PRIVACY INTERNATIONAL

The Right to Privacy in Namibia

Stakeholder Report
Universal Periodic Review
24th Session - Namibia

Submitted by Privacy International
June 2015

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.

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.[1] 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.[2]

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.[3]

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.*

---

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

3 A/HRC.17/14, para 78

(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].*"[4]

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.[5]

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.[6]

---

4 General Comment No. 16 (1988), para. 1https://www.ifex.org/namibia/2008/11/25/new_bill_on_communication_interception/

5 See: Namibia News Digest, *KK Accuses Govt of Spying*, 25 March 2014. Available at: http://www.namibianewsdigest.com/5439/; AllAfrica, *Namibia: Look Before You Leap,* 4 April 2014. Available at:

6 See: MISA, New bill on Communication interception infringes on free expression, says MISA, 25 November 2008. Available at: https://www.ifex.org/namibia/2008/11/25/new_bill_on_communication_interception/; Institute for Public Policy Research, *Comments regarding Communications Bill (as read a First Time) [BB.6-2009].*

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'.[7] 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.[8]

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 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[9] 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)

Available at: http://www.ippr.org.na/sites/default/files/IPPR-Nepru%20submission%20on%20Communications%20Bill.pdf

7 No 8 of 2008, Communications Act, published in government Gazette, 16 November 2009, No. 4378, Part 6, Para. 70-77. Available at: http://www.lac.org.na/laws/2009/4378.pdf

8 No. 10 of 1997, Namibia Central Intelligence Service Act, published in Government Gazette, 7 October 1997, No. 1699, Article 3 (a). Available at: http://www.lac.org.na/laws/1997/1699.pdf

9 The 2009 Communications grants under Article 70(3) the right to the Director General of the NCSI to specify which equipment and software the telecommunication service providers must install on their communications systems.

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.[10] 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. In order 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.[11] The function, management and operations of the NCIS is regulated by Namibian Central Intelligence Service (NCIS) Act, 1997 (Act No 19, 1997).[12] 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 fishing 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".*

---

10 Institute for Public Policy Research, *Comments regarding Communications Bill (as read a First Time) [BB.6-2009].* Available at: http://www.ippr.org.na/sites/default/files/IPPR-Nepru%20submission%20on%20Communications%20Bill.pdf

11 Namibia Central Intelligence Services, About us: Historical Background. Available at: http://209.88.21.36/opencms/opencms/NCIS/aboutus.html

12 No. 10 of 1997, Namibia Central Intelligence Service Act, published in Government Gazette, 7 October 1997, No. 1699. Available at: http://www.lac.org.na/laws/1997/1699.pdf

28. Further more 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.[13]

30. In August 2013, the NCIS was reported to have been in touch with the US National Security Agency (NSA) regarding plans for the them to implement a system which would allow it to monitor all emails and internet communications.[14]

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.[15]

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.[16]

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.[17]

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

---

13 Grobler, J., *Spy bill spooks experts*, The Namibian, 8 June 2014. Available at: http://www.namibian.com.na/indexx.php?archive_id=54177&page_type=archive_story_detail&page=3006

14 Insight Namibia, No protocol observed, 14 August 2013. Available at: http://www.insight.com.na/no-protocol-observed-71/

15 Budget speech by Honourable Jetekro Tweya, MP, Minister of Information and Communication Technology, Vote 29 of the Ministry of Information and Communication Technology, 22 April 2015. Available at: http://209.88.21.36/opencms/opencms/grnnet/MICTv2/t2news/news_0014.html

16 Insight Namibia, *Birth of the surveillance state,* 23 August 2014. Available at: http://www.insight.com.na/birth-of-the-surveillance-state/

17 No. 12 of 2012. Signed by the President on 5 December 2012 and published in the Government Gazette on 14 December 2012, No. 5095. Available at: http://www.lac.org.na/laws/2012/5095.pdf

page document.[18] The government justified the rush saying that it was a matter of urgency that Namibia adopt such a law amid global growing terror threats.[19]

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.[20]

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 (s 14), fairness (s 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.[21]

41. The current lack of a comprehensive data protection law is of particular concern in view of the following:

---

18 Muraranganda, E., *Anti-Terrorism Act rushed – IPPR*, Namibian Sun, 31 May 2013. Available at: http://www.namibiansun.com/government/anti-terrorism-act-rushed-ippr.53319

19 Nkala, O., *Namibia unveils anti-terror bill to plug national security loopholes* , DefenceWeb, 5 December 2012. Available at: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=28755:namibia-unveils-anti-terror-bill-to-plug-national-security-loopholes&catid=49:National%20Security&Itemid=115

20 See: HIPSSA Project, *Presentation of the draft data protection policy for Namibia* by Pria Chetty, ITU International Legal Expert on Data Protection. Available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/In-country%20support%20documents/Namibia_Data_Protection_Draft_Policy_Chetty_Version1.pdf

21 See: HIPSSA Project, *Presentation of the draft data protection policy for Namibia* by Samson Muhapi, ITU National Legal Expert on Data Protection. Available at http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/In-country%20support%20documents/Namibia_Final%20presentation%20Muhapi%20v5%20data%20protection.pdf

- 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.[22]
- 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.[23] 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 a 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. [24]*Namibia unveils 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.[25]

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 as well as 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 its citizens, and ensure those those responsible are sanctioned and case of

---

22 See: Government of Namibia, I*D Documents*. Available at: http://www.gov.na/identity-documents; Dentlingerm, L., Issuing of ID cards to be speeded up, The Namibian, 17 June 2005. Available at: http://www.namibian.com.na/indexx.php?archive_id=14606&page_type=archive_story_detail&page=6638

23 ITWeb, *Biometrics help stop healthcare fraud*, 26 September 2013. Available at: http://www.itweb.co.za/index.php?*option=com_content&view=article&id=67655*

24 Planet Biometrics, *Biometrics play supporting role in Namibia's electronic vote*, 28 November 2014. Available at: http://www.planetbiometrics.com/article-details/i/2450/

25 Mutelo, R., *Namibia's Biometric Systems' banking solution*, New Era, 10 September 2014. Available at: https://www.newera.com.na/2014/09/10/namibias-biometric-systems-banking-solution/