsection stating that "The duties and functions of the [Supervisory] Authority in terms of this Act are to monitor and enforce compliance by prescribing the use of terms of service icons on applicable websites, applications, and other internet-enabled platforms, and

providing guidance to controllers on the use of terms of service icons on these platforms."

Effective functioning of the Supervisory Authority:

Practically, the Bill establishes the Supervisory Authority in section 3 and provides in section 75 that a one-year "grace period" applies following the commencement of the Act. As a result, the Supervisory Authority is expected to be fully operational within one year of the commencement of the Act to ensure that it can monitor and enforce compliance with it. In order to ensure that the Supervisory Authority is established within the one year time period stipulated in section 75 of the Bill, practical steps should be taken to fully establish, fund, and staff the Supervisory Authority following the commencement of the Act, including taking pre-emptive measures to ensure that there are no delays with the establishment of the Supervisory Authority following the commencement of the Act.

Conclusion

As detailed above, the Bill, in its present form, requires further development to ensure that it meets the requirements of a contemporary data protection framework. Notably, the sections on the independence of the Supervisory Authority need to be reconsidered and substantially redrafted, and sections concerning offences, penalties, and administrative penalties need to be re-introduced and developed, among others. In its present form, the Bill is not fit for purpose…"

3.1.4.2. Input from EPRA

As stated earlier, the introduction of the (draft) Data Protection Bill is welcomed since it is long overdue. Its aim is to establish a Data Protection Supervisory Authority ("DPSA") and to, amongst others, regulate *"the processing of information relating to individuals to protect the fundamental rights and freedoms of individuals"*. It expressly deals with the right to privacy in respect of persons who have their data processed.

Key Definitions

Before we proceed to comment on the Data Protection Bill, it is important to familiarise ourselves with some of the key definitions:

"Biometric data", is defined as *"personal data relating to the physical, physiological, biological or behavioural characteristics of an individual which allows the unique identification or authentication of the individual including by facial images or dactyloscopic data"*.

"Consent", is defined as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, either by a statement or by clear affirmative action, signifies his or her agreement to the specified processing of personal data relating to him or her".*

"Controller", is defined as *"a natural or legal person or public body that alone or jointly with others ('joint-controllers'), has decision-making powers determining the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by an act, decree or ordinance, the controller is a natural person, legal person or public body that has been designated as such by that act, decree or ordinance. The controller shall be responsible for the processing of personal data carried out on its behalf by a processor".*

"Data Protection Supervisory Authority", is defined as *"an independent public authority responsible for ensuring that personal data is processed in compliance with the provisions of this Act. This implies a decision-making power independent of any direct or indirect external influence on that Authority".*

"Data subject", is defined as *"an identified or identifiable living individual to whom personal data relates. An "identified or Identifiable individual" means -*

> *(a) a person who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;*
>
> *(b) in identifying whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person authorised by the controller to identify the said person; and*
>
> *(c) an individual who is "identifiable" if the processing allows the individual to be 'singled out' from other individuals."*

"Personal data", is defined as *"any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, a pseudonym, and IP address, location data, factors relating to the economic, mental, cultural, physical".*

An appropriate start but room for improvement

We are generally satisfied with the stated aims of the Data Protection Bill. It's aims are as follow.

(i) protect data subjects by *"requiring that personal data is processed in a transparent, fair and lawful manner, on the basis of an individual's consent or another specified lawful basis"*; and

(ii) impose *"conditions on data controllers or a person acting under their authority … including conditions of accountability, processing limitation, purpose specification, information quality, openness, security safeguards and access to personal data by data subject."*

Unfortunately, there remains a risk that protection provided in the Data Protection Bill can be abused by bad actors (both private and public bodies) and/or nullified by the scope and application of the Cybercrime Bill. For example, the protection afforded to data subjects can be negatively impacted, if the controller or processor of personal data acts in exercising their "legal obligation". So, for instance, Csert (as discussed hereunder) could access personal data, and control and process it at will, through the powers obtained under the Cybercrime Bill.

Other general concerns follow.

3.1.4.3. Is The Data Protection Supervisory Authority Truly Independent?

The Data Protection Bill provides, in Part 2, for the establishment of DPSA. The DPSA has wide powers, including the power to monitor and enforce compliance with the Data Protection Bill – see section 5(1)(c).

The DPSA is funded by the government, which includes money appropriated by Parliament, levies imposed on data controllers, and fees paid to the DPSA for its services – see section 14.

The DPSA Board consists of no more than five (5) members and the chairperson and vice-chairperson are appointed by the MICT Minister - see section 7. The previous draft provided for appointment by Parliament. The DPSA is ostensibly an independent body. In reality, the MICT Minister has broad powers and neither private sector nor civil society have any input in the appointment of the DPSA Board.

Given the above red flags, the DPSA is effectively completely under Government control, and it will be naïve to think that it will always act as an independent body, immune from political influence.

3.1.4.4. Instances Where Protection Will Not Be Applicable

Personal data will not be protected where the following are threatened: national security, defence, public safety, and important economic and financial interests of the State. As stated under the section dealing with the Cybercrime Bill, it becomes a slippery slope when the State can access personal / private data, while competing commercially with those whose data has been obtained. The business intelligence available to the State to compete with the private sector will not be available to competing private sector entities.

This provides for an exceptionally unfair advantage to the State in commercial dealings and increases the State's ability to further encroach on private sector business. The above exception, i.e., "economic and financial interest of the State" will allow the State to process personal / private data (after it was obtained through the Cybercrime Bill) in a manner which is prohibited within private sector itself.

3.1.4.5. Lack Of Protection Against State Surveillance of Individuals

The Data Protection Bill allows for processing of personal data for national security and defence purposes, subject to "independent and effective review and supervision" – see section 43. The bill does not state who shall be tasked with such "review and supervision", and what such review and supervision will entail. So, for instance, the Namibian Central Intelligence Service can process personal data, claiming that it is for

the purpose of national security (and there is no oversight mechanism for a person under surveillance to test and/or verify this) and claiming further that the Namibian Central Intelligence Service itself was "dependent and effective" enough to satisfy the requirement under section 43. The said mentioned absence of an oversight mechanism is most likely to be abused.

It is a very likely scenario given the arguments provided by the Namibian Central Intelligence Service in a High Court matter heard in 2019 (see more detailed discussion hereunder of the case of Director-General of the Namibian Central Intelligence Service & another v Haufiku & 2 Others (SA33-2018) [2019] NASC (12 April 2019)). In that case National Intelligence did not regard its discretion and actions to be capable of scrutiny by the High Court. This should be of grave concern to every Namibian.

There should be clear and express provisions which *inter alia* prescribe the minimum standards and processes in reviewing and supervising state surveillance. Due process, judicial permission and oversight must be express preconditions. Without such clear provisions, meaningful review and supervision is unlikely to occur, and the current provision provides nothing but false hope of some sort of oversight of the State's surveillance of individuals.

3.1.4.6. Transfer of Data to Foreign Countries and Entities

The Data Protection Bill prohibits the transfer of personal data to foreign countries and organisations unless certain safeguards for protection of such data abroad are in place. This is commendable, but perhaps impractical given the nature of automated social media platforms such as Facebook, Instagram, Tik Tok and YouTube. Unfortunately, again, the Cybercrime Bill can still be used to transfer personal data to foreign bodies (as explained hereunder) and such transfer cannot possibly be protected under the Data Protection Bill.

3.1.4.7. Inspections by the DPSA

The DPSA has authority to *"supervise"* processing of data by both public authorities as well as private bodies. In such supervision the DPSA may conduct investigations, and may request any "record and thing" to be provided as per its sole discretion, and without having to obtain a court order beforehand – see section 62. There is no express limitation on the scope of such investigations, which leaves the power to conduct same

open for abuse of personal/private data by the DPSA itself. The concern raised in respect of the Cybercrime Bill hereunder is also applicable here - it could allow otherwise unlawful access to personal / private data by government functionaries.

3.1.4.8. Lack of Judicial Oversight

The DPSA has the powers to order a restriction of data (see section 43) "subject to objective and adequate safeguards". Note the discussion before on the vagueness of such, essentially, false safeguards which do not expressly require judicial oversight. As an example of how such public powers can be abused, a politically captured institution acting to protect a corrupt individual can use such provisions to not only block whistle-blowers from exposing corruption, but also to persecute and prosecute them.

As Government already competes with private sector for access to information and business (e.g., Namcor filling stations), these powers can also be used to frustrate or obstruct private sector businesses competing with Government (or even frustrate or obstruct the operations of civil society organisations), as exemptions and restrictions also apply when data relates to "*important economic and financial interests of the State*". Government competes with private sector in every sector of the Namibian economy. Surely these public sector entities, especially the commercial public enterprises can claim that their operations are "*important economic and financial interests*" to the State, and thus the exemptions and restrictions can be abused on that basis.

3.2. The Cybercrime Bill

In this section, we provide an assessment of the Cybercrime Bill which we believe (but cannot know for certain) is the latest version. This Cybercrime Bill is very likely unconstitutional, for various reasons. It clearly impugns the constitutional right to privacy. This is acknowledged in the bill itself. It provides for wide- ranging powers to a "Management Committee" (of possibly only two persons) to access any data and communication in private domain, on the sole discretion of the Minister responsible for technology.

There is no specific safeguard of data that would otherwise be confidential, for example information subject to attorney-client privilege, doctor-patient privilege, funding to political parties within the statutory prescribed limits, membership to private institutions, even intellectual property held by private organisations or businesses. During ongoing

investigations by the Anti-corruption Commission, data can also be accessed by persons appointed through political channels, and even be shared with foreign entities.

The Cybercrime Bill does address some legitimate issues of concern, such as cyber hacking and child pornography, but the powers provided to Government to access private information in the process are largely unlimited and unchecked. Once Government uses this power to obtain otherwise private data and communications, there is no remedy, for the data would have been accessed and possibly distributed already. A court cannot be approached to interdict the Government from accessing data as the process up to such point of access is done in secrecy, unknown to any affected person.

There is very limited safeguard against government surveillance of private citizens and organisations. Such surveillance can possibly be used for sinister reasons, which then allows for the State to become a surveillance state unchecked by constitutional safeguards. To assume the State will not abuse these powers is naive. We urge policymakers to revisit the Cybercrime Bill and reconsider the issues addressed herein.

3.2.1. Scope of the Cybercrime Bill

All computer systems and data messages fall within the scope of the Cybercrime Bill. This will include all storage and transmission of data as well as electronic mail, mobile communications, SMS messages, and video and audio recordings. All servers, personal laptops and mobile phones are regarded as computer systems.

All facilities generating, sending, receiving, storing or processing data or data messages fall under the Cybercrime Bill.

A person is deemed to personally possess data even if such data is stored by a third party as a service to such person.

3.2.2. Enforcement

A Computer Security Response Team (“Csert”) is established within the Communications Regulatory Authority of Namibia (“CRAN”) to enforce the Cybercrime Bill.

The powers of Csert vests in a Management Committee established by CRAN, which Management Committee can consist of, as few as two people. The Management Committee has all the powers, functions and duties conferred upon Csert.

Cert may collect *"all relevant information" and "monitor"* anything relating to the security and stability of computer and information systems. It may disseminate such information in its own discretion to any third party. Csert may also co-ordinate its actions with a foreign *"body"*.

Csert may "*take all necessary steps to diminish the risk of offences involving the uses of computer or information systems*", including the *"detection"* of such offences. These offences are extremely broad as discussed hereunder, and thus Csert essentially has carte blanche to access private information, in its own, at its sole discretion. Furthermore, the power to *"detect"* logically precedes an inference that an offence was committed, thus giving Csert the powers to access any data and communication on any electronic device without having to show reasonable cause that a crime is being committed. Reasonable belief that a crime is being committed, urgency, and a real risk of destruction of evidence are prerequisites for NAMPOL to breach the right to privacy. However, these prerequisites will however not be requirements under the Cybercrime Bill paving the way for unlimited surveillance without any due process being followed, and most notably, without any judicial oversight.

In addition to the general powers described above, Csert may take *"all reasonable steps"* to *"detect"* money laundering or the *"hiding of proceeds of crime"* through the use of a computer system. Again, the steps that can be taken to *"detect"* precedes an inference that such actions took place, thus giving Csert the powers to access any private data or communications based only on the assertion that such actions could possibly have taken place. Apart from these specific powers, Csert may also do anything that is necessary or desirable for the purpose referred to above. As per our common law, and more specially several recent judgments delivered by the Namibian Supreme Court[14], such unlimited powers cannot withstand constitutional muster.

[14] Most notably the Supreme Court Judgments in MAN vs NMRC and Telecom vs CRAN

The Cybercrime Bill also makes provision for CRAN's board to delegate *"any power or assign any duty or function"* to the Management Committee, even if not expressly stated as a power, duty or function of Csert in the Cybercrime Bill.

To enforce the Cybercrime Bill, inspections may be conducted, and *"any institution"* or *"person"* may be appointed as *"Computer Security Inspector"* ("CSI"), whether employed in Public Service or not. A CSIs may conduct inspections on *"security, stability or confidentiality"* of *"important"* databases. A CSI, or any person delegated by a CSI, may run a *"test"* on any *"important database"* without giving notice, and such test *"may involve the access of the system without authorisation"* of the official user. A CSI may issue fines.

3.2.3. Funding of Csert

A Computer Security Fund will be established to defray the expenses of Csert. The fund will be funded through Parliamentary budget, and "*monies paid as a consideration for security services provided by Csert*". The bill does not state who will determine such charges, who will be liable to pay such charges, and under what circumstances. Csert may also receive funds *"derived from any activity relating to its functions"*.

From the above it appears that policymakers wish to enable CRAN to impose levies and otherwise prescribe payments for mandatory services to be provided to certain entities, perhaps even individuals.

3.2.4. Effectivity, Full Access to All Data and Communications

The Minister may declare <u>any</u> data, including communications, as *"important data"* if in his/her sole discretion it is in the interest of national security, or *"the economic or social well- being of Namibia*". Once so declared Csert (read Government) obtains substantial control over such data. The Minister may issue regulations on *"any matter relating to access to, transfer and control of important databases"*. The Minister may also state to whom data must be revealed and may prescribe who may audit a database (which audit will be compulsory) as well as the content of an audit report to be provided to Csert.

Non-compliance with the newly formed powers of Csert to access data will be a criminal offence punishable by imprisonment for up to five years.

Apart from the fact that there is no Parliamentary oversight on the Minister's discretion to breach the constitutional protection of privacy, it can be argued that almost all data somehow relate to the "*economic or social well-being of Namibia*". We reiterate that Government (including public enterprises) competes with private sector in every economic sector. As such, all private sector entities will generate, possess and transmit data which, it can be argued, is somehow relevant to the "*economic or social well-being of Namibia*". Again, this allows for massive expansion of the surveillance state, with no remedy to affected citizens other than to challenge the constitutionality of the powers given to the State through the Cybercrime Bill itself.

Government is openly and actively expanding its encroachment on private sector business, and competing against private sector businesses with public funds. Government will have an even stronger, major advantage over private sector in the business intelligence it can collect. This is likely to result in a further decline of the private sector and investment, and as a result, a subdued economy and reduced tax revenue.

In illustration of the above: Namcor competes directly with private sector fuel wholesalers and retailers. Namcor is set to become an active player soon also in the complete fuel supply chain in Namibia. This is done with public funds, paid for by taxpayers and all consumers of fuel. Private sector is thus effectively funding its own demise, the reduction of the number of taxpayers, and tax revenue.

Through the Cybercrime Bill, Namcor, and several other public sector enterprises competing with private sector in all industries, may gain access to information which can provide them with a further advantage in competing with, and ultimately crowding out private sector, ironically under the guise of the "*economic or social well-being of Namibia*". In this regard the Cybercrime Bill appears to be a further step towards a Marxist / socialist economy (not to be confused with the concept of the welfare state), an economic model which has only failed in other countries in the past. The Government simply runs out of other peoples' money and potential investors flee, as we have witnessed in Namibia since at least 2016. Investors will now have to accept that their data and communications will now be freely available to Government, and any local or foreign entity which our government may wish to provide it to.

As stated before, the Cybercrime Bill makes no provision for protecting privileged / confidential information from being accessed by the Government.

3.2.5. Obscuring Public Data

For decades civil society has fought hard for the promulgation of the Access to Information Act. This is a crucial instrument in civil society's fight against government corruption, and especially at a time when public trust in public institutions established to fight corruption, is disappearing. The Access to Information Act has recently been promulgated, but not enacted, with no indication on when the enactment will take place. As with the Whistle-blowers Act, which also aims to fight corruption, and which is also not enacted, Government blames a lack of funding for not enacting these laws.

The Cybercrime Bill can be used to override, and thus undo all the progress made on the Access to Information Act. So, for instance, the Minister may restrict access to or transfer of any database (including communications) which in his/her sole discretion be regarded as *"important"*. The Minister may make regulations to *"secure confidentiality"* of such databases and prescribe the "*procedures and technological methods to be used for storage or archiving*" thereof including the specific information system it must be stored on, which could possibly include the actual location of such storage.

Once the Minister has decided that a database is *"important"*, he/she may also set the exact circumstances under which and to whom such data may or must be disclosed. The Minister may specify classes or categories of persons to whom *"important"* data may not be revealed and who may not have access to an *"important"* database. In addition to the above, the Minister may regulate "*any other matter*" pertaining to *inter alia* the confidentiality or control of *"important databases"*.

Non-compliance with the newly established powers of the Minister to conceal data, i.e., accessing data specified as "*important*" will be a criminal offence punishable by up to five years imprisonment.

These powers can easily be abused, as the Cybercrime Bill stands in its current format, to prohibit access to otherwise public information. For example, the Minister could declare the database on allocation of resettlement farms as "important data", and through the powers in this Bill, limit access thereto and ensure that same remain "*confidential*" and thus not open to public scrutiny. Same goes for fishing quotas for example, and/or public tenders.

3.2.6. Unauthorised Access

Accessing a computer system or information system, performing an action on data, while knowing that such access is unauthorised, is a criminal offence punishable by imprisonment of up to 10 years, and if the intent was to cause *"major disruption"* or *"serious damage"* (which terms are not defined and thus completely arbitrary) by up to 20 years.

While the rationale behind this part is understandable, to criminalise data hacking, cybercrime, ransomware etc., the wording of this part also criminalises, on same equivalence, a person accessing his/her spouse's mobile phone, or logging into his/her Facebook or Instagram account, with no malicious intention. Should the spouse become disgruntled with him/her at some point in time thereafter, even years later, for any reason imaginable, perhaps in bitter divorce proceedings, and he/she then decides to institute a criminal complaint, the spouse faces 10 years imprisonment, while having had no intention to cause any damage at the time.

3.2.7. Electronic Harassment (*vs* Freedom of Speech)

The part of the Cybercrime Bill dealing with electronic harassment criminalises the action of posting (i.e., on Facebook) or sending a data message (i.e. on Whatsapp) which causes *"serious emotional distress"*, and *"makes a credible threat of violence or other harm"* to a person (or entity, such as a political party, which in law is also regarded as a "person"). Similarly, it will be an offence to make a *"statement"* in such data posting or message knowing it is false, or with *"reckless disregard whether it is true or false, with the intention to do serious harm to the reputation of another person"*. Making a sexual suggestion knowing it to be *"offensive or annoying"* will also be a criminal offence. These said mentioned offences are punishable by a maximum of two years imprisonment.

Although these new offences may at first glance seem appropriate to some, they pose a material threat to the constitutional right to freedom of expression. This is illustrated by a few examples, some posed in question format, hereunder.

If one would publish a comment alluding to the fact that the former Inspector General's comment some time ago on NAMPOL taking control of the City of Windhoek's Council is not only undemocratic and flies against the principles of the Constitution but also

amounts to outright instigation of an authoritarian police state, the Inspector General would have been able to have that person arrested and prosecuted if the Cybercrime Bill was in force.

If one reposts an article on Facebook, which article is already in public domain, but it later turns out some statements in that article were not true, perhaps even speculative, or at least not properly researched, one commits a crime as, given the description of the crime, one has not shown sufficient regard whether the article is true or not. Now, one thus has a duty to conduct a forensic investigation of sorts on the accuracy of every post you receive, before reposting. The legal risk becomes enormous, and freedom of speech is abolished.

If one expresses a personal opinion that you believe a certain Minister is not competent enough to deliver on a given mandate, do you cause "*harm*" to that Minister, or can the Minister claim that you have offended his reputation? Likely so, and for that reason you have committed a crime and the Minister may institute criminal proceedings against you. This will also be the case even if your post alluded to "Government", generally.

If the leader of a political party distributes a newsletter to his followers, telling them that he believes those currently in power are corrupt, and should be replaced, has he injured their reputation, and may he be jailed for such statement under the Cybercrime Bill?

