SUBMISSION

DRAFT PROVISIONS OF THE ELECTRONIC TRANSACTIONS AND CYBERCRIME BILL (2017)

June 2017

At the time of writing this brief, indications were that the Namibian government, by way of the Ministry of Information and Communication Technology (MICT), was intent on promulgating the Electronic Transactions and Cybercrime Bill into law by the end of the third quarter of 2017. Urgency in this regard appears to have been an overriding driver behind the Bill's formulation.

However, it should be cautioned that urgency in drafting and promulgating legislation comes with the risk of a flawed and legally problematic regulatory framework eventually being implemented.

The latest draft of the Electronic Transactions and Cybercrime Bill, dated 2017, was put out for stakeholder comment despite the fact that the last meaningful consultations around the provisions of the proposed law had been conducted in 2010 as part of a process which started in 2005. Those consultations culminated with the first substantial draft Bill that was put together with the assistance of International Telecommunications Union (ITU) experts in 2013, through the ITU's Harmonization of the Telecommunication and ICT Policies in Africa (HIPSSA) project, which started in 2008, and produced the Computer Crime and Cybercrime: SADC Model Law, which was also launched in 2013. The 2017 Bill is largely the same as the document produced in 2013 from the ITU template.

In light of this, the ITU standards used to construct this Bill have been criticised for having been constructed “prior to 2014 without public consultation”[1].

With this in mind, relevant Namibian authorities' attention is drawn to a statement by the UN Economic Commission for Africa (UNECA): “It is important to understand that no one person or institution can have the requisite capacity to deal with cybersecurity. Cybersecurity is not an event but rather a process. As a result, it is not simply a matter of passing legislation, or something that belongs to lawyers only. Members of Parliament, lawyers, the judiciary, intelligence/military, civil society, media, young people and members of the public as key stakeholders should all be involved in efforts to deal with cybersecurity at the earliest available opportunity. It is important to engage all stakeholders to ensure the necessary buy-in and that they understand the issues and processes involved.”[2]

Against this backdrop, the following is a critical spotlighting of some of the significant shortcomings, flaws and concerns of the Electronic Transactions and Cybercrime Bill

[1] https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf
[2] http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

(2017).

ELECTRONIC TRANSACTIONS AND CYBERCRIME BILL 2017 – A CRITIQUE

1. Inappropriate two-in-one lawmaking

The Electronic Transactions and Cybercrime Bill (2017) is in essence the Electronic Transactions Bill with cybercrime provisions tagged on towards the end. This goes against best practice in legislating for cybersecurity, or against cybercrime, which mostly is addressed in comprehensive stand-alone cybersecurity laws. The Electronic Transactions and Cybercrime Bill (2017) is not an example of a modern cybersecurity framework proposal. A separate Cybercrime/cybersecurity bill should be crafted around what is captured in chapter 8. The lumping together of two related but different topics in such a significant statutory instrument is the consequence of using a flawed and outdated standard as guide. It is proposed that Namibian authorities separate the two topics and go back to the drawing board to construct a much-improved cybersecurity/cybercrime framework.

2. Problems with key definitions

The definitions section of the draft Bill is incomplete and does not contain definitions of key concepts. In fact, amongst others, neither **cybercrime** nor **cybersecurity** are defined in the proposed law. Such significant omissions certainly indicate that this draft is not a proposed cybersecurity/cybercrime framework. Other key definitions missing are those for "functionary" and "forensic tools", while basic concepts such as "access", "data", "privacy" or "seize" are also not included in the definitions. The list goes on. Some of these terms, including "child pornography", only come up for definition in chapter 8, which feeds into the notion that this bill is actually two draft laws unsatisfactorily melded into one.

Not only are key concepts not defined, but others, such as "computer system" are either woefully under-defined or outdated in their definition. The definitions section needs to be updated and expanded considerably, especially given the specialised and technical nature of the field that is being legislated for.

Against this backdrop, although there is no single, precise definition for cybersecurity or cybercrime, it nevertheless is clear to most in or around the field what is broadly meant by the term. Namibian authorities would do well to engage various and all relevant sectors and actors to put forward, in the first instance, credible, domestically subscribed to, but universally understood, definitions for the concepts falling under the cybersecurity umbrella.

3. Confusing arrangement of cybersecurity related provisions

Unlike cybersecurity laws the world over, the Electronic Transactions and Cybercrime Bill's (2017) cybersecurity provisions are a mish-mash and do not deal in a structured and substantially consequential way with the the necessary aspects of combatting cybercriminal activities. The Bill lacks coherence. To view what a coherent contemporary cybersecurity law proposal looks like, Namibian authorities are requested to view the Cybercrimes and Cybersecurity Bill (2017) of South Africa[3].