If a 20 year old man meets a 18 year old woman whom he really likes and is audacious enough to SMS her to state that he thinks she is a great person and hope to get to know her much better, and perhaps have an intimate relationship with her, should this be punishable by two years imprisonment if she happens to be a person who finds such a message "*annoying*"?

If a husband wishes to reconcile with his wife during a break-up period and sends her a message that he wishes to re-establish their intimate relationship, as they have been used to during the start of their marriage, and the wife finds this "*annoying*", should he be held criminally liable for the mere sending of this hopeful message?

The examples illustrating the absurd consequences of this Bill, can be unlimited.

The prohibitions stated through these offences far outstrip rationality, practicality of daily interactions of ordinary citizens in a free and democratic society, apart from the fact that

our civil and criminal law already caters for the bulk of the unwanted actions described therein. So, for instance *crimen injuria* (wilful injury of a person's dignity) is already a common law crime. An utterance based on racial discrimination is already a crime. Unlawful defamation is already grounds for civil action and compensation, and so forth. Curtailing freedom of expression through the broad descriptions of these offences will make most social media users instant criminals, for mere reporting of already public posts, and will severely curtail any criticism of any person or institution serving in any public position. Practically, no social media post can be forwarded without doing, and recording, a diligent fact-checking exercise, which is a duty no law should confer on the public, apart from that it severely hampers a free- flow of ideas, which is crucial for the advancement of a free, democratic society. The media will especially be at risk, and opinion pieces will soon disappear from newspapers. Anonymous opinions may very well be unlawful, as they may be regarded as constituting a criminal offence (and the Government has the powers and tools to establish the identity of the author in any event).

Ultimately, who decides what is true or false, what is harmful, what constitutes reputational damage? By creating these offences, the NAMPOL will be policing these value judgments, and in the discretion of the police, a person may be jailed until he/she is brought before a court. This advances a police state as described in George Orwell's book "1984", where citizens speak only in secrecy, and hide in the shadows, too afraid of the Thought Police. To curtail a whole nation's freedom of expression to protect the feelings of others is a dangerous turn towards a totalitarian and communist state; and definitely not aligned with the values cherished by free, constitutional democracies.

3.2.8. Extra-territorial Effect

Any offence created in the Cybercrime Bill is *"deemed to have been committed in Namibia … if any part of the offence was performed in Namibia …. or … if the offence was committed by a citizen of Namibia"*.

To further expand on the adverse implications of the offences created by the Cybercrime Bill, and more in particular the offences relating to *"electronic harassment"* the following real-life practical example is provided:

The now famous Al Jazeera documentary dubbed the '*Fishrot'* scandal first aired in Namibia in late 2019. It was aired on the Al Jazeera channel facilitated by Multichoice

Namibia, and was widely distributed on several social media platforms, including YouTube and Facebook.

There can be little doubt that the ministers implicated in that documentary must have felt "*harmed*" and their reputation damaged. As per their numerous defences in several courts so far, during several bail hearings, they obviously do not agree with the allegations made in that documentary. Namibian lawyer Norman Tjombe also provided his opinion in the documentary, stating that from what he has seen in the documentary, the crime of corruption was committed.

Under the Cybercrime Bill, in question Al Jazeera, and especially its journalists and management, could have been criminally prosecuted (for the documentary aired in Namibia). Facebook and Instagram could be criminally prosecuted, for these companies control information systems through which the documentary was distributed, and Norman Tjombe could be prosecuted, for it could be argued that his opinion, which led to "*harm*" to the ministers' reputation, did not follow his own, documented investigation into all the facts in the 'Fishrot' matter. Every person in Namibian and every Namibian citizen abroad who redistributed the video on social media platforms could have been prosecuted.

3.2.9. Duty to Provide Evidence Against Oneself

A crucial pillar to the constitutional right to a fair trial is the right not to be forced to incriminate oneself. So, for instance a suspected murderer, who refuses to tell the police where he hid the murder weapon, cannot be criminally liable for such refusal – only for the murder itself. Put differently, there is no duty on an accused person to do the work of the police or to assist them in any way in the investigation or prosecution of him.

The Cybercrime Bill changes this, most likely unconstitutionally, when it comes to all the crimes created in the bill. Any person who refuses to provide to the police a computer password or key, fails to render assistance as requested by the police in their investigation, fails to provide data as ordered by court (which is already an offence - contempt of court) will commit an offence punishable by a maximum of two years imprisonment. The order referred to above can be obtained by the police without the court hearing the other party. The duties, and possible criminal sanctions that may follow, thus stem from proceedings to which the affected person had no opportunity to

reply to. No relief can be obtained from a court beforehand, as the affected person was not aware of this invasion until it happened.

3.2.10. Provision of Data to Foreign Authorities

The Cybercrime Bill allows for information obtained under it to be provided to foreign *"institutions or bodies"*. So, for instance, data constituting crucial intellectual property of a private Namibian company can be provided to a foreign entity or government wanting to compete in the same and/or similar industry as the Namibian company. As outlandish as this may sound, this threat is real. The Namibian Government notoriously provides major capital projects to foreign-owned companies, most notably, China. The Namibian public has rightfully questioned the rationale for this, and possible ulterior motives behind what appears to have become a government practice.

Namibians, and especially the Namibian private sector, most often suffer for this. One example is the allegations that City of Windhoek partnered (directly or indirectly) with the Chinese tech company Huawei to monopolise the fibre communications space in Windhoek, possibly through corrupt deals with powerful local officials. The matter was reported to NAMPOL and then ACC many years ago, but nothing came of it. In the meantime, CRAN itself, the enforcer-to-be of this Bill, refused the business plan on which this scheme was based. This refusal was despite a duty to provide same, as the statutory steps required to keep such plan confidential, were not taken. Recently the High Court ruled against CRAN (and the City of Windhoek) on this matter, declaring the license CRAN provided to the City of Windhoek (a full spectrum license no less) as invalid.

China is an authoritarian surveillance state by any definition. One wonders what role the Cybercrime Bill may play in not only moving Namibia closer to becoming such a surveillance state as well, but perhaps even assisting other surveillance states for the advancement of the ulterior motives of a few corrupt elites?

3.2.11. Omnipotent Minister

Apart from the Minister's powers to make far reaching regulations as discussed above, the Minister is given the general powers to regulate *"any matter that is reasonably necessary or expedient to be prescribed to achieve the objectives"* of the Cybercrime

Bill. As stated before, such 'catch-all' statutory powers have previously been declared unconstitutional by the Supreme Court and should not be included future legislation.

The reasons forwarded in these several judgments also speak to EPRA's concerns over the Cybercrime Bill, unlimited powers, which are by their wideness open for abuse, and uncertainty on what Government (even only for a few nefarious actors) may eventually do with them. It is of little comfort to think this may never happen. The question is, can it happen under the Cybercrime Bill? Clearly the answer, as the Cybercrime Bill currently stands, is an unequivocal 'yes'".

3.2.12. Conclusion on Cybercrime Bill

We implore our policymakers to identify the numerous constitutional rights and freedoms (not only the right to privacy in the Cybercrime Bill itself) this Bill will breach and to then continue to engage civil society, the Namibian public, to amend the Cybercrime Bill. Amendment should be to ensure the protection the Bill aims to provide is balanced, reasonable, and achieved through constitutional means while upholding the principles of the Rule of Law.

3.3. Part 6 of the Communications Act (8 of 2009)

With credit to the Legal Assistance Centre (LAC) we provide the following analysis on Part 6 of the Communications Act that came into operation on 1 January 2023. The original commentary is amended to make it time-relevant and for purposes of brevity some references are omitted.[15]

Despite numerous and major concerns raised by numerous civil society- and human rights organisations on Part 6, this part was enacted without any amendment. The enactment of this part marked a major leap forward in establishing an almost totalitarian surveillance state in Namibia. This should be of concern to all Namibians, as well as foreigners visiting Namibia.

[15] For the fully referenced commentary can be obtained from the LAC webpage at www.lac.org.na

3.3.1. Assessment by the LAC

3.3.1.1. Introduction

3.3.1.1.1. What is Data Retention?

Telecommunications networks collect and generate an enormous amount of data that can reveal the identity of users as well as detailed profiles of their communications activity. An increasing number of States are enacting laws that require the retention and organisation of such data for later access by law enforcement officials who execute specific investigations. The theory is that this kind of data can be very helpful in preventing and combating crime, particularly in areas such as child pornography, organised crime and terrorism. Opponents of such schemes point to the widespread invasion of privacy involved, and the potential abuse for unjustified State surveillance, including the danger that such a treasure trove of data can be hacked by unauthorised persons and abused for purposes such as identity theft and corporate marketing.[16]

Namibia has now joined the ranks of States that mandate the retention of data about all telecommunications users. The question under consideration is whether Namibia's requirements for telecommunications data collection and retention might be unconstitutional. Since Namibia has virtually no jurisprudence on the constitutional right to privacy as yet, this memo focuses on key European Union cases and findings of unconstitutionality in India and South Africa.

3.3.1.2. Namibia

3.3.1.2.1. Legal Requirements

Communications Act, section 73

Namibia's Communications Act 8 of 2009, contains a provision that requires telecommunications service providers to collect and retain certain information about their customers:

[16] For a general introduction to the practice that focuses on its risks, see "Introduction to Data Retention Mandates", Center for Democracy & Technology, September 2012, https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf.

Duty to obtain information relating to customers:

> "*73. (1) Telecommunications service providers must ensure that the prescribed information is obtained from all customers.*
>
> *(2) The information referred to in subsection (1) must be sufficient to determine which telephone number or other identification has been issued to a specific customer in order to make it possible to intercept the telecommunications of that customer*."

The Act defines "*customer*" as follows:

> *"customer" means any person who concluded a contract with the provider of telecommunications services for the provision of such services".*

It defines "*telecommunications services*" as follows:

> *"telecommunications services" means services whose provision consists wholly or partly in the transmission or routing of information on telecommunications networks by means of telecommunications processes but does not include broadcast services".*

<u>New Namibian regulations on data retention</u>

The regulations to facilitate it's application of Part 6 have already been issued in 2021. These regulations, which were issued in March 2021 (GN 40/2021), provide details about the duty of telecommunications service providers to collect and retain certain information about their "*customers*". As the regulations were published (gazetted) before Part 6 came into force, the validity of the 2021 is in question. It is unlikely that the enactment of Part 6 on 1 January 2023 automatically renders the 2021 valid and applicable. The 2021 regulations are nonetheless assessed herein on the assumption that they are current.

The regulations contain a more detailed definition of "*customer*" than the one provided in the Act:

"customer", in relation to a service provider, means a person with whom a service provider has concluded a contract to provide a telecommunications service and if the service provider does not belong to a class of persons excluded by regulation 2(2) or regulation 2(3) and "customer" includes a prospective customer.

The excluded persons under regulation 2(2) are persons who provide telecommunications services as an incidental part of another business, by providing access to the internet or other telecommunications services to their customers or to people present on their premises, or those who allows their customers or their customers' guests to use telecommunications services obtained from a different service provider. This would apply, for instance, to internet services provided at places such as coffee shops, restaurants and hotels.

The excluded persons under regulation 2(3) are persons who operate an electronic network for their own purposes and allow employees or other persons to access the internet or other telecommunications services through that network. This would appear to cover businesses that provide telecommunications services through their own servers.

The wording of the definitions of "*customer*" in both the Act and the regulations appears to exclude the use of pre-paid cell phone services, due to the reference to a "*contract*". The regulations specifically indicate that the term "*customers*" does include "*foreign nationals*" (reg 7(1)).

Regulation 7(5) and (6) list the information that a telecommunications service provider must obtain from a customer before providing services to that customer.

"For customers who are natural persons:

(a) the full name of the customer;

(b) the address at which the customer ordinarily resides or if the customer ordinarily resides outside Namibia, the address at which the customer resides while he or she is in Namibia and the address at which the customer works or from which he or she conducts his or her business;

(c) a Namibian identity number or, if the customer in question does not have a Namibian identity number, the number of the document referred to in paragraph

(d) a copy of -

(i) any identity document containing a recent photograph of him or her issued under any law governing the identification of persons in Namibia or any such official document of identity issued by the government of any other country;

(ii) if the customer ordinarily resides outside Namibia or does not have a document referred to in subparagraph (i), a passport issued to the customer;

(iii) if the customer in question does not have a document referred to in subparagraph(i) or (ii), a driving licence or permit containing a recent photograph of him or her, whether issued in or outside Namibia."

For customers who are juristic persons such as companies or voluntary associations:

"(a) the information referred to in subregulation (5) of the natural person representing the juristic person in the conclusion of the contract with the service provider as well as that information of the natural person who will be using the service on behalf of the juristic person or if the service is not being used by a specific natural person, a statement of that fact and an explanation of the purpose of the service;

(b) the full name of the juristic person;

(c) the registration number of the juristic person, if any;

(d) the business address of the juristic person;

(e) a copy of a letter on the letterhead of the juristic person specifying that the person representing the juristic person has the authority to represent the

juristic person in the conclusion of a contract with a service provider to provide telecommunications services."

The collection of the listed information applies to new customers three months after the underlying legal provision comes into force [reg 7(1)], while there is a grace period of 12 months after that date for collecting the information from existing customers [reg 10(1)] – and telecommunications services for any customer must be cancelled if the information is not provided after the prescribed warnings have been given to the customer [reg 10(2)-(7)].

The service provider must store the listed identifying information with reference to the customer's full name and surname to facilitate retrieval [reg 7(7)], and it must retain the information for at least five years following the cancellation of the relevant contract along with the telephone number or other identification provided to the customer under the contract [reg 7(8)].

There is an exemption from the data retention requirement where the telecommunications services are provided by a Namibian service provider in terms of an agreement with a foreign service provider [reg 7(9)] – in other words, where the Namibian service provider is a customer of a foreign service provider that is providing the services.

The customer must complete a form containing the required identifying information and certifying that it is correct. It is a criminal offence to provide false information on this form (reg 8). The same rules apply if the "form" is digital instead of paper-based (reg 9).

Regulation 3(1) lists additional information that telecommunications service providers must collect and store for at least five years in respect of their customers ("*insofar as the information is applicable to the form of telecommunications services in question*"):

"(a) the telephone number or other identification of the customer concerned;

(b) the internet protocol address allocated to a customer (irrespective of whether that address is allocated only for the duration of a telecommunications session or whether it is allocated permanently to a specific customer) in addition to any

information that might be necessary to link a specific packet to a specific customer;

(c) the called number if the call is generated by the user of the service of the service provider and the calling number if the call is initiated by another party than the user of the service of the service provider;

(d) the source and destination of any other telecommunications in a form that is appropriate for the protocol or application in question: Provided that when a packet based protocol is used, it is not necessary to store the data relating to every packet, as long as a summary containing the total amount of data transferred and the source and destination of the transfer, is stored;

(e) the date, time and duration of the telecommunications;

(f) particulars similar to the information referred to in this subregulation relating to supplementary services or facilities used in association with the telecommunications such as multi-party conferencing, call diversion, abbreviated dialing [*sic*] *and voice mail;*

(g) intermediate numbers where the customer establishes conference calling or calls to link through services;

(h) identification of base station and cell site, in respect of all cellular phones or similar devices in such detail and at such resolution as is normally required to render an efficient service; and

(i) the nature of the telecommunications whether it is voice, fax, a message service or any other form of data".

The service provider must store the listed information in a manner that allows retrieval in terms of the regulations or any other law authorising the interception of telecommunications or requiring "*the provision of information relating to telecommunications to another institution*" (reg 3(2)).

Under regulation 5, information from the stored data about a specific person can be requested by a member of the NAMPOL or a staff member of the Namibia Central Intelligence Service, after getting authority from a judge or a magistrate. This application requires a statement of

- the offence being investigated (police) or the reasons for the request (intelligence services);
- the specific person whose information is required;
- a specific description of what information is being requested; and
- a statement under oath giving reasons why the required information is necessary or relevant for the investigation concerned and why it is not expedient to obtain the information in any other manner.

The word "*person*" appears in the singular, suggesting that separate applications are required for information about multiple individuals.

The judge or magistrate can grant the application only after being satisfied on three points: (1) that the requested information is "*necessary or relevant*" for the investigation concerned; (2) that there is "n*o other expedient manner of obtaining the information concerned*"; and (3) that "*the obtaining of the information is authorised by the law of Namibia*".

As is the usual case with similar laws on search warrants, the regulations make provision for NAMPOL (but not the intelligence services) to access customer information from a telecommunications service provider without court authorisation in urgent situations. However, the approach of this provision is odd because it places the decision-making burden on the telecommunications service provider instead of on the trained police officer. The regulations require the police officer making the request to convince the authorised officer at the telecommunications service provider "*on reasonable grounds*" of three things: (1) that the requested information is required urgently; (2) that the delay in getting court authorisation would defeat the purpose of the request; and (3) that a request to the court for authority for requesting the information would have been granted if it had been made [reg 5(7)]. In contrast, in terms of the

Criminal Procedure Act 51 of 1977, it is the police officer who must make that assessment.[17]

This approach presents several problems. Firstly, service providers designate staff members who will function as "*authorised staff members*", and they can be selected individually or identified based on the positions that they hold. The names/positions must be provided to the CRAN, but there are no requirements concerning qualifications, training or even orientation to the relevant law. The selection of these persons/positions is solely at the discretion of the service provider (reg 4). This means that the "*authorised staff members*" of telecommunications service providers are unlikely to have training or experience in legal matters. Secondly, a police officer is subject to statutory authority and could be disciplined if he or she abused the power to bypass judicial authorisation to access information – but there would no similar recourse against staff members of a private telecommunications service provider.

The regulations make provision for modest payments to telecommunications service providers in respect of each "interception target" and each information request, as well as amounts to cover printing costs and electronic copying costs and overtime work required to respond to requests for data or interceptions (reg 6).

3.3.1.2.2. Jurisprudence on Namibia's Constitutional Right to Privacy

Article 13 of the Namibian Constitution covers the protection of privacy, which is the constitutional right most closely implicated by the regulatory scheme described.
Article 13, stipulated in terms of Privacy as follow.

> *"(1) No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.*

[17] S 22. A police official may without a search warrant search any person or container or premises for the purpose of seizing any article referred to in section 20 - (a) if the person concerned consents to the search for and the seizure of the article in question, or if the person who may consent to the search of the container or premises consents to such search and the seizure of the article in question; or (b) if he [the police official] on reasonable grounds believes - (i) that a search warrant will be issued to him under paragraph (a) of section 21 (1) if he applies for such warrant; and (ii) that the delay in obtaining such warrant would defeat the object of the search.

(2) Searches of the person or the homes of individuals shall only be justified:

(a) where these are authorised by a competent judicial officer;

(b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied."

The constitutional right to privacy has been raised in support of cases seeking to invalidate portions of several statutes and one aspect of the common-law – but most of these cases have been decided on other grounds, and none contains any detailed judicial analysis of the right to privacy.

(1) In 1998, the High Court considered provisions in the Indecent and Obscene Photographic Matter Act, 37 of 1967 that prohibited the sale of "*indecent or obscene photographic matter*" as well as the sale of adult toys and novelties intended for use "*to perform unnatural sexual acts*" in violation of the Combating of Immoral Practices Act 21 of 1980. It was alleged that these provisions impermissibly violated the constitutional right to privacy, but the Court stated that the constitutional rights more directly implicated were the right to freedom of speech and expression and the freedom to carry on any trade or business. It found that the restrictions contained in the statutes in questions were overly broad mechanisms for achieving the State objective of upholding standards of decency and morality in society.[18]

(2) In 2002, the High Court considered several provisions of the Combating of Immoral Practices Act 21 of 1980 relating to prostitution. The right to privacy was raised, but the Court found that the only constitutional right infringed was the right to practise any profession, or carry on any occupation, trade or business. It found that, while the law's objective to maintain and promote public order, decency and morality was permissible, some of the expressions of prohibited activities were excessively sweeping and vague, thus going beyond restrictions that are reasonably required for the realisation of the Act's

[18] Fantasy Enterprises CC t/a Hustler The Shop v Minister of Home Affairs; Nasilowski v Minister of Justice 1998 NR 96 (HC).

objectives – and thus falling short of the minimum impairment rule and the requirement that limitations on a constitutional right must be proportional to the interests the Act is seeking to protect.[19]

(3) The Supreme Court, in the process of ruling that the delict of adultery has no further place in Namibian law, found that actions seeking damages for adulterous behaviour are incompatible with several constitutional values, including privacy – but without elaborating on the right to privacy:

> "*But ultimately, it is in respect of the determination of wrongfulness — with reference to the legal convictions of the community informed by our constitutional values and norms — that it is no longer reasonable to impose delictual liability for a claim founded on adultery. Whilst the changing societal norms are represented by a softening in the attitude towards adultery, the action is incompatible with the constitutional values of equality of men and women in marriage and rights to freedom and security of the person, privacy and freedom of association. Its patriarchal origin perpetuated in the form of the damages to be awarded is furthermore not compatible with our constitutional values of equality in marriage and human dignity.[20]"*

Another line of cases has taken the view that laws which provide justifiable interference with the right to privacy – by providing for searches and seizures or access to personal information – must be strictly construed and correctly applied.

(1) In 2019, the High Court considered a case where the procedure for obtaining information in terms of the Anti-Corruption Act 8 of 2003, had not been properly followed. The Court ruled that the legal procedures provided by the law must be strictly followed to avoid an inappropriate infringement of privacy, and held that the evidence obtained without following the prescribed procedures was inadmissible.[21] The crux of the Court's reasoning appears from the excerpt below:

[19] Hendricks v Attorney-General Namibia 2002 NR 353 (HC).
[20] JS v LC 2016 (4) NR 939 (SC), paragraph 55, emphasis added.
[21] S v Lameck 2019 (2) NR 368 (HC).

"Article 13 of the Namibian Constitution deals with the fundamental right of privacy… In terms of this article the right to privacy of a person is not absolute and may be interfered with by law i.e. by Act of Parliament. One such instance is sec 27(1) of the [Anti-Corruption] *Act where the ACC obtains access to a person's bank account which otherwise would have been impermissible due to the right to privacy between a banking institution and its client.*

As to the constitutionally guaranteed rights of a person, the court in Prosecutor-General vs Lameck and Others [2010 (1) NR 156 (HC)] echoed the same sentiments when stating at 172B – C:

"It cannot be emphasised enough that the powers under ss 24 and 25 are so invasive of people's constitutionally guaranteed rights and, potentially, their dignity and ultimately freedom, that this court must exact the highest standard of propriety from those whose interventions might affect those rights.

....

It is trite that 'the Constitution is based on the rule of law, affirms the democratic values of dignity and freedom, and guarantees the right to privacy, a fair trial and just administrative action'. Because of punitive measures provided for in respect of certain provisions in the Act, it requires that the procedural powers of the ACC must be interpreted in such a way that it least impinges on the rights and values of a person. The purpose of incorporating the right to privacy in the Constitution is that no one should be subjected to unreasonable invasions of a person's liberty, privacy, property or effects. Any invasion of these rights must be authorised by law in such manner that it least intrudes [on] *those rights enshrined in the Constitution. As far as it concerns the issue at hand, the issuing of any search and seizure warrant or summons by the ACC, as provided for in the Act, are instances where such encroachment is authorised by law.*

…

…The commission, by the issuing of summonses prior to the initiation of an investigation contemplated in s 18(3), had clearly acted outside its mandate by adopting procedure not prescribed by law.

…

…The correct procedures were available, but not followed. This rendered the summonses invalid and renders evidence obtained consequential thereto unlawful. The Constitution guarantees an accused a fair trial — which includes pre-trial procedures — whereby the accused's dignity and interests must at all times be respected and protected by the courts. To allow evidence that was unlawfully obtained (emanating from invalid summonses) would result in a gross violation of the accused persons' fundamental rights to privacy and a fair trial, guaranteed under the Constitution.

…

The commission's conduct in this regard must be discouraged in the strongest of terms as the courts cannot allow persons or institutions to be subjected to an abuse of power on its part. Although the ACC fulfils an important function in society with its main purpose to fight the seemingly unending scourge of corruption in this country, the commission must be reminded that it is also subject to the Constitution and the law, moreover, that it must give effect to the provisions of the Act, its creator, which brought it into existence.

…

In the result, summonses issued by the ACC on 11 June 2009 are invalid and evidence emanating from the impugned summonses is ruled inadmissible".

(2) Similarly, a 2018 High Court case set aside six search warrants for failure to follow the proper procedure:

"Whereas the right to privacy is guaranteed under art 13 of the Constitution it deserves a very high level of protection and demands a strict interpretation of the search and seizure provisions in the Act. Those provisions may, for obvious reasons, result in a serious encroachment on the rights of those persons subjected to them. Hence,

the courts will construe search and seizure warrants strictly and furthermore carefully scrutinise anything done in pursuance thereof. What this means is that the courts are obliged to employ a strict interpretation of the provisions relating to search and seizure warrants."

Other observations made about the right to privacy, in Namibian cases decided on other grounds, may be helpful pointers to future jurisprudence in this area.

(1) In a 2006 case, the High Court quoted with approval this statement from a South African Constitutional Court judgment:

"It should also be noted that there is a close link between human dignity and privacy in our constitutional order. The right to privacy recognises that human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion. This right serves to foster human dignity."

The Namibian Court observed that those remarks "*also hold true under our Constitution*".[22]

(2) In a case concerning the right to a fair trial, the Supreme Court took note of the similarity in various constitutional formulations on permissible limitations of constitutional rights, taking into account their judicial interpretation. The Court observed that the criteria for limitation of the right to privacy set out in Art 13(1) operate in much the same manner as the authority in Art 21(2) for limitations to the fundamental freedoms enumerated in art 21(1) – suggesting that case law on limitations to Art 21 freedoms may be applicable to limitations on the right to privacy under Art 13(1).[23]

The above-mentioned case may require, looking to leading cases such *Kauesa v Minister of Home Affairs & Others 1996 (4) SA 965 (NmS)*, that a court would require a lawful limitation on the right to privacy to be reasonable, necessary, rationally connected to a legitimate State objective and proportional to that objective. The Kauesa case also stated that, in assessing limitations to rights

[22] Afshani v Vaatz 2006 (1) NR 35 (HC), paragraph 29.
[23] Attorney-General of Namibia v Minister of Justice 2013 (3) NR 806 (SC), paragraphs 29-30.

and freedoms, a court must be "guided by the values and principles that are essential to a free and democratic society which respects the inherent dignity of the human person, equality, non-discrimination, social justice and other such values" (page 977), and that courts "should be strict in interpreting limitations to rights so that individuals are not unnecessarily deprived of the enjoyment of their rights" (page 980).

There is no Namibian case as yet, that provides a detailed focus on the contours of the right to privacy or the appropriate approach to analysing interference with that right.

3.3.1.2.3. International Obligations

International treaties that are binding on Namibia are part of Namibian law by virtue of Article 144 of the Namibian Constitution. The key international treaty on the right to privacy is the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR states that no one "*shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence nor to unlawful attacks on his honour and reputation*", and provides that everyone has "*the right to the protection of the law against such interference or attacks*".

The Human Rights Committee has expressed concern about the invasion of privacy by data retention schemes in its concluding observations on reports from several countries.

For instance, the Committee set out its interpretation of Article 19 in respect of bulk phone metadata surveillance carried out by the United States. It indicated that Article 17 requires that "*measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance*". It also emphasised that infringement on the right to privacy, family, home or correspondence must:

- be authorized by laws that are publicly accessible;
- be tailored to specific legitimate aims;
- be articulated in terms are sufficiently precise and detailed about the circumstances in which any interference with the right is permissible;

- specify the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance and procedures for the use and storage of data collected; and
- provide for effective safeguards against abuse.

Most importantly for the present discussion, the Committee has also urged States Parties to refrain "*from imposing mandatory retention of data by third parties*", and to ensure that "*affected persons have access to effective remedies in cases of abuse*".

In considering the country report of the United Kingdom, the Human Rights Committee made similar observations about UK legislation that provides wide powers for the retention of communications data, without limiting access to such data to cases involving "*the most serious crimes*".

In another example, the Human Rights Committee (HRC) urged Italy to review its regime regulating retention of communications data to ensure that it conforms with the obligations under Article 17 of the ICCPR, "*including the principles of legality, proportionality and necessity*". The HRC emphasised the need for judicial authorization in all cases, effective remedies in cases of abuse, and *ex post facto* notification to individuals who have been placed under surveillance.

In a report on *The Right to Privacy in the Digital Age*,[24] the UN High Commissioner for Human Rights also discussed the test for interference with the rights guaranteed by Article 17 of the ICCPR, emphasising the principles of legality, necessity and proportionality as follow.

> "*(1) With respect to legality, the limitation to privacy rights must be provided for by a law that is sufficiently accessible, clear and precise to enable an individual to know who is authorized to conduct data surveillance and under what circumstances.*
> *(2) In terms of necessity the law must serve a legitimate aim as well as having some chance of achieving the stated goal.*

[24] "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc

(3) Regarding proportionality, the law must impose the least intrusive option available. The degree of limitation to the right must not render the essence of the right meaningless, and it must be consistent with other human rights such as the prohibition of discrimination" (para 23).

In light of these principles, the Report makes the following observation on "*the increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes*":

Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate".

The Report acknowledges that governments justify digital communications surveillance programmes on the grounds of national security, including risks from terrorism, stating that, while this may indeed be a legitimate aim, the degree of interference must still be assessed "*against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose*".

"In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.".

A 2015 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression considered encryption and anonymity in communications considering the rights to privacy and freedom of opinion and expression found in the ICCPR as well as other universal and regional human rights instruments. This Report notes that encryption and anonymity "*provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks*". The Special Rapporteur notes that restrictions on "*encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on*

expression must be provided for by law; may only be imposed for legitimate grounds … and must conform to the strict tests of necessity and proportionality" [and therefore]:

> *"First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation. Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.*
>
> *Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. Even where a State prohibits by law "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3). No other grounds may justify restrictions on the freedom of expression. Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.*
>
> *Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.*

Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online. A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high. Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression…, emphasis added".

The Report asserts that anonymity plays an important role in safeguarding and advancing privacy, free expression, political accountability, public participation and debate and is particularly important for activists and protestors. It notes that laws requiring SIM card registration directly undermine anonymity and "*may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.*"

The Special Rapporteur expressed specific concern about the impact of data retention requirements in this regard:

"Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal

records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information".

The Special Rapporteur, also recommended against requiring identification for all SIM card users and online users:

"… States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users…Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals".

3.3.1.3. European Union (EU)

Data Retention Directive

In 2006, the EU adopted the Data Retention Directive (2006/24/EC) which mandated "*the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*". The objective of the Directive was to serve as a tool "*in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime*". In fact, the Directive followed in the wake of the 2005 terrorist attacks in London.

The Directive required EU Member States to ensure that communications providers retained the data specified in the Directive for a time period set by national law and falling between six (6) months and two (2) years (Art 6).

The data covered by the Directive fell into six categories, covering data necessary to identify: (1) the source of a communication; (2) the destination of a communication; (3) the date, time and duration of a communication; (4) the type of the communication; (5) the user's communication equipment; and (6) the location of any mobile communication equipment. It explicitly did not authorise retention of the content of the communication (Art 5).

The Directive left the rules and procedures for accessing data to national law, subject to the general principles that data could be made available only to competent national authorities and that the procedures and conditions for access must be cognizant of necessity and proportionality requirements (Art 4). The Directive also specified that providers of communications services which retained such data must be required to apply certain "*data security principles*": (1) The retained data must be of the same quality as data on the network, and subject to the same degree of security and protection. (2) It must be protected against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure. (3) There must be safeguards to ensure that the data can be accessed only by specially authorised personnel. (4) The retained data must be destroyed at the end of the specified period (Art 7).

Digital Rights Ireland (2014)

The Data Retention Directive was challenged on the grounds that it impermissibly interfered with several rights protected by the Charter of Fundamental Rights of the European Union, including the right to privacy, the right to protection of personal data, the right to freedom of expression and the right to good administration. The ensuing Digital Rights Ireland case was decided by the Grand Chamber of the Court of Justice of the European Union.[25]

The Court found that the breadth of the data covered by the retention requirements constituted a severe encroachment into the right of privacy, even though content was excluded:

> *"Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.*

[25] Case C-293/12 - Digital Rights Ireland LTD v Minister for Communications, Marine and Natural Resources, and Others and C-594/12 - Kartner Landesregierung and Others, 8 April 2014.

Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (paras 26-27)".

The Court also found that the intrusiveness of such data retention requirements might discourage the use of certain means of communication, thereby impinging on the exercise of the freedom of expression (para 28). In addition, because the requirements involved the processing of personal data, they invoked the data protection principles provided by the Charter (para 29).

The key question was whether the intrusion into these rights was justifiable. Article 52(1) of the Charter provides that any limitation on the exercise of protected rights and freedoms must be (a) provided for by law; (b) respect the essence of the rights in question; and (c) interfere with protected rights only to the extent necessary to meet objectives of general interest or to protect the rights and freedoms of others, subject to the principle of proportionality.

The Court was satisfied that the Directive did not affect the essence of any of the cited rights, and that the objectives of enhancing public security, and combating international terrorism and organised crime, were valid ones. The problem was the proportionality of the infringements (paras 38-ff).

The Court found that the Directive should have provided, "*clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data*" (para 54).

In fact, the interference was not limited to what is strictly necessary, because it required the retention of traffic data in respect of fixed telephones, mobile telephones, Internet access, Internet e-mail and Internet telephones. Thus, covering essentially all means of electronic communication and entailing an interference with the fundamental rights of practically the entire European population, without requiring any evidence suggesting

that their conduct might have any link whatsoever with serious crime (paras 56, 58). In addition, there was no requirement of a specific relationship between the data retained and a threat to public security, nor any limitations to particular time periods, geographical areas or circles of persons likely to be involved in criminal activities or likely to be able to contribute to the prevention, detection or prosecution of crimes (paras 56-59).

An additional problem was the lack of any objective criteria for determining when access to data by competent national authorities would be allowed, nor any provisions on the conditions of access. The Court suggested that the Directive should have made access to the retained data dependent on a prior review carried out by a court or an independent administrative body, with a view to limiting access to the data and its use "*to what is strictly necessary for the purpose of attaining the objective pursued*" (paras 60-62).

Also, the period for the retention of the data was not based on any objective criteria (paras 63-64).

The Court concluded that the Directive, "*entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*" (para 65). It also concluded that the Directive failed to provide sufficient safeguards "*to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data*" (para 66-ff). The Directive therefore failed to satisfy the requirements of proportionality and was ruled invalid (para 71).

Tele2 Sverige AB/Watson and the EU E-Privacy Directive (2016)

In the aftermath of the Digital Rights Ireland case, EU Member States were expected to make their national legislation compliant with the Court's judgment and other EU Directives. This gave rise to more questions about what was permissible under EU law.

Two cases involving Sweden and the UK were joined (Tele2 Sverige AB and Watson[26]) and considered in December 2016 in a preliminary ruling by the Grand Chamber on the

[26] Joined Cases C-203/15: Tele2 Sverige AB v Post-och telestyrelsen and C-698/15: Watson & others v Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland), 21 December 2016,

question of how another EU Directive, the E-Privacy Directive (Directive 2002/58/EC), applies to national telecommunications data retention schemes.

The E-Privacy Directive contains provisions protecting several rights:

- EU Member States must enact legislation protecting "*the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services*", and provides that Member States must accordingly ensure that information and access to stored information takes place only with the consent of the affected person (Art 5).
- Traffic data (any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof) may be stored only as long as it is required for communication transmission, billing or (with the user's consent) marketing, and must be erased after that (Art 6).
- Location data (data indicating the geographic position of the terminal equipment of the user (may be processed only when made anonymous, or with the consent of users or subscribers, and only to the extent and for the time necessary for the provision of a value-added service (Art 9(1)).
- EU Member States may adopt legislative measures that restrict these rights "*when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system*". To these ends, the legislative measures may provide for the retention of data for a limited period justified by the purpose (Art 15(1)).

The Court found that the E-Privacy Directive has the following impact on national legislation on data retention:

full text of the judgment available in English at:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=17504

(1) It precludes national legislation that, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. This approach is disproportionate to the objective, because it provides for the retention of data of persons with no link whatsoever to serious criminal activity or public security (judgment, paras 94-112).

(2) It requires that national legislation governing access to retained data by competent national authorities must ensure that such access does not exceed the limits of what is strictly necessary. It must also contain "*clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data*".

Access must generally be limited to the data of individuals suspected of planning, committing or having committed a serious crime, or of being implicated in some way with a serious crime. However, access to the data of other persons might also be granted where there is objective evidence in a specific case that such data make an effective contribution to combating activities such as terrorism that could threaten national security, defence or public security interests. This means that access must generally be subject to prior review by a court or an independent administrative body, except in cases of "*validly established urgency*".

The law must also provide for notice of the access to the data to be given to the affected persons, as soon as this is no longer likely to jeopardise the investigations being undertaken by national authorities. In addition, there must be provision for review by an independent authority of the data retention scheme's compliance with the data protection principles that apply to the processing of any personal data. This includes measures to protect the retained data against misuse and unlawful access, provision for the data to be retained within the European Union and destruction of the data at the end of the authorised data retention period (paras 113-125).

Concisely, the Court's decision did not indicate that all data retention requirements would be unlawful. It left the door open for Member States to introduce legislation on targeted data retention for the purpose of preventing serious crime (in contrast to "*general and indiscriminate*" data retention) – provided that such measures are limited to what is strictly necessary in terms of the categories of data retained, the persons affected and the time period covered.[27]

In many EU countries, litigation and amendments to laws in force continue in the wake of these decisions of the European Court, as countries consider how to apply the principles articulated in the judgments.[28]

Breyer v Germany (2020)

In this recent case, the European Court of Human Rights considered provisions of Germany's Telecommunications Act that require telecommunications service providers to collect and store certain personal data regarding their customers, after Germany's Federal Constitutional Court had held that they were compatible with German's Basic Law (Grundgesetz).

The law in question obligated telecommunications service providers to store certain information in respect of all users, whether the service provider in question allocated telephone numbers directly or provided connections for telephone numbers allocated by other parties:

1. The telephone numbers and other identifiers of the respective allocation.
2. The name and address of the allocation holder.
3. The date of birth in the case of natural persons.
4. In the case of fixed lines, additionally the address for the line.
5. In cases in which a mobile-communication end device is made available together with the mobile-communication allocation, also the device number of the said device.
6. The effective date of the contract.

[27] Orla Lynskey, "Tele2 Sverige AB and Watson et al: Continuity and Radical Change", European Law Blog, 12 January 2017, https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/.

[28] See, for instance "National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe", Privacy International, September 2017, pages 15-ff, https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf.

This legal provision had been amended in 2016 to oblige service providers to verify the personal data against presentation of an identity card, a passport or other official identity document. This obligation applied to users of pre-paid mobile phone SIM cards and customers who entered into phone service contracts.

The law required that the entities storing the information must make it available to the Federal Network Agency by automated means, so that this Agency could make it available on request to any of several State authorities to the extent that knowledge of the data was necessary for them to execute their legal functions. The list of authorities included, amongst others:

- the courts and criminal prosecution authorities;
- law-enforcement authorities "*for purposes of averting danger*";
- customs investigation offices, for various customs-related purposes;
- intelligence agencies;
- emergency service centres; and
- the Federal Financial Supervisory Authority.

The main question before the Court was whether the law impermissibly infringed the right to private and family life in the Charter of Fundamental Rights of the European Union. The parties agreed that the law infringed these rights, so the issue was whether the infringement was justifiable – with the key point being whether the interference was proportionate and struck a fair balance between competing public and private interests.

The Court placed significant weight on the fact that the law required storage of only a limited data set relating to identification of the user, without calling for the storage of any individual communication events or data that could track users' movements. It relied on this distinction to distinguish this case from the previous ones decided by the Court of Justice of the European Union (discussed above), even though the law required the collection and storage of this limited data in respect of all users instead of only persons under some kind of suspicion.

In terms of access to the data, the Court found that even though the list appears broad, all authorities cited were concerned with law enforcement or the protection of national security. It found further protection against "*excessive or abusive information requests*", by the fact that "*the requesting authority requires an additional legal basis to retrieve*

the data", and the provision that limits information retrieval to necessary data. Another safeguard was the law's requirement that any authority that retrieves information must erase any data they do not need without undue delay. The Court also noted that each retrieval must be recorded to allow for supervision by independent data protection authorities. These authorities have power to consider complaints from anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies.

The Court thus concluded that the challenged law did not constitute an impermissible interference with the right to private and family life.

The dissenting opinion by one judge took the view that there was an unjustified infringement of the right to private and family life, emphasising the following points:

- Access to the personal data in question was not confined to issues of terrorism or other serious crimes or national security risks, but extended to other authorities such as customs investigation services, emergency services, the financial supervisory authority and several intelligence agencies.
- Even though the law did not mandate the storage of any sensitive personal information, it covered data that enables a person to be linked with a phone number or a phone number and thus with communications made through that number, which could reveal sensitive personal information.
- Because the law affected all telecommunications users, the case was comparable to the Digital Rights Ireland case and the Tele2 Sverige/ Watson cases which invalidated similar laws.
- The majority judgment failed to consider the importance of anonymity in promoting the free flow of ideas and information.
- The failure to fully consider the impact of the law meant that the majority opinion underestimated the level of interference with the right to private and family life (para 9) – which in turn affected the assessment of proportionality.
- Although the law required a legal basis for accessing the identifying data, it did not set a threshold limiting data collection to the investigation of serious crimes or specific serious threats to national security.
- The search function authorised by the law does not limit the data retrieved to specific telephone numbers or names, but may extract personal data

concerning a large number of persons who have not even an indirect or remote link to criminal or regulatory offences.