[3] http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

4. Unauthorised access, secret warrants and warrantless search & seizure

Of utmost concern is that various sections of the Bill appear to enable warrantless search and seizure operations, while other sections seem to allow for a system of secret warrants and unauthorised access by state agents. In this regard, chapter 5, in sections 43 (2) and (3), seems to enable unauthorised access and access without notification by CRAN and others to computer systems, which would amount to government hacking of private computer systems. The legality of these provisions are highly questionable.

Similarly, in chapter 7, in section 61 (6), (7) and (8), a "Computer Security Inspector", which can be anyone, is also authorised to access computer systems without giving notification or seeking legal authorisation. At the same time, sections of chapter 8, in sections 70 (2) and all of section 72, allow for a system of secret warrants while vaguely defining the conditions under which such secret warrants can be sought. These provisions open the door to pervasive communications surveillance and interception without appropriate oversight mechanisms to monitor the conduct of those carrying out such surveillance or interception activities. It seems clear that unauthorised access by state agents and interception of communications is underregulated, especially when viewed against the body of available literature on these topics.

It has to be further pointed out, in relation to secret warrants, that unlike South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act (Rica), which also provides for a "designated judge" to hear intercept applications, this Bill makes no provision for even the most basic of accounting for such requests. Although Rica's provisions on accounting standards are significantly flawed, they do present some measure of transparency and do provide the public with basic insight, by way of a public annual report by the designated judge into state surveillance and interception. No Namibian law, including this Bill, allows for such transparency or insights.

A system of secret warrants and warrantless accessing of private data and communications and computer systems basically means that "the target of an interception order is never granted the opportunity to test whether the intrusion was lawfully approved – and on the basis of a reasonable suspicion".[4] This is because the judicial process of apply for and granting such warrants is not adverserial.

In this regard the following should be borne in mind: "Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorisation from a competent judicial authority." And also: "States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions."[5]

While some of the Bill's draft provisions are similar to sections of the Communications Act of 2009, it has to be pointed out that the **constitutionality of some of these provisions, along with those of concern in the Communications Act, is highly debatable and challengeable.**

---

4 https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/

5 https://www.eff.org/files/2014/01/05/13p-onepagerfinal.pdf

5. Lack of data and privacy protections

The Electronic Transactions and Cybercrime Bill (2017) is worryingly thin on personal data and privacy protections, and the little that is there comes across as severely under-developed. The draft law does not in any way adequately provide for personal data protection or proscribe the rights of data subjects, in line with international best practice. In this regard: "To assure the public that their data is being appropriately protected, states that do not already have comprehensive personal data protection legislation and a privacy enforcement authority with legal enforcement powers should take steps to create such regimes."[6]

Related to the issue of absent or under-developed privacy and data protection safeguards, as well as the concerns sketched in point 4 above, is that the Bill is silent "on the correct procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from the interceptions".[7]

In the same vein, and in this context of invasion of privacy, this is highly problematic, as the "target of the interception order is never informed of the order, even after the period of interception has ended and even after any investigation has been concluded."[8] When it comes to informing or notifiying targets, after the fact, of invasive surveillance and interception, perhaps Namibian authorities should look at frameworks used in the US, Japan, Austria and Chile, which seem to be the countries with user notification legal dispensations that can be emulated.

Given that the right to privacy is explicitly enshrined in the Namibian Constitution, **the absence of substantive personal data and privacy protections in the draft law raises serious constitutional questions**, especially in relation to the concerns sketched in point 4 above.

Against this backdrop, Namibian authorities are thus encouraged to formulate a comprehensive data protection framework and can look to such countries as Singapore[9] for guidance, as well as to the EU and South Africa.

6. Undermining of encryption and anonymity

Chapter 5 (Accreditation of Security Services or Products) of the draft law deals with the regulation of encryption devices and technologies.

This chapter, which seeks to introduce a rather onerous and intrusive registration regime, appears throughout to enable state agents to establish and open "backdoors" in encryption tecnologies.

These provisions should be tested against best practice and brought up to date. In this regard, the Global Commission on Internet Governance (GCIG) states[10]: "Anonymity-granting technologies and end-to-end encryption provide the security and privacy necessary for exercising fundamental human rights online and for individuals, businesses and governments to engage activities that support economic growth and social progress."

6 https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf
7 https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/
8 https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1/
9 https://www.pdpc.gov.sg/legislation-and-guidelines/overview
10 https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

And it recommends that: “Governments should not compromise or require third parties to weaken or compromise encryption standards, for example, through hidden “backdoors” into the technology as such efforts would weaken the overall security of digital data flows and transactions.” The proposed provisions of the 2017 draft should be measured against such assertions, with particular and appropriate input from the technical community, as well as other stakeholders.

In our analysis, provisions seeking to regulate the use of encryption technologies do seem to be aimed at weakening such technologies, and thus would open the door to such technologies being infiltrated by criminal and other malignant actors.