- There are insufficient safeguards against misuse and abuse of personal data in the regulatory scheme. Retrievals of personal data did not require an order by a judicial or otherwise independent authority, and those requesting access via the Federal Network Agency did not have to motivate their requests with reasons. Information requests could take place without the knowledge of the telecommunications service provider or the relevant subscriber. There is no legal duty to notify a mobile telephone subscriber at any stage that his or her personal details have been retrieved – which prevent any review of the information retrieval, especially where there is no further investigation or surveillance of the individual in question. The supervision by the data protection authority cited by the majority was not adequate given the huge number of data sets at issue.

The dissenting judge thus concluded that the law violated the Charter's protection for private and family life (para 27).[29]

3.3.1.4. India

In India, biometric-backed identification numbers are issued by the Unique Identification Authority of India (UIDAI) under the Aadhaar Act. ('*Aadhaar*' is a Hindi word that means 'foundation' or 'base'.) Each legal resident in India can enrol in the *Aadhaar* system by submitting personal information along with certain biometrics (currently fingerprints and an iris scan). The person in question is then assigned a unique twelve-digit identity number that is intended to serve as primary form of identification. The identification data is stored in a centralised data base. *Aadhaar* cards are issued to those who have registered, but the crux of the scheme is the unique identification number which can be authenticated against the individual's biometrics. The law governing the scheme gives State authorities a duty to secure all identification information that they hold, and prescribe rules for data-sharing. It is not legally mandatory to enrol in the *Aadhaar* scheme, but so many state services require secure identification that it is compulsory in a practical sense.

[29] See also Judith Vermeulen, "Bulk retention of private-sector subscriber data for governmental purposes does not violate the Convention: Breyer v. Germany", Strasbourg Observers, 5 March 2020, https://strasbourgobservers.com/2020/03/05/bulk-retention-of-private-sector-subscriber-data-for-governmental-purposes-does-not-violate-the-convention-breyer-v-germany/.

The constitutionality of the overarching *Aadhaar* scheme was challenged on numerous grounds in a case decided by the Supreme Court in 2018. The issue most relevant to this discussion is the assertion that the entire identification scheme violated the right to privacy, which is not directly articulated in the Indian Constitution but has been established and developed through jurisprudence. The Court described privacy as being a right that "*ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusions*" and is furthermore "intrinsic to freedom, liberty and dignity" (majority opinion).

It was argued that the scheme constituted an invasion into the personal right to privacy because it could "*lead to a surveillance state where each individual can be kept under surveillance by creating his/her life profile and movement as well on his/her use of Aadhaar*". The opposing views on the overall scheme were summarised by the Court as follows:

> *"Those in favour see Aadhaar project as ushering the nation into a regime of good governance, advancing socio-economic rights, economic prosperity etc. and in the process they claim that it may make the nation a world leader… Those opposing Aadhaar are apprehensive that it may excessively intrude into the privacy of citizenry and has the tendency to create a totalitarian state, which would impinge upon the democratic and constitutional values".*

In Indian jurisprudence, privacy has three aspects: (i) intrusion with an individual's physical body; (ii) informational privacy; and (iii) privacy of personal choices. To test whether there has been an unwarranted interference with the right to privacy, the Court must apply a three-part test of proportionality: (a) the interference with the right must be sanctioned by law; (b) the proposed interference must be necessary in a democratic society for a legitimate aim; and (c) the extent of such interference must be proportionate to the need for such interference.

Applying the above test, the Court found that the overall identification scheme passed the test of constitutionality, by imposing a minimal interference with privacy which was necessary for the legitimate State purpose of enrolling unprivileged and marginalised members of the society, to empower them by giving them access to welfare schemes

that would enhance their dignity. The Court held that the *Aadhaar* Act "*has struck a fair balance between the right of privacy of the individual with right to life of the same individual as a beneficiary*" (para 313).

Once the Court had established the constitutionality of the underlying *Aadhaar* scheme, it considered some specific aspects of that scheme separately.

One of these was a 2017 directive requiring all mobile service subscribers (pre-paid or post-paid, and new or existing) to link their mobile numbers to their *Aadhaar* number. In addition to objecting to the fact that this requirement was contained in a circular rather than a law, the Court also noted the existence of less intrusive alternatives: "*For the misuse of such SIM cards by a handful of persons, the entire population cannot be subjected to intrusion into their private lives.*" The Court thus found the requirement to be an unconstitutional interference with the right to privacy.

A separate judgement by Justice Chandrachud disagreed with the majority on the overarching constitutionality of the *Aadhaar* scheme but agreed with the majority holding on the unconstitutionality of linking mobile phone usage with *Aadhaar* identity. This separate opinion elaborated on the issue of proportionality, after noting that the State does "*have a legitimate concern over the existence of SIM cards obtained against identities which are not genuine*".

> *"But the real issue is whether the linking of Aadhaar cards is the least intrusive method of obviating the problems associated with subscriber verification. The state cannot be oblivious to the need to protect privacy and of the dangers inherent in the utilization of the Aadhaar platform by telecom service providers. In the absence of adequate safeguards, the biometric data of mobile subscribers can be seriously compromised and exploited for commercial gain. While asserting the need for proper verification, the state cannot disregard the countervailing requirements of preserving the integrity of biometric data and the privacy of mobile phone subscribers. Nor can we accept the argument that cell phone data is so universal that one can become blasé about the dangers inherent in the revealing of biometric information….*
>
> *…The mere existence of a legitimate state aim will not justify the means which are adopted. Ends do not justify means, at least as a matter of constitutional*

principle. For the means to be valid, they must be carefully tailored to achieve a legitimate state aim and should not be either disproportionate or excessive in their encroachment on individual liberties…

Mobile technology has become a ubiquitous feature of our age. Mobile phones are not just instruments to facilitate a telephone conversation. They are a storehouse of data reflecting upon personal preferences, lifestyles and individual choices. They bear upon family life, the workplace and personal intimacies. The conflation of biometric data with SIM cards is replete with grave dangers to personal autonomy. A constitution based on liberal values cannot countenance an encroachment of this nature. The decision to link Aadhaar numbers to SIM cards and to enforce a regime of e-KYC [Know Your Customer] authentication clearly does not pass constitutional muster and must stand invalidated."

During January 2021, the Supreme Court received a group of petitions requesting re-examination of the majority holding in the 2018 case – but, by a vote of 4-1, declined to review the 2018 decision.

3.3.1.5. South Africa

In South Africa, the Constitutional Court recently invalidated the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) on the grounds that it constituted an impermissible interference with the constitutional right to privacy.[30]

This Act covered various forms of surveillance and interception of communications – including data retention by telecommunications providers and access to that data by State officials, which was covered by Chapter 7 of RICA (sections 39-41). The Constitutional Court judgment did not focus on this aspect of the law, but many of its

[30] Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC & Others 2021 (3) SA 246 (CC),
https://collections.concourt.org.za/bitstream/handle/20.500.12144/36631/%5bJudgment%5d%20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf?sequence=42&isAllowed=y.
The Act, which has been amended several times, was sourced through the subscription service Juta's Statutes of South Africa.

concerns about surveillance in general would be applicable to this form of data retention and access also.[31]

As a background to the Constitutional Court's consideration of the Act's general impact on the right to privacy, the Court noted that the country's *apartheid* history was characterised by "*the wanton invasion of the privacy of people by the state through searches and seizures, the interception of their communications and generally by spying on them in all manner of forms*" (majority Constitutional Court judgement, para 26) – a point that is equally relevant to Namibia. The Court also noted at the outset that invasion of an individual's privacy also infringes that individual's right to dignity, which is of fundamental importance (para 28). However, it also took note of the argument that the law serves the important purpose of facilitating investigation and combating of serious crime, protecting national security and maintaining public order – thereby ensuring the safety of the population (para 29).

Against this backdrop, the Court considered specific components of the legal challenge to RICA. Only those which could have relevance to Namibia's regulatory scheme on telecommunications data are discussed here.

Notification

The Court was disturbed by the lack of provision for notification to the subject of surveillance, even after the fact. When authority is given for a traditional search, this eventually comes to the notice of the person who is searched. But when surveillance is authorised, the person whose communications are intercepted may never know. This complete secrecy makes surveillance under the Act susceptible to abuse. The lawfulness of the authority for the surveillance can never be challenged if the surveillance remains unknown – which could lead to a culture of impunity on the part of law enforcement officials. The upshot is that "an individual whose privacy has been violated in the most intrusive, egregious and unconstitutional manner never becomes aware of this and is thus denied an opportunity to seek legal redress for the violation of

[31] This portion of the Act was challenged in the High Court on the grounds that it lacked adequate safeguards regarding the archiving of data and subsequent access to it. More specifically, the applicants challenged the requirement that the specified data must be retained by electronic communications service providers for 2 to 5 years, and the procedures for managing this data in question (examining, copying, sharing, sorting through, using, destroying or storing it). The High Court dismissed the challenge regarding the period of retention on the grounds that this was within the province of Parliament to decide, but upheld the challenge regarding insufficient safeguards for the management of the data in question (as described in the majority Constitutional Court judgement, para 18).

her or his right to privacy" (paras 38-44). The Court thus held that post-surveillance notification should be the default position, unless the State can present justifiable reasons why an exception should be made in a specific case (paras 45-48).

Although this part of the constitutional challenge applied to surveillance, it would be equally relevant to law enforcement access to retained communications data about an individual; to prevent abuses of the process, it can be argued there should be a requirement that the individual receives notification of access if this would not jeopardise the object of the investigation.

Safeguards for *ex parte* process

In respect of authority for surveillance, an issue of concern is that the application is necessarily *ex parte* – since the surveillance would be pointless if the subject were aware of it in advance. This means that the application is granted "*on the basis of information provided only by the state agency requesting the direction*". The judge must decide based on one-sided information and, unless there are obvious shortcomings, inaccuracies or falsehoods, the decision-maker is not in a position "*meaningfully to interrogate the information*" (para 96). The applicants asserted that this undermines the principle that both sides must be heard, and so violates the right to fair hearing; other forms of *ex parte* proceedings are usually granted only on an interim basis, but orders that allow interception of communications are final. Therefore, the applicants suggested that some form of adversarial process should be applied to ensure "*that the interests of the subject of surveillance are properly protected and ventilated". They suggested that a "public advocate*", could play this role.

The Constitutional Court held that the absence of sufficient safeguards to address the fact that authority to intercept communications is sought and obtained *ex parte* was a factor that rendered the law unconstitutional. However, it declined to recommend a specific mechanism to remedy this problem, ruling that the "*choice of safeguards to address the inadequacies resulting from the ex parte nature of the process is something best left to Parliament*" (paras 95-100).

Again, although this issue was discussed in the context of the interception of communications, it also has relevance for *ex parte* applications for access to retained communications data about an individual.

Management of information

The applicants also challenged the law's lack of safeguards for how information from intercepted communications is handled, stored and eventually destroyed. The Court was concerned that the legal scheme provided no clarity or detail on:

> *"what must be stored; how and where it must be stored; the security of such storage; precautions around access to the stored data (who may have access and who may not); the purposes for accessing the data; and how and at what point the data may or must be destroyed. Thus there is a real risk that the private information of individuals may land in wrong hands or, even if in the "right" hands, may be used for purposes other than those envisaged in RICA. All this exacerbates the risk of unnecessary intrusions into the privacy of individuals" (para 107).*

The Court concluded that the law was rendered unconstitutional to the extent of its failure to adequately prescribe procedures, "*to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data*" (para 108).

This would seem to apply also to retained communications data – perhaps even more forcibly since this data is stored by telecommunications service providers rather than by State officials. In fact, one amicus (advisor to the court) in the South African case urged the Court to rule that this concern applied with equal force to data retained by private telecommunications service providers; the Court declined to do so on the grounds that this issue had not been fully ventilated due to the manner in which it was raised, but it did observe that "*in our age of mass data surveillance, private actors arguably pose a comparable threat to privacy as does the state*" (para 111).

Overall, the Court found RICA to be unconstitutional to the extent that it fell short in respect of these and other safeguards. It suspended, the declaration of unconstitutionality for 36 months to afford Parliament an opportunity to cure the defects that were noted, and read certain safeguards into the law as an interim measure.[32]

[32] There was one dissenting opinion which focused on an issue peculiar to the South African law which is not relevant to the discussion here.

3.3.1.6. Possible Constitutional Problems with the Namibian Regime

An examination of the relevant international standards and comparative jurisprudence points to some worrying problems with Namibia's regulatory scheme as follow.

1) Overbreadth leading to lack of proportionality

One characteristic of the scheme of immediate note is that telecommunications service providers are required to collect and store data about every user who meets the definition of "*customer*" – thus retaining a massive amount of data of which only a tiny proportion is likely to ever be requested by NAMPOL or intelligence services. This would likely mean that the approach taken could not satisfy the principle that justifiable interference with a constitutional right must be as minimal as possible, and only what is reasonably necessary to serve the objective.

As has been seen in respect of other jurisdictions, it is more likely that a targeted data retention scheme will pass constitutional muster - with data being retained and stored in the first place *only in respect of persons who are reasonably suspected of having some connection to serious crime*.

This is a data preservation approach rather than a data retention approach:

> Data preservation is an alternative to data retention that can help law enforcement while minimising the impact on human rights. Under a data preservation regime, a law enforcement officer can demand that an Internet company begin storing – "preserving" – data relevant to a specified investigation or proceeding. Typically, the company is required to continue preserving this data for a period of time, such as 90 days.[33]

Indeed, this is the approach that is taken by the latest version of Namibia's Cybercrime Bill (in the draft circulated by the Ministry of Information, Communications and Technology for comment in June 2021) (also discussed above):

[33] See, for example, "Introduction To Data Retention Mandates", Center for Democracy & Technology, September 2012, page 6, https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf.

Preservation

20. (1) If a member of the Namibian police is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation might be lost, modified or destroyed, that member may issue a written notice instructing a person in control of that computer data to ensure that the data described in the notice must be preserved for the period specified in the notice which period may not be longer than seven days.

(2) A notice referred to in subsection (1) may be extended by a judge or magistrate for a period that does not exceed three months at a time.

The types of data that must be collected and retained may also be found to go beyond what is strictly necessary for the law's purposes. As been noted elsewhere, the listed data would be sufficient to provide a detailed profile of communications activity that can reveal many aspects of a person's private life, including their relationships, interests and movements. This list should be re-considered in light of the principle of proportionality.

2) Lack of suitability to serve the objective

Another question of concern is what purpose the data retention requirements can serve given the exclusion of (a) pre-paid telecommunications services and (b) services accessed via foreign telecommunications service providers. Anyone with a communication to hide would surely simply utilise one of the excluded channels – meaning that the interference with the privacy of other customers would be likely to be for naught.

Yet there might be problems entailed with broadening the scheme.[34] For instance, in September 2014, the Romanian Constitutional Court invalidated an Emergency Ordinance that required registration of all pre-paid SIM cards and the users of free public Wifi hotspots, on top of more general requirements about the retention of data of users

[34] For an overview of the issue of requiring identification of SIM care users, see "The Mandatory Registration of Prepaid SIM Card Users: A White Paper", GMSA, November 2013, www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf. GSMA, which is commonly referred to only by its acronym, is the Global System for Mobile Communications Association, with "GSM" originally denoting Groupe Spécial Mobile. It represents the interests of mobile operators worldwide.

of telecommunications services.[35] As with general telecommunications data retention, the motivation for the new legal provisions was "*the need to adopt measures to facilitate criminal investigation activities or those for knowing, preventing and counteracting risks or threats to national security*". The law was enacted after police tragically failed to save a teenage girl who had been abducted but managed to call the 112 emergency number three times before she was murdered.

The Court noted that the basic data retention regime contemplated the completion of a standard form when entering into a contract for telecommunications services, in advance of the provision of those services. But in the case of pre-paid services and access to public Wifi networks, the sale is often via an intermediary dealer – which raises serious questions about who would bear the duty to guarantee the confidentiality and security of the data and prevent unauthorised use. In the case of public Wifi networks, the Court noted that such services are often accessed through private entities such as commercial and leisure areas, cafes, restaurants, hotels and airports, or via public institutions such as educational facilities, public libraries and medical clinics (para 41). The Court continued (as machine-translated):

> *The imposition on these persons of the obligation to retain and store personal data requires, in a correlative manner, the express regulation of appropriate, firm and unequivocal measures, such as to ensure the confidence of citizens that the personal data they have provide are registered and kept confidential. In this respect, the law is limited to establishing measures for data retention and storage, without amending or supplementing the legal provisions on the guarantees that the state must provide in the exercise of the fundamental rights of citizens. However, the regulatory framework in such a sensitive area must be carried out in a clear, predictable and non-confusing manner, so as to remove, as far as possible, the possibility of arbitrariness or abuse of those called upon to apply the legal provisions (para 41).*

The Court invalidated the provisions at issue on the basis that they lacked the precision and predictability necessary for proportional interference with individual rights and failed

[35] The challenge to the law was mounted by the Romanian Ombudsman, at the urging of several human rights groups. The case is "Decizia Curții Constituționale nr. 461/2014 – lege prepay și înregistrare utilizatori WiFi, DECIZIA Nr.461 din 16 Septembrie 2014", https://privacy.apti.ro/decizie-curtea-constitutionala-prepay-461-2014/, available only in Romanian, with machine translation into English.

to ensure the confidentiality of personal data - thus infringing the very essence of fundamental rights regarding privacy, family and private life and the secrecy of correspondence, as well as freedom of expression (paras 44, 46).[36]

3) No *ex post facto* notice to affected individuals and no other safeguards for *ex parte* proceedings

It is a point in favour of the Namibian law that access to retained data would ordinarily require authorisation by a court. However, the concerns raised by the South African Constitutional Court in respect of *ex parte* proceedings are relevant here. The affected persons may never know that their data has been accessed – in contrast to traditional searches and seizures which generally become known by their nature. This creates a situation where the validity of the access may never be challenged. While the person who is being monitored could normally not be informed of the situation at the time without defeating the purpose of the investigation, provision could be made for notice to the affected person after the investigation was finalised (regardless of its outcome).

In addition, an *ex parte* request for access to stored data has a final rather than an interim outcome, yet the procedure incorporates no adversarial component. Some have proposed that a public advocate could be used to play such a role; perhaps the Office of the Ombudsman could serve such a function in Namibia.

4) Inappropriate decision-making process in urgent situations

As detailed above, the regulations make provision for NAMPOL (but not the intelligence services) to access customer information from a telecommunications service provider without court authorisation in urgent situations. Even if this exception to court authorisation were found to be warranted, the procedure places the key decision-making burden on the authorised persons appointed by telecommunications service providers instead of on trained police officers. It seems inappropriate to give this responsibility to a private individual rather than to the police officer concerned.

[36] A subsequent attempt to introduce a similar law was also declared unconstitutional. See Valentina Pavel "Romania: Mandatory SIM registration declared unconstitutional, again", European Digital Rights (EDRi), 26 February 2020, https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/. which reports that this case invalidated the law in question on procedural grounds without conducting a substantive analysis.

5) No attention to data security principles

Although Namibia does not yet have a data protection law in place, guidance on basic data protection principles can be drawn from the African Union Convention on Cyber Security and Personal Data Protection, 2014 which has been signed and ratified by Namibia, but has not yet received sufficient support to come into force. Whether or not the approach to telecommunications data is narrowed, the scheme needs to comply with basic data protection principles – including measures pertaining to the security of the data and protections for confidentiality and the prevention of unauthorised access, and provision for the erasure or destruction of data after the requisite time period for its retention has expired.

3.3.1.7. LAC's Conclusion

Based on the survey of comparative law outlined here, it seems likely that Namibia's telecommunications data retention scheme might be found to be an unconstitutional infringement of the right to privacy overall, given the intrusion into the privacy of large segments of the population in a manner that has a questionable ability to serve the intended objectives. At the very least, it seems to be unconstitutionally faulty in some key aspects relating to the breadth of its coverage and the kinds of data required to be collected, the lack of procedural safeguards and the lack of attention to data protection principles. It does not seem to be appropriately proportional to its aims.

3.3.2. IPPR: Articles on SIM Card Registration and Service Disruption

This subsection contains a thought-provoking article written by Frederico Links of the IPPR. It was published in *The Namibian* on 5 August 2022 and serves as an excellent illustration on the possibility and consequences of the abuse of power that can follow the provisions of Part 6 of the Communications Act. This article was commissioned by the Media Policy and Democracy Project (MPDP), an initiative of the University of Johannesburg's Department of Journalism, Film and TV; and Unisa's Department of Communication Science.

Imagine you're in a food price protest in August 2023.

It's been seven months since the operationalising of mandatory SIM card registration and data retention regulations under Part 6 of the Communications Act of 2009.

You, and everyone else in the protest of about 300 to 500 people have your phone out recording the demonstration and communicating with others about what's happening via WhatsApp or social media.

But because you have registered your SIM card and are now subject to data retention rules that have also come into effect in early 2023, everyone in the demonstration appear as clearly identifiable pinpoints on the surveillance systems of the state.

They can see exactly where you are, who you're standing close to, and who you're communicating with.

And they can use that information to target you, individually, or the whole group with a communication or internet shutdown, or they can isolate and target those they perceive to be ringleaders, or track them to where they can be picked up, arrested or isolated for intimidation.

WHAT THEY HAVE

Through your SIM registration with your mobile service provider the state will have your name, home address, identity or passport numbers, and or a copy of your driving licence containing your photo.

At the same time, under the data retention rules, they will have your telephone number, your internet protocol address, all the numbers you call, the date, time and duration of all your calls and internet activities, the closest base station and cell site when you made those calls or were online, and the nature of your telecommunications – whether it was a call, an SMS or WhatsApp message or any other form of data usage, such as accessing a social media platform.

With all this information, the Namibian state surveillance apparatus can know and pinpoint where everyone with an active Namibian SIM card or access to an internet service in Namibia is with absolute accuracy at any moment in time beyond January 2023.

They'll know when, how and who you're communicating with at all times, and they'll know when, how and how long you've been accessing the internet at all times.

They'll know all this because your mobile and internet service provider has to store all this data for five years.

This effectively means from January 2023 onwards, everyone using a mobile or internet service in Namibia will be under permanent, around-the-clock surveillance by their service provider at the behest of the state.

This is permanent mass surveillance.

This permanent mass surveillance is being implemented under the pretexts of 'national security' and 'crime prevention' through the Communications Regulatory Authority of Namibia (CRAN).

CRIME PREVENTION?

But these pretexts are highly questionable.

Over the last decade and a half, or so, more than 150 countries worldwide have adopted mandatory SIM card registration and data retention schemes similar to what Namibia will be implementing as from 2023.

And yet, the last decade, from about 2010, has seen an exponential growth in global cybercrime, indicating that the widespread adoption of mandatory SIM card registration and data retention schemes has not deterred or prevented cybercrime.

In a January 2019 report, international privacy and digital rights organisation Privacy International (PI) stated: "SIM registration has not been effective in curbing crime, but instead has fuelled it: States which have adopted SIM card registration have seen the growth of identity-related crime, and have witnessed black markets quickly pop up to service those wishing to remain anonymous. Moreover, SIMs can be illicitly cloned, or criminals can use foreign SIMs on roaming mode, or internet and satellite telephones, to circumvent SIM registration requirements."

HOW NAMIBIANS FEEL

When the scenario of the hypothetical protest in the context of permanent mass surveillance was sketched to two groups of Namibian young people at the recent YouthQuake event, hosted by the Namibia Media Trust, the overwhelming responses were shock and alarm.

Some young people said the scope of the state's access to their communication and online footprints would deter or make them more cautious about using mobile telecommunications or internet services.

Namibians appear to not be in favour of having their mobile or online communications permanently spied on by the state.

In round 8 of the Afrobarometer survey, Namibians were asked two questions under question 74 of the survey, the results of which were fully released in October 2021.

The first question asked whether the government "should be able to monitor private communications, for example on mobile phones, to make sure people are not plotting violence?", to which only 38% of respondents answered yes.

The second question asked whether people "should have the right to communicate in private without a government agency reading or listening to what they are saying?", to which 60% answered yes.

Namibians' fears are well-founded, for the Uganda-based Collaboration on International ICT Policy for East and Southern Africa, in a September 2021 report states that such extensive personal data retention schemes by countries across the continent have "greatly undermined the ability of citizens to communicate anonymously, given the amount of personal data that is collected, retained and shared through these exercises, without adequate oversight and respect for individuals' privacy rights".

Another article by the IPPR, also published in *The Namibian*, 23 December 2022, addresses the unintended (or perhaps secretly planned) consequences of implementing Part 6 of the Act. The largest cell phone communications provider in Namibia, MTC (which is majority government owned, and thus government controlled), now requires the collection of biometric data of customers, which is not required by law. Although not required by law, all MTC customers must comply, or lose the ability to communicate via

MTC's cell / data networks. It can be safely assumed that the bulk of Namibia's cell phone users use MTC's network. This article follows:

Questionable Harvesting of Biometric Data

MTC has been scanning fingerprints and taking face photos while the legal framework only requires basic information for SIM registration.

In a usually empty retail space just around the corner from the box office inside the MTC Dome in Swakopmund, a crowd of people filled out forms and then queued to have their fingerprints scanned and then a photo taken of their faces by MTC Namibia employees.

The same was happening inside the MTC Dome arena where, under a branded gazebo, MTC Namibia officers were also accepting forms, scanning fingers [fingerprints] and taking photos of patrons of the four-day Namibia Sport Expo, which ran from 8-11 December 2022.

Namibia's biggest mobile and internet service provider used the opportunity of the sport expo to encourage its customers who attended the event to also register their SIM cards before 31 December 2022.

From the beginning of October 2022, Namibians were called on to voluntarily register their SIM cards during a three-month window period so that by the time mandatory SIM card registration was to be implemented, as from 1 January through to December 31 2023, they were already compliant with the law.

What was striking about what was happening at the MTC Namibia SIM card registration points was the collection of fingerprint and facial biometric data.

The regulations for Part 6 of Chapter 5 of the Communications Act of 2009, as well as the further conditions on telecommunications licensees, require operators to collect basic information such as names, dates of birth, addresses, and copies of identification documents to register a SIM card. There is no mention of biometric information being legally required or necessary for SIM card registration.

From the start of the three-month window period for SIM card registration that began on 1 October, the Institute for Public Policy Research (IPPR), and this writer in particular, received a number of queries through various channels – from emails to phone calls

and SMSs – from associates and members of the public who expressed concern and discomfort that they are required to hand over biometric data in order to register their SIM cards.

Dubious practice

These concerns have been raised with the management of both the Communications Regulatory Authority of Namibia (CRAN) and MTC Namibia.

Specifically, the CRAN management was asked what the regulator's position was on the harvesting of facial and fingerprint biometric data by telecoms companies for the purpose of registering subscribers in the absence of legislated data protection safeguards.

MTC Namibia was asked on what legal basis it was collecting facial and fingerprint biometric data in order to register customers.

On 9 January 2023, CRAN responded: "Operators are required to only collect customer identification information as stipulated in the regulations and conditions. Kindly contact Mobile Telecommunications Limited for their consideration and possible response to [your other questions]."

CRAN had also sent a complaint form a few days earlier, encouraging this author to file a complaint for adjudication, if that was what was desired to address the matter.

In mid-December 2022, MTC Namibia's Tim Ekandjo had indicated that this writer would receive a response to the questions sent to the state-owned telecoms firm on Wednesday, 21 December 2022. When contacted again in early January 2023 for a response, Ekandjo did not commit to responding to the questions or the issues as sketched in the article that was published.

That said, the issue of a regulator being silent or complicit in the face of legally questionable or unlawful biometric data collection practices by a telecommunications company is not only a concern in Namibia, but across the African continent.

In Kenya, since late 2021, human rights defenders have been battling the Kenyan regulator and the country's largest mobile operator, Safaricom, over the company's unlawful collection of subscriber biometric data for SIM card registration.

After first siding with Safaricom, and other mobile operators who had been harvesting biometric data from subscribers, in April 2022, the Communications Authority of Kenya (CAK) backtracked in the face of legal challenges from civil society and members of the public and conceded that Kenyans were not legally required to provide biometric data to register their SIM cards.

Since then, Safaricom – which had stopped collecting biometric data in May 2022 – has been called upon by human rights organisations and the Law Society of Kenya to delete the illegal biometric database it had created during its SIM registration drive.

In an open letter to Safaricom published online on 14 December 2022, a campaigner for global human rights organisation Access Now, Jaimee Kokonya, once again called on the company to delete the illegal biometric database, stating: "Safaricom misrepresented the law's requirements to people who subscribe to your services on several occasions between November 2021 and April 2022, informing them that they were in fact required to provide facial biometrics in order to comply with SIM registration requirements, and warning that failure to do so would see your company disconnect their services. Collecting facial biometrics during this process is in clear violation of various laws."

The issue of unregulated or legally questionable collecting of biometric data was also recently spotlighted by the Uganda-based Collaboration on International ICT Policy for East and Southern Africa (CIPESA), in its September 2022 report titled 'The Rise of Biometric Surveillance'.

The CIPESA report states that a feature of biometric data collection practices by African states and mobile operators has been a lack of transparency and that "the public provides biometric data without question or prior informed consent, but out of necessity in order to acquire critical services".

"Where there have been public campaigns, these have been carried out over short periods and sporadically, often with limited disclosures and misleading information on the technologies and the purpose of the programmes [and] coercive directives to ensure compliance without question," CIPESA adds.

'Lawful' processing

Namibia does not have an online privacy and data protection law, but consultations around such a draft law have been ongoing since 2019, with the latest call for public inputs ending on 30 November 2022.

The draft law does not deal in depth or appropriately with biometric data, even though Namibia is looking to be compliant with the General Data Protection Regulation of the European Union (EU), which is considered the best practice example for data protection internationally and which prohibits the collection and processing of biometric data, except under very specific circumstances.

An online summary of GDPR's provisions dealing with biometric data clearly states: " The processing of biometric data generally produces higher risks to the freedoms and rights of the individual. As a result, the processing of biometric data for the purpose of uniquely identifying a natural person is prohibited according to art. 9 (1) of GDPR."

According to GDPR, and other international best practice guidance, the processing of biometric data should be "lawful", meaning based in clear and comprehensive legal frameworks.

Against this backdrop, the question is whether what is happening in Namibia right now – MTC Namibia collecting biometric data in the absence of a legal framework and safeguards while the regulator is seemingly silent – is "lawful"?

EPRA considered the question as to whether the forced collection of biometric data is lawful, and the answer is an emphatic "No". One can argue whether the collection of such data is indeed forced. The bulk of cell phone users in Namibia are MTC customers. Only in large urban centers are there alternative (private sector) providers. Thus, non-compliance with MTC's requirements will leave one essentially, disconnected. If all MTC customers would refuse to comply, the bulk of Namibian cell phone (and data) users will become disconnected. There can thus be no doubt that MTC's requirements are forced even if customers grudgingly agree to comply – they simply have no choice.

Subsequent to the IPPR article above, MTC did explain (as per media reports) that the reason for requiring biometrics is, because some who come to register SIM cards attempt to defraud MTC with false documents. This may well have been the case, but it

still does not warrant MTC usurping the powers of the legislator, re-writing the statutory requirements, and breaching the constitutional rights of over two million active MTC subscribers.[37]

Most recently, CRAN instructed MTC to stop its collection of biometric data for the purpose of SIM card registration. Alarmingly, MTC did not hesitate to inform the public that it will not adhere to CRAN's direction, and that it will not stop this practice. This should concern every Namibian and is a crucial litmus test for CRAN; to show that it will take appropriate action to protect the public against the rise of the (now apparently rogue) surveillance state. It must not be forgotten that MTC is still Government-owned and controlled.

Another very relevant article by Frederico Links was published on 26 September 2022 in Issue One of the Southern Africa Digital Rights publication[38] and distributed by the Association of Progressive Communication. The article follows:

Namibia has become the latest African country to introduce mandatory SIM card registration and data retention regulations that will have a far-reaching impact on online privacy and data protection in the country. On 28 April 2022, barely days before World Press Freedom Day 2022 was marked under the theme "Journalism Under Digital Siege", conditions to be imposed on internet and telecommunications service providers were gazetted.

The newly gazetted regulatory conditions [1] followed from the gazetting of regulations under Part 6 [2] of the Communications Act of 2009 on 15 March 2021.

Part 6 of Namibia's Communications Act [3] provides the enabling framework for wide-ranging telecommunications surveillance by the state, but has never been officially operationalised since the law was passed almost 13 years ago, because regulations for implementation had not been finalised in all that time.

[37] As per MTC's website: www.mtc.com.na

[38] an online publication produced under "The African Declaration on Internet Rights and Freedoms: Fostering a human rights-centred approach to privacy, data protection and access to the internet in Southern Africa" project – obtainable at https://www.apc.org/en/news/new-surveillance-regulations-lurk-threateningly-namibia

The Part 6 regulations and conditions come at a time when Namibia is still busy formulating and drafting a data protection bill, a process that has also been ongoing for more than a decade.

However, while the Part 6 regulations and conditions have been gazetted, they have not been implemented as the directives, issued by the Minister of Information and Communication Technology (MICT) and the Communications Regulatory Authority of Namibia (CRAN), that set the operationalising date had not been issued yet by end May 2022.

The regulatory conditions and their potential threat to data and online privacy first came to light in October 2021, following reports of discussions [4] of the then draft conditions between the Communications Regulatory Authority of Namibia (CRAN) and telecommunications and internet service providers.

The regulations and conditions have come as Namibians appear to be highly suspicious of state communications surveillance practices.

The eighth round of the Afrobarometer survey, [5] from 2019, found that almost exactly 60% of respondents "agree with" or "very strongly agree with" the statement that people "should have the right to communicate in private without a government agency reading or listening to what they are saying".

The threats

The danger that the Part 6 regulations and conditions pose to online and data privacy was articulated by the executive director of the Ministry of Information and Communication Technology (MICT), Mbeuta Ua-Ndjarakana in an official communique [6] issued on 26 October 2021, in which he stated: "The benefits of SIM card registration is that it eradicates anonymity of communications, which aids in legal surveillance and interception."

The eradication of anonymity of communications is to be achieved through two ways that are extensively prescribed in the Part 6 regulations and conditions – through mandatory SIM card registration and data retention by telecommunications and internet service providers.

When selling and registering a SIM card or registering a customer for an internet connection, telecommunications service providers would be required to collect all sorts of identifying information or data from the customer.

The customer information to be collected is: the full name of the customer, the residential address of the customer; and the Namibian identity or passport or driving licence number of the customer.

In terms of data retention, telecommunication and internet service providers would also be required to store all telecommunications and internet traffic of all users for a period of five years.

The regulations and conditions mean that mobile phone and internet users in Namibia will all be instantly and permanently identifiable and trackable – the definition of continuous bulk or mass surveillance.

This sort of surveillance environment will probably have the effect of stifling critical media reporting, [7] as it enables the easy identification of journalistic sources and whistleblowers, as well as undermining lawyer-client or doctor-patient confidentiality, to point out just some of the obvious threats to sectors where privacy, anonymity and confidentiality are highly prized.

A legal response

For Namibian public interest law firm, the Legal Assistance Centre (LAC), there's one important question swirling around the Part 6 regulations and conditions, and that is "whether Namibia's requirements for telecommunications data collection and retention might be unconstitutional"?

In a policy brief [8] published around the time the conditions were being discussed and finalised, the LAC answered this question by stating "the scheme needs to comply with basic data protection principles – including measures pertaining to the security of the data and protections for confidentiality and the prevention of unauthorised access, as well as provision for the erasure or destruction of data after the requisite time period for its retention has expired".

The legal assessment concludes that "it seems likely that Namibia's telecommunications data retention scheme might be found to be an unconstitutional

infringement of the right to privacy overall, given the intrusion into the privacy of large segments of the population in a manner that has a questionable ability to serve the intended objectives".

The LAC assessment of the emerging Namibian surveillance environment echoes sentiments and concerns expressed by former UN special rapporteur on freedom of expression, David Kaye, in a report submitted to the UN Human Rights Council [9] in May 2015.

Kaye states of broad data retention regulations, such as those now on the verge of being rolled out in Namibia, that they "limit an individual's ability to remain anonymous. A State's ability to require internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."

He adds that a "State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information".

The special rapporteur's report concludes, among others, that "Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity".

The report goes on to state that because "of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective".

It is these principles that civil society organisations, such as the LAC and the Institute for Public Policy Research (IPPR), an independent Namibian think-tank which has for years been sounding the warnings on the looming threats of increased state surveillance powers through law and regulation, have been citing to advocate for transparency and accountability around state surveillance measures and mechanisms to minimise the avenues for surveillance abuse and overreach.

As the Namibian state moves to implement the Part 6 regulations and conditions, these CSOs and others are looking to increase their advocacy engagements around the emerging state surveillance environment.

A final article by IPPR hereunder deals with the danger of Government controlling the means of communication, directly or indirectly. The article is not focused on Part 6 of the Act *per se*, but addresses, in general, the dangerous consequences of Government having access to data, and the means to disrupt services whereby citizens communicate. This is an important aspect of Government controlling communications, as we are witnessing an increase in the number of oppressive Governments in the world completely shutting down digital communications during for instance civil protests. Such actions severely undermine citizens' ability to keep governments accountable, by terminating the right to freedom of expression in the blink of an eye. The article, published in The Namibian on 29 October 2022, follows:

Sabotage Aimed at Disruption

IN RECENT YEARS an increasingly common tactic used by states and malicious non-state actors to disrupt the online activities of civil society has been to shut down or restrict access to internet-based communication channels.

An example of how this was used in the Namibian context played out earlier this year [2022]*, as the Windhoek-based Institute for Public Policy Research (IPPR) was preparing to host what the institute's executive director, Graham Hopwood, described as "an important sideline meeting on corruption and human rights that we were organising at the United Nations Human Rights Council (UNHRC) in Geneva".*

The event was a virtual panel discussion, co-hosted by the IPPR, the Food First Information and Action Network (FIAN International), and the International Commission of Jurists (ICJ), on 31 March during the 49th session of the UNHRC.

An IPPR email address was used to register participants for the online event, titled 'Human Rights Violations, Transnational Corporations, and a Scandal in the Fishing Industry'.

However, the event was preceded by what IPPR's Hopwood labelled a "curious 24-hour period of apparent sabotage aimed at disrupting preparations for our sideline event at the UNHRC".

Describing what happened, Hopwood says: "Telecom Namibia [Government owned] *could not provide access to our email addresses for 24 hours before an important sideline meeting on corruption and human rights that we were organising at the UN HRC in Geneva.*

"An IPPR email address was being used as the key contact point for the meeting and had been advertised as the means of registering to attend.

"Despite discussions with several Telecom technicians and officials we were not given an adequate explanation as to why our emails were not working. We were told our emails were being 'quarantined somewhere'.

"The email service returned just an hour before the meeting was due to start and severely disrupted the registration process and limited the international audience that wanted to attend the online panel discussion."

The IPPR director says Telecom Namibia made "various other odd excuses, but nothing that made sense. In the end one technician said they thought there had been interference, but from outside Namibia".

To date Telecom Namibia has not provided a clear explanation about what happened.

DENIAL OF SERVICE

Such targeted denial of service attacks as experienced by the IPPR earlier this year are enabled and perpetrated through the use of ever-more sophisticated communication surveillance technologies and hacking services available to states, and increasingly non-state entities, on international surveillance tech markets.

Cybersecurity experts spoken to by the IPPR in the wake of the denial of email service attack, while not discounting Namibian state involvement, voiced the suspicion that the Icelandic fishing company implicated in the Namibian Fishrot fisheries corruption scandal, and whose conduct and activities were primarily the focus of the virtual panel discussion, could have been behind the attack.

However, cybersecurity sources spoken to for this article have also indicated that Namibian law-enforcement and security agencies have apparently been engaging with suppliers of sophisticated digital surveillance tools and services as recently as 2021.

One of the international suppliers mentioned (due to this being unconfirmed, the name is not mentioned here) sells what is said to be a modification of the Israeli NSO Group's notorious Pegasus surveillance tool.

NSO Group's Pegasus spyware, and similar surveillance tech, such as that which Namibian authorities were said to be looking at acquiring recently, has been documented to be widely used to spy on civil society activists and journalists in different parts of the world, including some African countries.

These spyware systems enable total access to infected mobile devices.

According to organisations such as the Uganda-based Collaboration on International ICT Policy in East and Southern Africa (Cipesa), in its annual 'State of Internet Freedom in Africa' report, human rights defenders and anti-corruption advocates have been primary targets of African governments' often unlawful and unjustified use of such systems and surveillance practices.

FEAR AT THE MARGINS

Coupled with the use of such invasive spyware technologies and services is the increasing enactment across the continent over recent years of questionable laws and regulations that enable such practices.

Such laws and regulations – especially around cybersecurity and cybercrime – have been documented to be used for oppressive purposes, contributing to a deterioration in African civic spaces both offline and online, according to international civil society monitor Civicus.

These sorts of laws, regulations and practices have also been deployed to spy on and enable repression of historically marginalised groups and communities, including gay rights advocates or lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI+) activists.