7. Lack of transparency and access to information

The draft law throughout suffers from a lack of transparency-inducing measures, and does not in any way compel government authorities, law enforcement or private companies to account for their actions openly. In this regard, the emerging trend is that: “Private companies should publish transparency reports that reveal the amount of content being restricted or blocked in response to requests by governments, for what purposes and by what means. Governments must allow companies to publish aggregate information about what they have requested and how the company responded.[11]

Such measures would allay fears of the abuse of secret warrants, amongst others, and would give the public confidence that the law was not being used gratuitously to violate individual privacy and the integrity of private data systems.

On a related aspect, the draft law does not appear to explicitly encourage access to information. This appears to be inconsistent with ongoing access to information legislating in Namibia and current and emergent global best practice.

8. Excessive and unaccountable ministerial power

Related to the point above about a lack of transparency, is the vesting of discretionary decision-making and appointing power in the minister. No oversight or accountability measures are included with regard to ministerial conduct under the provisions of this draft law. In this regard the AU Convention on Cyber Security and Personal Data Protection calls on states to: “Establish clear accountability in matters of cyber security at all levels of government by defining the roles and responsibilities in precise terms.”

It has to be questioned to what extent the relevant draft provisions that vest various powers in the minister, and those he empowers, would be in line with Namibia's emerging access to information legislation (which also appears set for promulgation before the end of the third quarter of 2017) and current best practice, which points to the emergence of more collaborative systems of accountability in dealing with cybersecurity issues. It would seem that the Electronic Transactions and Cybercrime Bill (2017) would not be compatible with such emergent legal and best practice dispensations.

9. Too lenient an approach to service provider or intermediate liability

While the law incorporates provisions in Chapter 6 (Liability of Service Providers for

[11] https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf

Unlawful Material) to protect service providers who merely serve as hosts or conduits for third-party content, concerning such provisions AccessNow states that: “This type of legal protection enabled the growth of the internet and allows the smooth functioning of the global web at scale, so these provisions must be retained.”[12] Whether the provisions of the Electronic Transactions and Cybercrime Bill (2017) are up to standard in terms of intermediate liability is open to question, and should be further investigated through a process of open and extensive consultation.

It is the contention of this submission that the Electronic Transactions and Cybercrime Bill (2017) takes too lenient an approach to intermediate or service provider liability.

10. General observations

In the final analysis, the Electronic Transactions and Cybercrime Bill (2017) is substantially weak on adequate and appropriate judicial, legislative and public oversight mechanisms, to especially prevent abuse of potential communications surveillance and interception provisions and mechanisms. To put it bluntly, this draft law makes no provision for multistakeholder oversight mechanisms, and given the Namibian state's acknowledged capacity limitations, this could make for constrained implementation of any cybersecurity regulatory framework ultimately promulgated.

CONCLUSION

With some of the provisions of the Electronic Transactions and Cybercrime Bill (2017) not having been crafted or completed in an extensively consultative process, it is concerning that the latest draft managed to make it this far, and even briefly onto the parliamentary agenda. The draft that has been put out for stakeholder comment and inputs appears significantly flawed and would not be fit for purpose if enacted in its current form.

And in conclusion we wish to reiterate that “Cyber policy and law making is in its infancy and requires the input of different stakeholders. Truly effective security must be done as a collaboration and no one actor can claim to have the solution. This requires trust and efforts to understand different stakeholder perspectives.”[13]

It is against this backdrop that we make the following recommendations.

RECOMMENDATIONS

1. In the first instance, we call on the relevant Namibian authorities to withdraw the Electronic Transactions and Cybercrime Bill (2017) as a matter of urgency;

2. We call on relevant Namibian authorities to use the best possible examples of cybersecurity/cybercrime frameworks as guides for designing, drafting and implementing a Namibian framework;

3. In the process of coming up with such a framework, it is recommended that relevant Namibian decision and law-making authorities, as well as legal drafters, as an initial

[12] https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf
[13] https://www.privacyinternational.org/sites/default/files/CyberSecurity_2017.pdf

step, commence a review of the extensive existing body of literature and materials on cybersecurity-related issues and measures in order to, firstly, acquaint themselves with the issues and the myriad voices on the constantly-evolving cybercrime and cybersecurity landscape, and secondly, assess whether Namibia's proposed cybersecurity efforts are in line with emergent trends and best practices towards the installation of the best possible framework for the Namibian context;

4. And most importantly, and in line with international best practice, we recommend that any cybersecurity law and institutional framework be the product of an extensive and meaningful cooperative multi-stakeholder consultative process and that the eventual framework make provision for some level of multi-stakeholder oversight involvement.

Finally, we herewith make ourselves available to assist relevant Namibian authorities in any way possible in the drafting, redrafting or researching of the best possible cybersecurity/cybercrime legislative and regulatory framework.

Submitted by:

Frederico Links,
Chairperson, ACTION Namibia Coalition
fredericojlinks@gmail.com
081 233 4705

Graham Hopwood,
Executive Director, Institute for Public Policy Research (IPPR)
director@ippr.org.na
081 294 3340