The fears from within this community in Namibia surfaced in September this year [2022].

This author was approached by an organisation working at the intersection of LGBTQI+ rights and HIV-AIDS healthcare to provide an impact assessment of surveillance-enabling mandatory SIM card registration and data retention regulations.

Of special concern was the privacy and anonymity of LGBTQI+ individuals accessing HIV-AIDS related healthcare services.

These fears are well-grounded, as the former executive director of the Ministry of Information and Communications Technology officially plainly stated in October 2021 that the aim of the introduction of mandatory SIM-card registration was that it "eradicates anonymity of communications, which aids in legal surveillance and interception".

The concerns of the LGBTQI+ community should be seen in the light of a March 2022 report by international human rights organisation Article 19 detailing how some African governments have used surveillance-enabling laws and spy technologies especially to harass, intimidate and imprison LGBTQI+ individuals and rights activists over recent years under the pretext of policing societal morality.

As discussed before, it is entirely possible that nefarious actors in Government could have been involved, right up to the level of National Intelligence. This should concern every Namibian.

3.3.3. Privacy International

In conclusion of this section, we provide a 2015 report compiled by Privacy International, following their 24th Stakeholder Session on Namibia. This report also addresses concerns over several other laws in Namibia that raise concern over the breach of the right to privacy. It specifically addresses the concern over the powers of National Intelligence. The report follows - references and other footnotes are not included.[39]

Introduction

1. *This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.*

[39] The full referenced report by Privacy International can be obtained at https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf

2. *PI wishes to bring concerns about the protection and promotion of the right to privacy in Namibia before the Human Rights Council for consideration in Namibia's upcoming review.*

The right to privacy

3. *Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.*
4. *Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.*

Follow up to the previous UPR

5. *There was no mention of the right to privacy and data protection in the National Report submitted by Namibia nor in the stakeholders' submissions. However, during the official review, despite no recommendations included on the issue in the report of the Working Group, Canada expressed its concern for the potential limitations of the right to privacy by the Communications Act.*

Domestic laws related to privacy

6. *The Constitution of the Republic of Namibia guarantees the protection and respect of the rights to privacy under Article 13, which states that:*
   (1) No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.
   (2) Searches of the person or the homes of individuals shall only be justified:
      (a) where these are authorised by a competent judicial officer;
      (b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest,

and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.

International obligations

7. *Namibia has ratified the International Covenant on Civil and Political Rights ('ICCPR'), which under Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".*
8. *The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."*
9. *In accordance with Article 144 of the Namibian Constitution "unless otherwise provided by this Constitution or Act of Parliament, the general rules of public international law and international agreements binding upon Namibia under this Constitution shall form part of the law of Namibia."*

Areas of concern

I. Communications surveillance

10. *Whilst the technological surveillance capabilities of Namibia are unknown, the various legislation it has adopted over the last few years have raised concerns about the increasing powers to conduct surveillance, the omission to establish and enforce prior judicial authorisation, and the broader powers of intelligence agencies without oversight.*
11. *In March 2014, a member of the South West Africa People's Organisation (SWAPO), the governing party in Namibia since its independence in 1990, Kazenambo Kazenambo accused the government of abusing its power to conduct lawful interception.*

State surveillance: powers to intercept and access communications data

12. *During the drafting phase, the 2009 Communications bill was condemned by civil society but also the media and opposition political parties as an infringement on*

privacy contrary to Article 13 of the Constitution as well as freedom of expression and the right to information as enshrined in Chapter 3 of the Constitution of Namibia.

13. *Nevertheless on the 16 July 2009 the Communications Bill was adopted by the National Assembly.*
14. *There are various provisions which are of particular concern, these include the following.*
15. *Part 6 of the 2009 Communications Act regulates the "Interception of Telecommunications'. The 2009 Communications Act directly threatens the respect and protection of privacy rights, as it allows broad powers to the government to monitor telephone calls, e-mail, and internet usage without a warrant.*
16. *The vague language around references to laws that may require a warrant for any person or institution to intercept or monitor electronic communications or to perform similar activities are baseless, given that even though the law was passed in 2009, the relevant regulations to implement Part 6 have yet to be adopted. In effect this means, that there is not judicial authorisation required to conduct surveillance nor any oversight of any authorisation process. Therefore there is not limitation on who is subject to the surveillance, and the duration, scope, purpose and method of interception operations.*
17. *Also the wording of the Act, "staff members", seems to place no restrictions as to who may conduct the interception, or impose that it be conducted by someone with a certain level of seniority.*
18. *Article 70 (9) provides broad powers as to the methods that maybe used to conduct surveillance as it reads that, "Any staff member employed in an interception centre may do anything necessary in order to perform the interception or monitoring concerned (as well as any decoding or decryption necessary to make the information in question intelligible)".*
19. *The only directives provided for the interception of communications are those the Director-General may chose to issue as outlined by Article 70 (11) and which include how the information obtained must be handled, who may handle it, who can perform any actions relating to the interception and other technical and procedural matter to ensure that the information by means of interception is only used for the intended purpose. The General Directorate in the 2009 Act refers to*

the Director-General of the Namibia Central Intelligence Service in accordance with the 1997 Act.

20. *Article 71 of the 2009 Communications Act outlines the duties of licensee and other providers of telecommunications services including the duty to:*
    - *Provide a telecommunication service in such a manner that is capable of being intercepted (1).*
    - *Store such information relating to the originator, destination, contents of, and other information relating to the telecommunications concerned as may be prescribed (2).*
    - *Acquire at its own cost whether by purchasing or leasing the facilities and capabilities necessary to comply with the duties referred to in subsection (1) and (2) (3).*
21. *Article 73 of the same Act, also requires telecommunications service providers to ensure that information prescribed is obtained for all customers, and that the information is "sufficient to determine which telephone number or other identification has been issued to a specific customer in order to make it possible to intercept the telecommunications of that customer."*
22. *The obligation the Act places on telecommunications service providers to provide access to their systems and the data of their users without a court order violates the right to privacy. Furthermore, compelling service providers to build into their systems surveillance and monitoring capabilities threatens the integrity, security and privacy of communication systems.*
23. *The new regulatory body that is created by the Act, the Communications Regulatory Authority of Namibia (CRAN), is subject to the Stated-owned Enterprise Governance Act of 2006. However, the CRAN is not an enterprise but a regulatory institution. It should not fall under the authority of the Minister but it should be truly independent and report to the Parliament.*
24. *These provisions provide the framework to allow authorities to conduct mass surveillance of its citizens. To comply with international human rights laws and standards, laws regulations communication surveillance must respect the principles of legality, proportionality and necessity, including by defining whose communications are to be intercepted, which types of communication can be intercepted, and for what purpose.*

Intelligence agencies: judicial authorisation and oversight

25. *The Namibian Central Intelligence Service (NCIS) is responsible for internal and external security. The function, management and operations of the NCIS is regulated by Namibian Central Intelligence Service (NCIS)Act, 1997 (Act No 19, 1997). The Namibia Central Intelligence Service Act, which sets out clear safeguards to prevent abuse and upholds Article 13 of Constitution of the Republic of Namibia which guarantees the protection and respect of the rights to privacy.*
26. *The 1997 Acts provides a strict legal framework for the NCIS to conduct interceptions which under Article 25 requires it to obtain a High Court warrant, which rests on the conditions of evidence of a serious threat to state security, and it prevents it from conducting phishing expedition, as the request must be specific to a type of communication and target.*
27. *However, the 2009 Communications Act, which, includes little or no safeguards to protect the right to privacy and the confidentiality of users' data and information, expanded the powers of the intelligence agency to conduct surveillance without judicial authorisation. The only provision which seems to include some protection is Article 121 (3), which says that the power awarded to the Authority to monitory compliance with the provisions of this Act, do not allow to use it "to obtain the contents of any message or information transmitted over that network, or to obtain any information relating to the behaviour of any customer or user of any telecommunications service".*
28. *Furthermore under Article 70(7) of the 2009 Communications Act, "The Director-General must designate a staff member in the Namibia Central Intelligence Service as the head of every interception centre".*
29. *Section 1 of 1997 Act imposes for the NCIS to remain neutral from the Executive, to prevent political abuse, and sets down a strict oversight mechanism which includes reporting to the Parliamentary Committee on Security under Article 32, however it was reported by current members of Parliament that this Committee had ceased to exist.*
30. *In August 2013, the NCIS was reported to have been in touch with the US National Security Agency (NSA) regarding plans for them to implement a system which would allow it to monitor all emails and internet communications.*

Electronic Transactions and Cyber Crime Bill

31. *The Ministry of Information and Communication of Namibia has been working with the International Telecommunications Union (ITU) to draft an Electronic Transactions and Cyber Crime Bill (ETC). Even though, the bill has not yet been open for public consultation, the Minister of Information and Communication Technology announced in a budget speech he delivered on 22 April 2015 that the ETC was now with the legal drafters to be finalised.*
32. *The ETC bill, if adopted in its current form, would allow the Namibian government to conduct search and seizure operations of databases and computers, the interception of communications, as well as remote monitoring for a period of up to three months. It will also force telecommunications service providers, or any other entity that may have information relating to a matter of interest to government, to co-operate and provide all relevant data.*
33. *Privacy International is concerned that the ETC bill may represent an extension of the surveillance powers contained in the Communications Act.*

Anti-terrorism Act 2012

34. *In 2012, the Combating and Prevention of Terrorist Activities Act was adopted in Namibia.*
35. *The government released the draft bill on 5 December, and was passed within 9 days by the Parliament. The opposition as well as some civil society organisations such as the Institute for Public Policy Research (IPPR) expressed concern and criticised the fact the Bill was rushed through Parliament, leaving limited time to members of Parliament to consider the 39 page document. The government justified the rush saying that it was a matter of urgency that Namibia adopt such a law amid global growing terror threats.*
36. *The definition provided under Section 1 (1) of the Act defines "terrorist activities": as "any act committed by a person with the intention of instilling terror and which is a violation of the criminal laws of Namibia and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, or group of persons or causes or may cause damage to public or private property, natural resources, the environment or cultural heritage."*
37. *The broad scope of the Act raises human rights concerns and whilst recognising, a State's legitimate security concerns and the need to protect their citizens, it is*

essential that it does not do so as the expense of the individual's human rights, including the right to privacy, freedom of expression and association. Privacy International is concerned that such a vague and broad definition of the "terrorist activities" may be (ab)used to prosecute and convict individuals for the legitimate exercise of their human rights and that such vagueness makes it difficult/impossible to identify which conducts would be criminalise, thereby violating the principle of legality under international human rights law.

38. *Any anti-terrorism policy must align itself with Namibia's national and international human rights obligations to respect and protect the right to privacy of its citizens.*

II. *Lack of comprehensive data protection law*

39. *Namibia does not have yet a comprehensive data protection law. According to various reports, and statements made by the ITU, a data protection bill is or has been drafted.*
40. *It appears that the current draft of the bill would include the establishment of Data Protection Authority (DPA) under Section 3 to 12, and include ten principles of data protection including accuracy (Sec. 13) legitimacy (Sec. 15), purpose (Sec. 15), necessity and proportionality (Sec. 14), fairness (Sec. 14), security and confidentiality (Sec. 26), transparency, stringent protection for sensitive personal data and personal data used for marketing. A section has also been included which would require that any Surveillance (via Audio, Video, and data) of identifiable people be strictly limited by law and that an authorisation from the DPA would be required prior to using technical means for monitoring people.*
41. *The current lack of a comprehensive data protection law is of particular concern in view of the following:*
    - *In 2005, Namibia introduced a new biometric identity card system for all Namibian citizens or permanent residence permit holders who are 16 years old or older.*
    - *In 2013, leading medical schemes announced they would start using fingerprint technology to counter fraud. This was particularly concerning as the technology was developed by two South African companies. This aspect raises concerns as to the ownership of personal (sensitive) data, and the responsibility and accountability of the government and the company to protect the data from abuse,*

theft, and loss. Given that Namibia does not have a data protection law, it is essential that the government takes the steps necessary to ensure the protection of its citizens' personal data when engaging with third parties.

- *In the 2014 elections, Namibia deployed biometric voter verification machines. Prior to the elections, voters were required to submit themselves to 10-finger biometrics scans. The devices were intended to match each voter to their identity cards. Namibia unveils the anti-terror bill to plug national security loopholes.*
- *In 2014, it was reported that Namibia's banking sector was considering the deployment of a biometric system.*

Recommendations

42. We recommend that the Government of Namibia:

- *Recognise and take steps towards compliance with international human rights law and standards by ensuring the application of the following principles to communication surveillance, namely: legality, legitimacy, necessity, adequacy, proportionality and respecting process of authorisation from a competent judicial authority; due process, user notification, transparency, public oversight and respect for the integrity of communications and systems, ensuring safeguards against illegitimate access, and right to effective remedy.*
- *Investigate reported unlawful communications surveillance activities by Namibian security agencies, and take necessary measures to ensure access to redress in case of violations.*
- *Adopt a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority.*
- *Investigate and take necessary measures to address security breaches of personal data which directly threaten the right to privacy of citizens, ensure that those responsible are sanctioned and in cases of recognised violations, victims have access to redress.*

4. PART TWO – BIG BROTHER IS WATCHING: WILL NAMIBIA BE A SURVEILLANCE STATE BY 2035?

4.1. Introduction

During 2018 *The Namibian* ran a series of rather ominous articles reporting on the rise of the Namibian surveillance state (Links, 2018). The newspaper reported that Namibia was stockpiling sophisticated surveillance and interception tools under the guise of promoting state security. These activities are largely conducted under the radar and, critically, without a comprehensive legal framework to protect and support the right to privacy enjoyed by ordinary citizens. The concern, shared by many, is that increased state surveillance will undermine state security, as opposed to the argument advanced by the Namibian Central Intelligence Service (NCIS) that exposing these activities will undermine state security.

Concerns about increased state surveillance is not limited to Namibia. During 2016, the United Nations issued recommendations for Namibia (including Sweden, New Zealand, Rwanda and South Africa) to strengthen surveillance and privacy protection. The committee was particularly concerned that Namibia was conducting interception and surveillance operations without a proper legal basis to do so. Privacy International (a privacy rights charity based in London) also issued a stakeholder report to the UN Human Rights Council (HRC) in respect of Namibia's upcoming review. It argued that privacy is a fundamental human right (enshrined in Article 13 of the Namibian Constitution) and it was concerned that Namibia was not doing enough to protect privacy. Privacy International also raised concerns about increased state surveillance and interception of communications (without an adequate legal framework to regulate these activities). It called on Namibia to take steps to comply with international human rights law and to adopt a comprehensive data protection law to safeguard privacy rights.

Namibia is hardly alone when it comes to concerns about increasing levels of state surveillance and erosion of fundamental human rights and freedoms (including privacy and, increasingly, data protection). There is a global argument that, under the guise of neoliberal modernity, we are giving states a degree of control over our private lives which exceeds the level and complexity envisioned by George Orwell in his seminal dystopian futures novel, 1984 (Giroux, 2015).

Giroux argues that, especially in the United States, market forces and loss of public memory and political identity collude to steer us towards an almost inevitable totalitarian future. The irony is that most of us embark on this journey willingly. In an age of pervasive social media, we appear quite happy to trade our personal information and right to privacy for the illusion of greater security, or online acceptance, or simply for something as mundane as daily convenience. Increasingly, state actors are monitoring online chats and exerting influence over private online forms.

For example, on 9 March 2019, the BBC reported that Singapore passed its "Protection from Online Falsehoods and Manipulations Bill" (Wong, 2019). The Singapore government emphasised that the Bill aims to protect the public from online trolls and false information. Privacy rights groups are understandably concerned that the Bill will affect freedom of speech, specifically, because it also aims to monitor online (encrypted) content between private users on applications such as Whatsapp. It prompted Phil Robertson (the deputy director of Human Rights Watch Asia) to say that "this is really moving towards a Big Brother style of control and censorship". About two months later, on 14 May 2019, the BBC reported that Whatsapp was the target of a sophisticated surveillance attack by (presumably) a private company working together with state actors (Lee, 2019). There is also pushback in some sectors against big brother surveillance technology. For example, on 15 March 2019 CNN reported that San Francisco became the first US city to ban facial recognition software in the City. It would still apply to San Francisco International airport however, as this is run by a federal agency (Metz, 2019). The Washington Post reports that the increasing trade tensions surrounding the United States and China as the opening salvo of a technology trade war to determine who controls the future of sensitive technology (Lynch, 2019).

We most probably suffer from cognitive dissonance and collective amnesia when it comes to the conflict between national security interests and the right to individual privacy. It must be said that not all surveillance is bad, and individual rights are not absolute. However, one does get the sense that digital innovation and transformation coupled with state intervention is moving us all ever closer to a potential surveillance future. In such an environment, many nations are struggling to find the right balance between protecting legitimate national security interests and upholding individual or collective rights and freedoms. It is debatable at what point in time the rise of the modern surveillance state started, or when the (real or perceived) assault on privacy rights commenced.

The September 11, 2001 attack on the World Trade Centre ushered in a new era of mass surveillance. Sweeping and divisive statements such as *'the war on terror'* and *'clash of civilizations'* and *'axis of evil'* entered the public discourse, and what followed was a period of prolonged asymmetric warfare on a nefarious and largely invisible enemy all over the Middle East and parts of Europe and North Africa . In Europe and the United States of America, fear of terrorist attacks led us relinquish increasingly our personal rights, freedoms, and liberties which were so visibly cherished only a decade ago. In large parts of the Middle East and North Africa (Iraq, Syria, Algeria, Libya and others) ordinary (and often innocent) people bore the brunt of proxy wars played out by global superpowers and local militias intent on preserving their own factional power base.

During the previous two decades, our world morphed into an intricate spider's web of cultural, religious, economic, and political alliances played out over an asymmetric, global battlefield. In such a complex and fluid environment, it was no longer clear who the good guys or the bad guys were (with a few notable exceptions). In 2035, we may look back at 2001 as the dawn of a new era, where big data, machine learning and artificial intelligence converged with a heightened fear of terrorist attacks to facilitate the rise of a Big Brother surveillance state.

4.2. Methodology

Part Two focuses on Namibia's surveillance future in 2035. Specifically,, given Namibia's transactional and contextual environment, the key question is whether Namibia will be a surveillance state in 2035? To answer this question, we will broadly adopt a futures methodology approach where we will first scope the key issues by providing some context and background to local and global surveillance issues, then scan the horizon in Namibia across a contextual environment, followed by forecasting a baseline and alternative futures for 2035 (essentially a scenario exercise), and finally synthesize the results into a preferred surveillance future for Namibia in 2035.

4.3. Scoping the Issues: The Global Context and the Rise of Big Brother

In 2035, big data analytics, artificial intelligence, machine learning, facial recognition software, surveillance cameras, biometric data, and other emerging technologies will have matured sufficiently and converged to create a perfect platform for mass digital population surveillance. Some might even argue that we are already operating in such

a contextual environment during 2023. Certainly, there are several countries that are increasingly focused on surveillance (both internal and external). Before we analyse Namibia, it is useful to examine some detail what two substantive global powers are currently doing (notably China and India).

4.4. China: A Totalitarian Blueprint for a Dystopian Future?

Most tourists to China will be familiar with the scale and grandeur of the Great Wall of China. But are they also aware of the so-called 'great firewall' of China which aims to regulate China's online world? Under the leadership of President Xi Jinping, China's state surveillance model increased rapidly, both in scope and content. There are precious few independent checks and balances on China's government, which is perhaps not entirely surprising given that China is effectively ruled by a one-party dictatorship and has no robust and independent Rule of Law. Reporters Without Borders publish an annual Press Freedom Index. During 2022, China ranked 175th out of 180 countries polled. In contrast, Namibia ranked 18th (the highest in Africa).

China is a world leader in technology innovation, which means it has the technological capacity (and certainly political will) to manipulate big data and resource asymmetric to control its population. In some instances, this means private companies are forced to cooperate with state institutions (or do so willingly) to provide data on everything from traffic offenses to credit scores, to monitoring social media content, to more serious crimes. This also means China is uniquely placed to monitor citizens' online behaviour, to purposefully control public opinion and prevent opposing views from crystallising.

Qiang, X, writing in the Journal of Democracy published by John Hopkins University Press in 2019, paints a rather dystopian picture of China's Big Brother ambitions which would even have impressed George Orwell. A timeline of recent events paints a rather ominous picture of total state control:

- In 2012, the Standing Committee of the National People's Congress of China made it mandatory for anyone wishing to use the internet or register social media accounts to provide their legally registered names to internet providers.

- In 2013, China passed legislation that imposes a three-year prison term on anyone who posts rumors which are deemed defamatory. It is not clear exactly

what would constitute defamatory behavior, but presumably, it would depend on whatever the state decides it is.

- China has also dramatically increased the use of surveillance cameras, and is now the world's fastest-growing country in this area. It is not difficult to see that an extensive network of surveillance cameras, coupled with AI, big data analytics, and sophisticated face recognition algorism can lead to a very centralized surveillance system. In any regime, not only dictatorial, such a system is open to almost infinite abuse.

- In 2015, China commenced its 'Sharp Eyes' project which implants massive video surveillance on the "Skynet" video-surveillance program initiated in 2005 to create an "omnipresent, fully networked, always working and fully controllable" control system based on facial recognition. The project reportedly came online during 2017.

- China is also expanding its DNA database and aims to double it from the current 54 million to almost 100 million by 2020. In September 2016, passport applicants in certain provinces (notably Xinjiang) needed to provide blood samples and other biometric data to obtain passports. There is widespread concern that this information will be used to suppress ethnic minorities, in particular the Uyghurs.

- In July 2017, China's State Council made it a public policy priority to become a world leader in AI. The next year, President Xi Jinping removed the two-term presidency limit from China's constitution which paved the way for him to consolidate power over a very long term.

- Finally, China is also working on a social credit system that would effectively assign a "good citizen" credit scope to each of its citizens. Depending on this score, citizens would be allowed to travel (or not), conduct business (or not), and interact with others (or not). The list goes on, and illustrates a rather concerning trend towards totalitarian state control in the daily business of ordinary citizens.

In summary, China currently has the world's largest population at approximately 1.42 billion (although arguably now surpassed by India) is effectively controlled and monitored by an even larger network of sophisticated surveillance cameras, artificial

intelligence, and smart algorithms, coupled with a vast DNA and biometric database. It is not difficult to imagine where this unchallenged and unchecked power could potentially lead, especially in the hands of a totalitarian state with a sub-optimal track record of protecting personal freedoms. But what about other countries and privately owned data dictatorships? Social media platforms such as Facebook and YouTube already have the data and power to control thought and behaviour through restricting freedom of expression as exponentially increased during 2019 – 2022 (Covid 19) in most, if not all, countries. Is massive state surveillance limited to totalitarian states, or does it also apply to democracies? A sobering reminder that large-scale surveillance also applies to democratic countries can be found in India, the world's largest democracy.

4.5. India: Increased Surveillance in the World's Largest Democracy

We are by now, with huge gratitude towards Edward Snowden, familiar with the large scale 'Prism' surveillance systems designed and implemented by America's National Security Agency (NSA). It was however somewhat surprising that India, the world's largest democracy, already commenced work in 2007 on a large-scale surveillance system that dwarfs that of the NSA. The system is called the Central Monitoring System (CMS) and it enables Indian authorities (including spy agencies) to monitor, in real time, over 900 million telephones (mobile and landline) and 160 million internet users (Litton, 2015). In essence, CMS allows authorities to intercept, monitor and access almost all electronic voice and data communications and to track GPS movements in real time. All of this can be done with virtually no judicial oversight, no parliamentary control, and even less public scrutiny which means that the right to privacy and freedom of speech could potentially come under severe threat. All of this is, again, made possible by technological advancements and the desire (some would say, obsession) by some states to control what its citizens, think, do and are generally up to.

In line with similar programmes worldwide, India's laws criminalise the dissemination of information deemed offensive or libel (which is never clearly defined and therefore leaves wide scope for expansive interpretation). There has been, rightly so, outrage by privacy activists in India about the scope and scale of CMS and it remains to be seen whether some of the more sweeping powers will be curtailed. Time constraints will not allow EPRA to go into great detail about CMS operating environment, suffice it to say that it illustrates that sweeping, mass surveillance is not limited to single-party states or

authoritarian (undemocratic) regimes. For example, the so-called '5 eyes' intelligence sharing programme is a joint cooperative effort between the United States of America, Canada, the United Kingdom, Australia and New Zealand. It is by no means the only global intelligence-sharing programme, only perhaps the most well-known. Some argue in favour of a global push to safeguard domestic security concerns which arise from secretive intelligence-sharing agreements without diminishing the impact and checks and balances provided by national laws (Taylor, 2018).

4.6. Namibia: What Will Determine its Surveillance Status in 2035?

Namibia is by no stretch of the imagination a totalitarian surveillance state. It has a thriving democracy, a relatively stable government, and spends a large percentage of its budget on education and healthcare. In terms of global impact, however, Namibia remains rather insignificant. Its citizens can therefore be forgiven for thinking that they are far removed from the world of mass surveillance employed elsewhere. In recent years, there have been ominous signs that Namibia is indeed moving towards a surveillance state regime that is not compatible with its status as a free, open, free, and democratic society. In 2018, Namibians were rudely awoken from their collective slumber when the Namibia Central Intelligence Service (NCIS) tried to prevent a local newspaper from publishing (seemingly innocuous) information related to corruption and misuse of public funds involving the NCIS. It is worthwhile exploring this case in some detail.

4.7. Case Study: The Patriot Newspaper

In April 2019, the Supreme Court of Namibia issued a judgment on a matter of critical importance to freedom of the press and national security provisions as enshrined in Namibian law. This case is likely to set a precedent for many years to come. It neatly illustrates the breadth and depth of a potential future Namibian surveillance state where state organs (such as the NCIS) are prepared to go to great lengths to keep information they deem secret out of the public domain, and preferably without judicial oversight.

4.7.1. Background

In April 2018, *The Patriot* newspaper intended to publish information related to the improper use of state funds by the NCIS who purchased certain farms and houses for or on behalf of former NCIS employees (the Association).

Prior to publication, *The Patriot* contacted the NCIS for their comments on the story. The Government Attorney's Office responded on behalf of the NCIS and the Government of the Republic of Namibia. It is worthwhile to quote its response in full:

". . . all information that you seek that relates to the properties and assets of the Namibia Central Intelligence Service falls within the scope of sensitive matters and/ or classified information. In terms of the provisions of the Protection of Information Act 84 of 1982 read with the provisions of the Namibia Central Intelligence Service Act 10 of 1997, possession, disclosure, and or publication of that information is prohibited and it constitutes a criminal offence. In the light of this position be advised that you are prohibited by law from possessing, disclosure and or publishing of that information. As a result of this position, your request to be provided with answers in respect of your questions and or to confirm or deny the veracity of the information you have is denied. With regard to your questions regarding the association, kindly be advised that the Namibia Central Intelligence Service …. cannot comment or answer questions or issues that relate to another entity. On this basis, our clients are not in a position to answer any question that relates to other entities".

In essence, the NCIS argued that *"the story which The Patriot wanted to publish related to the properties and or assets of the NCIS and that, by law, the unlawful possession, circulation and publication of any information concerning the properties, means and capabilities of the NCIS is prohibited and punishable by law"* and *"any disclosure of information which showed either the capability or a lack of resources on the part of the NCIS is unlawful as it undermines the effectiveness of the institution and with that posed a security vulnerability to the State of Namibia".*

The NCIS then approached the High Court of Namibia for an urgent interdict preventing *The Patriot* from publishing the story.

4.7.2. The High Court of Namibia

The matter was heard before Judge Geier who had to balance the right of NCIS to protect sensitive information from public disclosure with the right to freedom of speech and the press as enshrined in the Namibian constitution. The High Court refused to grant an interdict to NCIS on the basis that *The Patriot* acted reasonably in obtaining the information and the NCIS failed to make out a case that the information was

sufficiently sensitive not to be disclosed. The NCIS then took the matter on appeal to the Supreme Court of Namibia.

4.7.3. The Supreme Court of Namibia

On appeal, the NCIS relied on rather draconian provisions in the Protection of Information Act 84 of 1982 (PIA) read with the provisions of the Namibia Central Intelligence Service Act 10 of 1997 (NCISA) to argue that they have wide ranging powers (both statutory and constitutional) to protect sensitive information and to prevent such information from being published. It is illuminating to note that the NCIS, in essence, appointed itself as the final judge, jury and executioner when it comes to deciding what information should be regarded as secret. The NCIS did assume such conflicting roles to the point that they failed to disclose, even before the court, the exact nature of the information obtained by *The Patriot*. The newspaper, in turn, argued that the information it intended to publish was obtained legally, it was in the public interest because the media had an obligation to report on corrupt activities, and Article 21(1) of the Namibian Constitution protects freedom of speech and the press.

The Supreme Court of Namibia issued a judgment during April 2019 under Case Number 33 of 2018. The full citation is *Director-General of the Namibian Central Intelligence Service & another v Haufiku & 2 Others (SA33-2018) [2019] NASC (12 April 2019)*. The court held that the NCIS failed to convince it that the information was obtained unlawfully or that it will harm national security. In particular, the court was not impressed with the fact that the NCIS failed to present any substantive or credible evidence to support their allegation that the information was secret or would harm national security interests if it were to be disclosed. Rather importantly, the court rejected the notion that the executive can invoke secrecy and national security (simply by saying that something is secret) without judicial oversight because this would be inconsistent with the values of an open and democratic society based on the rule of law. The Supreme Court therefore dismissed the application by the NCIS (with costs) and clawed back some control when it comes to the ubiquitous and nefarious operations of state security.

4.7.4. Commentary

This court case provides an interesting snapshot of Namibia's approach to state security for mainly two reasons:

Firstly, it offers a rare glimpse into the mental model of the NCIS who demonstrated a 'Big Brother' mentality when it comes to secret information. The NCIS laboured under the misguided assumption that it, and it alone, gets to decide what constitutes secret information (applied as broadly as possible). Putting it another way; the NCIS felt that simply stating that something is secret makes it secret and thereby removes it from any other public or judicial oversight. It went to great lengths (and costs) to prevent *The Patriot* from publishing seemingly innocuous information which certainly, by any objective measure, did not constitute state secrets in the first place.

Secondly, the Namibian courts re-affirmed their judicial independence and held, that the executive cannot make unilateral decisions which are removed from judicial oversight (or public interest). This has important implications for Namibia's future by 2035 as a potential surveillance state, and it is encouraging that Namibia's courts in 2019 have gone to great lengths to protect freedoms enshrined in the Namibian Constitution. It can only be hoped that this trend will continue. However, given the latest trend in new laws, i.e., Part 6 of the Communications Act now enacted, and the Cybercrime Bill on its way, hope is diminishing.

4.8. Quo Vadis Namibia?

Where is Namibia heading in terms of a potential 2035 surveillance future? To answer this question, we first need to examine the contextual environment in which Namibia operates, and then extrapolate the trends and finally conduct a scenario exercise to forecast its possible, probable, and preferable 2035 surveillance future.

4.8.1. Scanning Namibia's Contextual Surveillance Environment

It is said that 'no man is an island' - and the same applies to countries. Namibia operates in a certain social, technological, economic, environmental, and political contextual landscape (commonly referred to as PESTLE, STEEP, or by various other acronyms).

Systems thinking teaches us that everything is connected (often in surprising ways) and each of these environments therefore has an impact on Namibia's 2035 surveillance future. It is, therefore, worthwhile exploring these areas in more detail to see how it impacts a potential state surveillance future.

Social Environment: Namibia is a relatively large country with a relatively small population. It is, in fact, one of the least densely populated countries in the world (226th worldwide). According to data obtained from World Population Review (2023), Namibia's population in 2023 is estimated at 2,604,172 people – see https://worldpopulationreview.com/countries

The projected 2,6 million population is to increase to approximately 3,520,740 by 2035. The largest ethnic group is Owambo (approximately 50% of the population), followed by Kavango (9.3%), Damara (7.5%), Herero (7.5%), white (6.4%), Nama (4.8%) Caprivian (3.7%), San (2.9%), and Basters (2.5%). Namibia has made significant progress across its social environment, but several challenges remain. For example, health, education, and very limited institutional capacity. The national unemployment rate is estimated to exceed 34% and some economists estimate the youth unemployment rate closer to 60% (in absence of a national census not executed during 2022 because of alleged lack of government funds). Unemployment is at least 40% (UN, 2018). According to data obtained from the Namibia Statistics Agency, Namibia had 1,756 schools in 2014 (of which 99 were privately owned). In 2015, there were 703,144 learners enrolled in school. Namibia currently has three tertiary higher-level education institutions, namely the University of Namibia (UNAM), Namibian University for Science and Technology (NUST) and International University of Management (IUM). Total enrollment at these institutions (during 2014) was 39,160. Namibia has relatively high levels of orphans and vulnerable children, who essentially rely on government grants to survive (approximately 170,000 grants were awarded during March 2015). By 2019, grant recipients increased to 211,000. In terms of healthcare, Namibia had 352 public healthcare facilities in 2015.

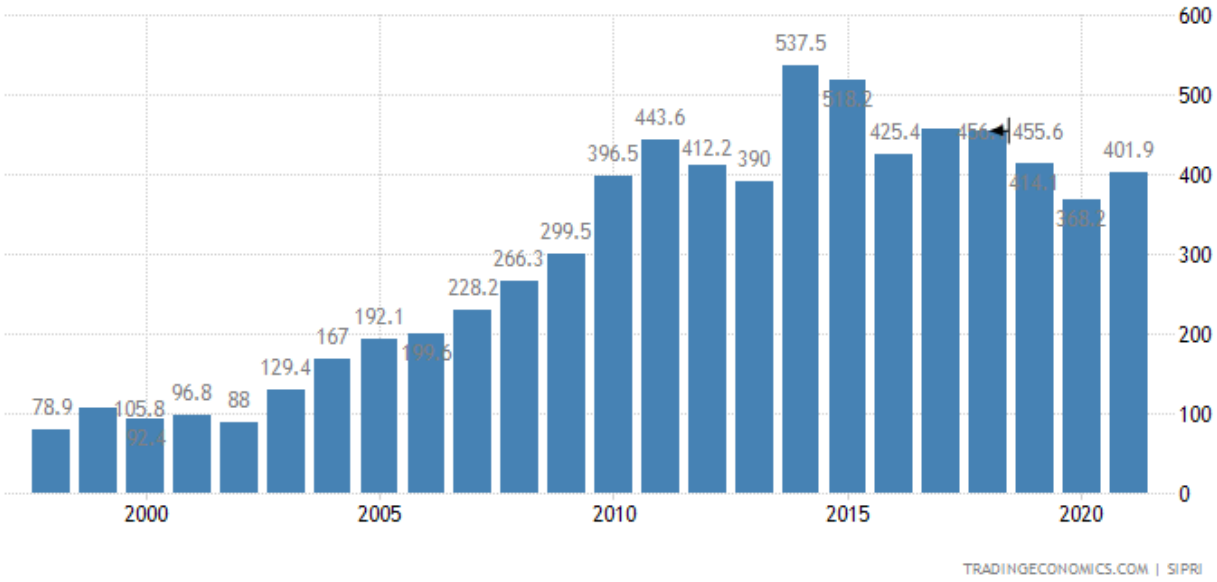
Generally, Namibia enjoys relatively high levels of peace, stability and security (despite the fact that it is, in effect, a one-party state because the ruling SWAPO party has governed with an absolute majority since Independence in 1990). Significant socio-economic challenges remain however, as reflected that Namibia occupies a relatively modest 139th position (out of 154) on the 2022 Human Development Index (HDI) published by the UNDP[40] . These challenges are likely to become more acute in 2035, which also potentially impact Namibia's security and surveillance environment.

[40] see https://hdr.undp.org/data-center/country-insights#/ranks

Technological Environment: It would be fair to say that Namibia is not a world leader in terms of home-grown technological development. However, smaller states do not have to develop their own technology to benefit from the 4th Industrial Revolution. They can purchase the technology from more developed nations. Each year the MIT Technology Review lists 10 breakthrough technologies that are bound to have a global impact. In 2018, these technologies included dueling neural networks and zero-proof protocols. In essence, a general adversarial network produces realistic-sounding speech and photographic images that can fool most humans. It means AI is evolving exponentially, and starting to make sense of the world independent from human input. The potential of course exists, in the wrong hands, that this technology can be used to manipulate public opinion. At the other side of the spectrum, scientists are working on a cryptographic protocol called zero proof which would, in theory at least, make online privacy a reality. In terms of surveillance, we have already alluded to the convergence of big data with AI, gene mapping and facial recognition. All these tools are, without doubt, available to state security institutions. The net effect is that technology for mass surveillance already exists and is likely to become more mature and effective in 2035. The key question however remains: how will states use and/or abuse this technology?

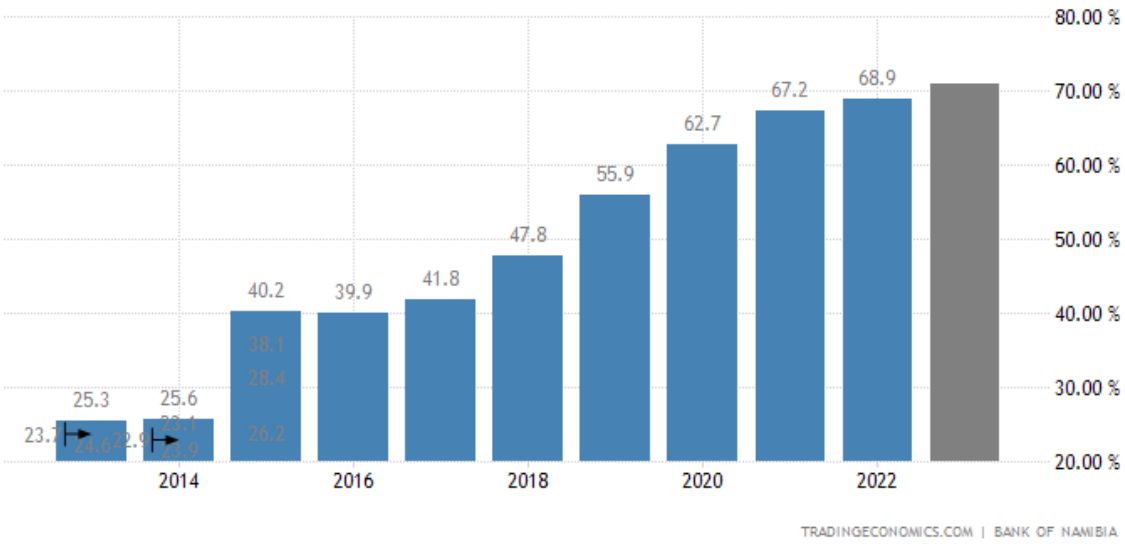
Economic Environment: Namibia's economy has been struggling for a while. According to data released by Cirrus Capital after the 2019 budget speech, Namibia's economy was projected to do marginally better during 2019, but would have experienced stresses. Total expenditure reduced somewhat from N$ 64.3 billion estimates to N$ 63.9 billion. Although the defence budget decreased in overall terms, it was still the fourth largest beneficiary of the budget (after education, finance and health and social services) and amongst the highest (per capita) in the world, as illustrated by the following graph:

Graph 1: Namibia: Military Spending



Rather worryingly, Namibia's debt to GDP ratio increased dramatically since 2014 as illustrated by the following graph:

Graph 2: Namibia Debt to GDP Ratio



The considered consensus is that Namibia's economy is likely to remain under pressure for some time to come. A struggling economy does not bode well for socio economic upliftment and (potentially at least) puts pressure on individual freedoms and rights as people who struggle to make a living tend to also become restless socially. More social unrest can in turn lead to greater surveillance and oppression as states desperately try to control their populations. In addition, Namibia's economy is bound to be influenced by global (macro) economic factors over which it has little or no control (for example,

the price of commodities, international trade wars, global slowdown in the economy, etc).

Institutional Environment: Two Namibian institutions are of particular importance when it comes to the protection of fundamental rights and freedoms. These are the courts (which are independent but generally very expensive) and the Office of the Ombudsman, given its constitutional powers. Unfortunately, the Office of the Ombudsman is notoriously underfunded and understaffed, and it recently took the official position that it cannot approach the courts on behalf of any complainant. This Office is therefore unlikely to provide any meaningful protection to the public in the event of a surveillance state, disregarding constitutional rights and freedoms. Experience has shown that approaching the High Court in constitutional applications can easily cost several million, not counting the risk of a cost order against the applicant. Very few Namibians have this luxury. Namibia's civil society organisations are relatively few, weak and underfunded, to say the least, with very limited funds they do receive, are coming from foreign donors. This creates fertile ground for abuse of unchallenged public power.

Political Environment: Namibia's political landscape has, since Independence on 21 March 1990, been dominated by a single party, SWAPO. In the first democratic elections of 1989 SWAPO obtained 57% of the votes. SWAPO's support increased to 80% in the 2014 elections, but decreased substantially to 65.5% in the 2019 National Elections, and further to 56.5% in the 2020 Regional Elections. Namibia has generally free and fair elections, but opposition parties have so far failed to gain significant representation in the National Assembly. Lack of influential opposition also means that SWAPO is effectively in total control of most policy and government decisions in Namibia. Considering this absolute majority, SWAPO has generally followed a constrained free market policy, which has of late become marred by increased regulation and government control over private sector. SWAPO recently introduced several policies aimed at 'redistribution of wealth' which, as EPRA has reported in previous reports on NEEEB and the Investment Bill, can only benefit a very small group, which are most likely already empowered, or politically well connected.

Legal Environment: Namibia is a constitutional democracy which means that its constitution reigns supreme. It adopted an enviable constitution in 1990, with progressive and liberal protection of fundamental human rights and freedoms (including

section 13, the right to privacy) enshrined in Chapter 3 of the Namibian Constitution. Other rights protected by Namibia's Constitution include the right to protection and liberty (section 7), the right not to be arbitrarily detained or arrested (section 11), the right to a fair trial (section 12), and fundamental freedoms such as freedom of speech and expression (section 21). These rights can be limited by general application (provided its fair and reasonable). However, these rights, interpreted together, means Namibia has a very strong culture of protecting individual rights and freedoms enshrined in its Constitution, at least at the level of the Judiciary. These rights can and do, however from time to time come under pressure and may very well be tested in future with the development of mass surveillance.

The Namibian Central Intelligence Service (NCIS) is the main body tasked with internal and external security in Namibia. The NCIS obtains its powers pursuant to the Namibian Central Intelligence Service Act 19 of 1997, as amended (the NCIS Act). The NCIS Act has safeguards to protect privacy as enshrined in Article 13 of the Namibian Constitution. However, there is concern that these rights are being eroded by the introduction of other laws, notably the Communications Act and the Combating and Prevention of Terrorist Activities Act 12 of 2012 (CPTA Act). The CPTA Act was rushed through Parliament in a matter of days (with very limited public input). It has a broad definition of what exactly constitutes terrorist activities and grants broad powers to intelligence agencies. There is concern that these powers could be abused. Namibia's Access to Information Bill has been many years in the making, and has been passed by parliament, but is yet to be operationalized, seemingly for lack of funds, the same reason the Whistle-blower Act has not been operationalised yet.

Based on a 2017 study of the Institute for Public Policy Research (IPPR), Namibia is experiencing a transparency deficit when it comes to access to information. The IPPR study found that approximately 80% of private institutions could not (or would not) respond to requests for information, 85% of public enterprises were unresponsive, and it recommended that Namibia adopts laws to guarantee access to information. Namibia is signatory to several conventions and protocols that deal with access to information. These include the United Nation's Universal Declaration of Human Rights (Article 19 states that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"), the 2000 SADC Protocol on Culture, Information and Sport (which requires states to strengthen

institutional frameworks for the implementation of information based policies), and the 2002 Declaration of Principles of Freedom of Expression of the African Union (which emphasises the need for states to develop policies to safeguard freedom of expression and access to information).

There are also other laws which may impact on Namibia's potential surveillance future. For example, the Namibia Communications Act 8 of 2009, as amended (Communications Act) came into force during 2015. The Communications Act aims to regulate telecoms providers. It provides for information to be provided to CRAN. Part 6, which came into operation 1 January 2023, is of particular importance. It provides for the establishment of interception centres to "combat crime and national security" (section 70). These interception centres are staffed by, amongst others, intelligence operators. Licensed telecoms operators must provide telecommunications services in such a way that it is capable of being intercepted (section 71). The Minister of Communications has wide discretion in terms of regulations passed under the Communications Act, and it is by no means clear whether there is sufficient oversight to temper any abuse under this Act. In addition, both the Protection of Information Act 84 of 1982 and the Namibia Central Intelligence Service Act 10 of 1997 give wide ranging and sometime draconian powers to the Namibian Intelligence Agency in respect of its operations. As discussed above, the mooted Cybercrime Bill poses an even bigger risk for abuse of public power, in breach of constitutional rights. Taken together, these laws potentially set a platform for mass surveillance.

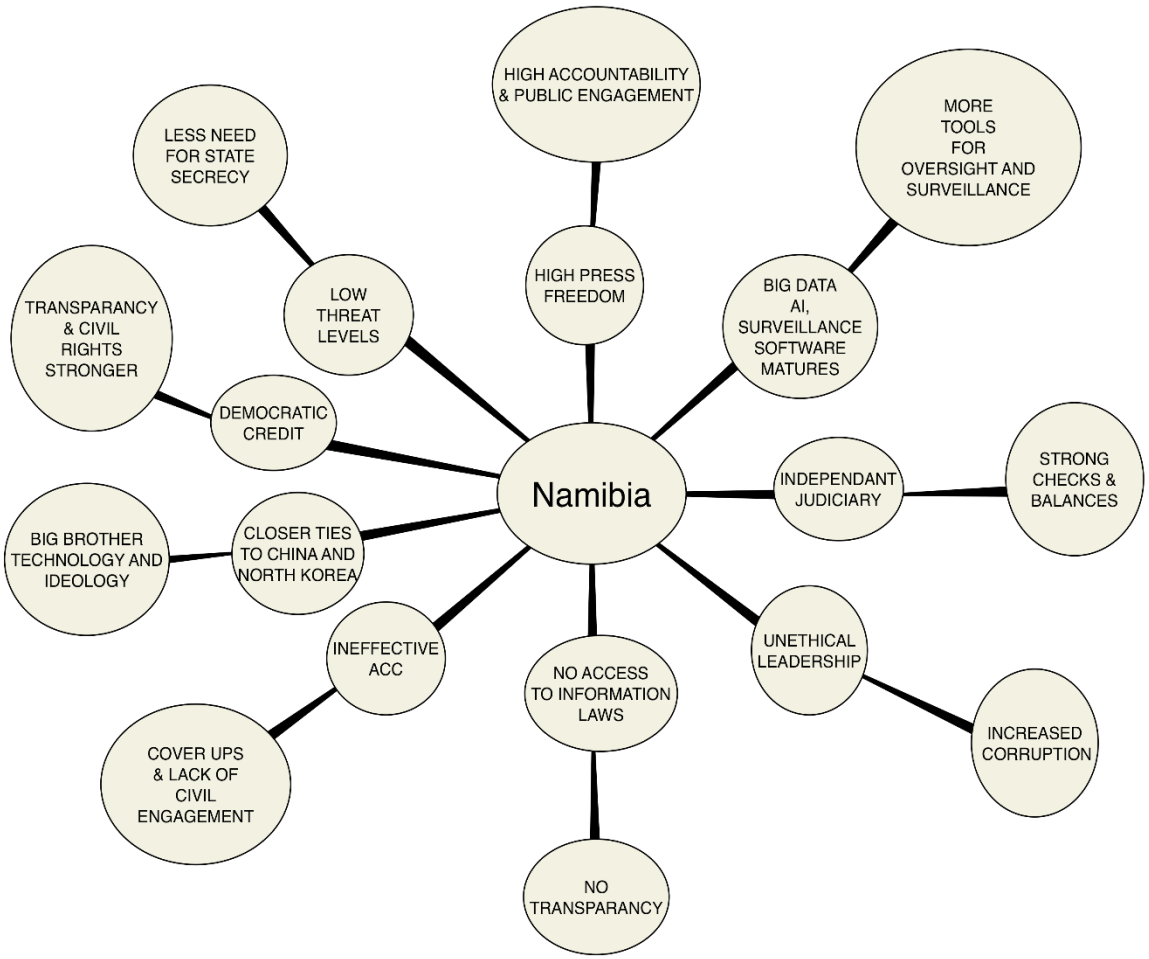
In summary, in the past Namibia had a fairly appropriate legislative framework to balance individual rights and freedoms against national security interests. However, this did however depend on the willingness of the Government of Namibia to protect and enforce those fundamental rights. Of late, and despite public utterances to enhance transparency and accountability, and to cease from invading privacy and curtail the right to freedom of expression, there are worrying signs that increasingly lip service is being paid thereto. Namibia's future as a potential surveillance state in 2035 depends, to a large degree, on how willing and able the government is to protect individual rights and freedoms. Recent laws, and mooted laws, indicate that government's willingness to do so is diminishing rather fast.

4.8.2. Forecasting Namibia's Surveillance Future: Trend Analyses

To forecast Namibia's potential surveillance future in 2035, it is first critical to establish where we are in 2023, and then to determine where we are heading in 2035. Big data, facial recognition, machine learning, and video surveillance are undoubtedly on the increase globally. For example, in November 2018, Investorideas.com released a security stocks bulletin in respect of the growing global video surveillance market (a market worth approximately USD 30 billion in 2017) and projected rapid growth of approximately USD 105 billion by 2026. Global investment in the AI market is notoriously difficult to predict, but the trend can very safely be assumed to be upwards. For example, Tractica (a market research firm) estimates revenue from AI software to increase from USD 9.51 billion in 2018 to USD 118.6 billion in 2025 (Statista, 2019). It is not difficult to see that there is rapid growth in the AI and surveillance market. The combination of big data, AI, facial recognition, deep learning, DNA / biometric data and surveillance technologies create a perfect digital platform for mass digital and real time surveillance. Surveillance technology exists, and is maturing. We must remember, however that technology does not spy on people, people spy on people. The key question(s), therefore, is: will this technology be used to control populations and stifle dissent or to combat crime and increase security? The jury is still out on these questions.

4.8.3. Futures Wheel

A futures wheel is essentially a mind map to determine first and second-order consequences. If we look at Namibia in the context of a surveillance state, then the following (non-exhaustive) first and second order consequences come to mind:



4.8.4. Mapping Namibia's Baseline and Alternative Surveillance Futures: Scenario Development

A scenario exercise is a useful tool to develop plausible and compelling stories about Namibia's potential 2035 surveillance future. It narrows the cone of uncertainty through which we view the world (Business Futures, 2016) and enables us to prepare baseline and alternative scenarios to fully understand how the environment (internal and external) could develop and impact Namibia's surveillance future.

Having scanned the contextual environment we can see that surveillance technology is on the rise globally. From this report, it is clear that many countries (including Namibia) are aggressively pursuing surveillance technology and techniques that potentially encroach on the right to privacy. In some instances, states are using surveillance technology to address legitimate security concerns. In other cases, states are using surveillance technology to control populations. There is pushback (both globally and in Namibia) at the rate of Big Brother surveillance, and it remains to be seen whether we can find a balanced middle ground between legitimate security concerns and the

protection of privacy. By conducting a scenario development exercise, we can develop three plausible surveillance future scenarios for Namibia in 2035 as follow.

Scenario 1 (Rising Big Brother): This is the most plausible baseline future (assuming most things stay the same and/or similar). In such a scenario, Namibia continues to pursue state surveillance, but its reach and impact are tempered by a lack of funds (to pursue mass surveillance), civic opposition to mass or arbitrary surveillance, and low strategic importance of pursuing a surveillance state (given Namibia's other socio-economic challenges). Dubious political players and politically connected 'tenderpreneurs' are fairly freely able to abuse the surveillance apparatus for personal gain, but not without fear of being caught. There is some measure of judicial oversight and active citizen engagement. Namibia becomes more open and transparent when it comes to some state surveillance, but still operates in the shadows on most state security matters. Newspapers report on overreach, and the courts generally enforce the right to privacy. As a relatively small player on the global scene, Namibia is stuck somewhere between a totalitarian surveillance state and a democratic nation that values individual freedoms, oversight, and transparency.

Scenario 2 (Aggressive Big Brother): In this dystopian scenario, Namibia actively pursues state surveillance to its fullest extent possible. Namibia moves closer (both economically and in terms of ideology) to China, Russia, and North Korea (with whom it has liberation era emotional attachment and connections). Mass surveillance is used to settle political scores and to suppress political dissent. The NCIS avoids judicial oversight at all costs. The Data Protection Act, Access to Information Act and Whistleblower Act creates an illusion of privacy and public protection, but mask what is going on behind the scenes. Economic decline leads to social unrest, which means citizens' behaviour is actively monitored, state security legislation is strengthened, and public dissent is not tolerated. Namibia becomes a proxy state to other totalitarian regimes and a testing ground for mass digital surveillance. Dubious political players and politically connected 'tenderpreneurs' can abuse the surveillance apparatus for personal gain; politically protected and without fear. The shadow of Big Brother looms ominously over the Namibian landscape. No legally bound citizen, not even the media, dares to expose corruption or politically captured institutions.

Scenario 3 (Friendly Big Brother): In this preferred (but unlikely) scenario, Namibia stays focused on protecting fundamental human rights and freedoms enshrined in its

constitution. No attempts are made at mass surveillance and Namibia becomes a world leader in terms of adopting open, transparent surveillance systems technology and laws. Judicial oversight, by an uncompromised judiciary, is at the heart of all surveillance. The Data Protection Act is effective and protects personal data, and the public against abuse of public power. Private citizens' rights (including the right to privacy) are valued and enforced, and citizens trust the NCIS and the government to protect them from legitimate security threats. Namibia purchases cutting-edge surveillance technology, but its use is always subject to protecting fundamental human rights (including the right to privacy). Judicial and intra-government oversight is encouraged and strengthened, and Namibia strikes the equilibrium between addressing legitimate security concerns and protecting personal rights and freedoms.

4.9. Conclusion

We live in an age of rapid technological advancement especially in the fields of AI, big data, biometrics, deep learning, video surveillance, facial recognition, and other surveillance technologies. We also live in an increasingly polarised world dominated, at least in part, by heightened fears of terrorist attacks and the rise of the Big Brother surveillance state. In such a complex, fast-paced and fluid environment, it is only natural that people seek protection. Some of us become nostalgic and hark back to 'the good old times' when things were simpler. Others realise that change is inevitable, but we can (and should) seek to influence the drivers of change to reach a preferred future.

In the battle of political ideas, we are confronted daily between those seeking a more insular and nationalist world, and those who embrace globalization and believe we are stronger and better together. Systems thinking teaches us that we are all interdependent and interconnected. This does not mean that there is no space for individual nations, or that there will not be a divergence of opinions, or that rights and freedoms should not be balanced with legitimate security concerns. It does however mean that isolating ourselves from the world will, ultimately, be a futile exercise. We are all in this together and we should all, collectively, try to solve the world's problems in a holistic and sensible manner.

We value and cherish our personal freedoms and liberties. We also appreciate that surveillance is sometimes necessary and can be used to protect us from those who seek to destroy. Truth often tends to be the first casualty in warfare. We will therefore

leave it to sensible and rational minds to research whether terrorism kills more people than those who die having an accident in the bath (spoiler alert: it does not) or whether our current heightened state of paranoia justifies abdicating our privacy and right of freedom of speech to governments globally (it should not). As with so many things in life, a time of crisis requires us to seek the equilibrium between legitimate security concerns and individual freedoms.

In a globalised world, we need to take a step back (to see the big picture), inhale deeply (to calm down), switch on our rational minds and empathic hearts, and then work together in a pragmatic, sensible and holistic manner to address the world's security problems. This is diametrically opposed to the current insular and isolationist approach which appears to take hold in certain corners of the world where we all retreat into our individual (or national) caves and blame others when the sky falls on our heads.

To forecast Namibia's 2035 surveillance future environment with absolute certainty, is not possible. The main reason for this is that humans are both the object of the forecast and the agents who can change the outcome of the forecast. We can, however state with some degree of certainty that a totalitarian surveillance future in 2035 is not an inevitable outcome of developments and trends taking place in 2023. It can and should be possible for Namibia to reach a preferred surveillance future, provided appropriate influence is exercised over the drivers for change. This means that Namibians will need to scan the horizon and remain informed of the global and local trends and forces shaping their future. It will require continuous, active, constructive, informed and critical engagement between all relevant stakeholders (especially civil society, the media, human rights organisations, government and the NCIS) across the political, security, policy and socio-economic spectrum to reach a preferred surveillance future outcome.

Our hope is that Namibia will find itself in its preferred surveillance future in 2035, where individual rights and freedoms are protected and appropriately balanced with the legitimate need for surveillance and state security. There are encouraging signs (for example the 2019 *The Patriot* case) that can suggest that this future is possible. However, we can never take any preferred future outcome for granted. There are always emerging and disruptive factors that could signal a descent into a totalitarian surveillance future. It is incumbent upon all of us to guard against negative drivers which erode fundamental human rights and freedoms, whilst being cognisant of the legitimate need for state security and surveillance.

As stated earlier, technology does not spy on people, people spy on people. Technology is therefore not the enemy or something to be feared. There is no need to enter a dystopian surveillance future. We can and should influence the drivers for change to reach a preferred surveillance future that recognises our common humanity and protects our fundamental human rights and freedoms in Namibia. Such a future is however unlikely to materialise if civil society does not recognise its crucial role in actively pursuing such change. Left to its own devices, Government is unlikely to limit its own surveillance capacities and opportunities to abuse public power and breach constitutional rights and freedoms.

References

Bishop, PC and Hines, A. (2012). Teaching about the future. London, Palgrave, Macmillan.

Cirrus Securities. (2019). *Namibia Budget review 2019/2020.* Retrieved at: http://data.cirrus.com.na/pdf/Budget%20Review%202019.pdf

Giroux, H. (2014). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies, 29*(2), 1-33.

Global video surveillance market to reach $105.99 billion by 2026 and how new technology will play key role; DirectView holdings, inc (OTC: DIRV), FLIR systems, honeywell and panasonic corporation. (2018, Nov 29). *NASDAQ OMX's News Release Distribution Channel*. Retrieved at: https://search-proquest-com.ez.sun.ac.za/docview/2139020070?rfr_id=info%3Axri%2Fsid%3Aprimo

Institute for Public Policy Research. (2017). *Access to Information in Namibia.* Retrieved at: https://ippr.org.na/wp-content/uploads/2017/12/AccessDenied_WEB01122017.pdf

Lee, D. (2019, May 14). *Whatsapp discovers 'targeted' surveillance attack.* BBC World. Retrieved at: https://www.bbc.com/news/technology-48262681

Links, F. (2018, March 15). *The rise of the Namibian surveillance state: Part 3.* The Namibian. Retrieved at: https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-state

Litton, A. (2015). The state of surveillance in India: The central monitoring system's chilling effect on self-expression. *Washington University Global Studies Law Review, 14*(4), 799-823.

Lynch, D. (2019, May 22). *How the U.S. – China trade war became a conflict over the future of tech.* The Washington Post. Retrieved at: https://www.washingtonpost.com/business/economy/how-the-us-china-trade-war-became-a-conflict-over-the-future-of-tech/2019/05/22/18148d1c-7ccc-11e9-8ede-f4abf521ef17_story.html?utm_term=.95c59cf7f411

Metz, R. (2019, March 15). *San Francisco just banned facial-recognition technology.* CNN Business. Retrieved at: https://edition.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html

MIT. (2019). *Technology Review: 10 Breakthrough Technologies 2018.* Retrieved at: https://www.technologyreview.com/lists/technologies/2018/

Montag, et al. (2021). EDRi-European Digital Rights. EIJI. *The rise and rise of biometric mass surveillance in the EU*. City and publisher?

Namibia Statistics Agency. (2016). *Namibia Statistical Abstract Report.* Retrieved at: https://d3rp5jatom3eyn.cloudfront.net/cms/assets/documents/Namibia_Statistical_Abstract_Report.pdf

National Planning Commission. (2017*). Namibia's 5th National Development Plan (NDP5)*. Retrieved at: http://www.gov.na/documents/10181/14226/NDP+5/5a0620ab-4f8f-4606-a449-ea0c810898cc?version=1.0

Privacy International. (2015). *The right to privacy in Namibia. Stakeholder report universal periodic review 24th session – Namibia.* Retrieved at: https://www.google.com/search?client=safari&rls=en&q=UN+human+rights+commitee+namibia+surveillance&ie=UTF-8&oe=UTF-8

Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy* 30(1), 53-67. Johns Hopkins University Press. Retrieved May 15, 2019, from Project MUSE database.

Reporters Without Borders. (2022). *World Press Freedom Index.* Retrieved at: https://rsf.org/en/index

Statista. (2019). *Revenues from the artificial intelligence (AI) software market worldwide from 2018 to 2025 (in billion U.S. dollars).* Retrieved at: https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/

Taylor, Rachel C. (2018). Intelligence-sharing agreements & international data protection: avoiding a global surveillance state. *Washington University Global Studies Law Review, 17*(3), 731-760.

The Supreme Court of Namibia. Director-General of the Namibian Central Intelligence Service & another v Haufiku & 2 Others (SA33-2018) [2019] NASC (12 April 2019).

United Nations. (2018). *Namibia Annual United Nations Country Results Report 2017.* Retrieved at: https://www.un.org.na/home_htm_files/Namibia%20Annual%20United%20Nations%20Country%20Results%20Report%202017.pdf

United Nations Development Programme. (2018). *Human Development Report: 2021-2022* Retrieved from https://hdr.undp.org/content/human-development-report-2021-22

Wong, T. (2019, May 19). *Singapore fake news law polices chats and online platforms.* BBC Asia. Retrieved from https://www.bbc.com/news/world-asia-48196985

World Population Review. (2023). Retrieved from https://worldpopulationreview.com