PRIVACY INTERNATIONAL

Stakeholder Report Universal Periodic Review
25th Session – Tanzania

The Right to Privacy in the United Republic of Tanzania

Submitted by Privacy International, Tanzania Human Rights Defenders Coalition, Collaboration on International ICT Policy in East and Southern Africa

September 2015

I. Introduction

1. This stakeholder report is submitted by the Tanzania Human Rights Defenders Coalition, the Collaboration on International ICT Policy in East and Southern Africa and Privacy International (PI).

2. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. The Tanzania Human Rights Defenders Coalition (THRDC) is membership Organization in Tanzania, with over 115 members, both individual Human Rights Defenders and Human Rights Organizations membership working towards enhancing the security and protection of Human Rights Defenders (HRDs) in Tanzania. THRDC's long-term goals are to see a free and secured environment for human rights defenders in Tanzania, and to ensure HRDs in our country are able to carry out their essential work free from harm and repression, in accordance with the UN Declaration on Human rights defenders of 1998. The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) is one of two centres established in 2004 under the Catalysing Access to Information and Communication Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA is a leading centre for research and information brokerage to enable policy makers in the region to understand ICT policy issues, and for various stakeholders to use ICT to improve governance and livelihoods.

3. PI, THRDC and CIPESA wish to bring concerns about the protection and promotion of the right to privacy in the United Republic of Tanzania (thereafter "Tanzania") before the Human Rights Council for consideration in its upcoming review.

The right to privacy

4. 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.

5. 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]

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.

Follow up to the previous UPR

6. There was no mention of the right to privacy and data protection in the National Report submitted by Tanzania. Previous UPR stakeholder reports[3] raised concerns about lack of adequate guidelines for when a patient's HIV status could be disclosed to a third party.[4]

Domestic laws related to privacy

7. The Constitution of the United Republic of Tanzania[5] guarantees a right to privacy under Article 16:

> "*16. - (1) Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications."*
> *(2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.*"

8. Under Article 18(c) of Constitution further guarantees the freedom to communicate and protection from interference, and reads as follows,

> "*18. - Every person -*
> *(c) has the freedom to communicate and a freedom with protection from interference from his communication;*"

International obligations

9. Tanzania 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*" .

10. 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].*"[6]

II. Areas of concern

Lack of judicial authorisation and oversight of communication surveillance

11. The capacity of Tanzania to conduct surveillance of communications is unknown, but the US State Department Human Rights report of 2014 for Tanzania noted that "it

3 Summary of Stakeholder Submissions to the Universal Periodic Review. Human Rights Council. October 2011, http://www.ohchr.org/EN/HRBodies/UPR/Pages/TZSession12.aspx
4 A/HRC/WG.6/12/TZA/3, para 34. Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/151/48/PDF/G1115148.pdf?OpenElement
5 The Constitution of the United Republic of Tanzania, 1977. Available at: http://www.judiciary.go.tz/downloads/constitution.pdf
6 General Comment No. 16 (1988), para. 1

was widely believed that state actors monitored telephones and correspondence of some citizens and foreign residents. The actual nature and extent of this practice were unknown".[7]

12. In 2011, JamiiForums, an online forum that has been called the "Swahili language version of Wikileaks, was cloned by the Tanzanian government to disrupt the conversations of members associated with the opposition. The founders of the forum were also detained and interrogated for 24 hours in 2008.[8]

13. Also, emails released by WikiLeaks on 8 July 2015 from the Italian surveillance malware vendor Hacking Team, reveal an exchange between representative from the Tanzanian President's Office and HackingTeam.[9] An email from the government representative expressed interest in visiting Hacking Team's office in view of purchasing its Galileo surveillance system[10], which has the ability of this surveillance technology to bypass encryption, take control of a user's device, and to monitor all activities conducted on the device, poses significant threats to the right to privacy.

14. These instances are of significant concern, given that the legal framework and oversight of interception of communication falls short of applicable international human rights standards.

15. In 2012, Tanzania adopted the Electronic and Postal Communications Act (ECOPA)[11]. When it was being drafted, civil society had expressed concern over certain provisions which would negatively impact the right to privacy.[12]

16. Whilst ECOPA does not include a specific provision for the interception of communications, it can be argued that Section 120 of the Act implies a power to intercept as this Section provides that the interception of communications without lawful authority under this Act or any other written law, constitute an offence.[13]

17. Furthermore, under Section 121 of the Act, "It shall be lawful under this Act for an officer, employee or agent of any network facilities provider, network service provider, application service provider or content service provider whose facilities or services are used in communications, to intercept, disclose, or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the performance of his facilities or services or to the protection of the rights or property of the provider of the facilities or services, but the provider shall not utilize the facilities or services for observing or random monitoring".

18. Interception of communications is explicitly provided in the 2002 Prevention of Terrorism Act and the 1996 Intelligence and Security Service Act.

19. Under Section 31 of the 2002 Prevention of Terrorism Act, "a police officer may for

7 US State Department, Tanzania 2014 Human Rights Report, Available at: http://www.state.gov/documents/organization/236626.pdf
8 CIPESA, State of Internet Freedoms in Tanzania 2014: An Investigation Into the Policies And Practices Defining Internet Freedom in Tanzania, May 2014. Available at: http://www.cipesa.org/?wpfb_dl=182
9 Available at: https://wikileaks.org/hackingteam/emails/emailid/11776
10 Galileo is a remote control system which allows to take control of a target and to monitor them even if they are using encryption. Hacking Team sells it as a tool to "bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain." For more information: https://www.hackingteam.it/images/stories/galileo.pdf
11 This Act replaced the Tanzania Communications Act No.18/1993 and Tanzania Broadcasting Services Act No.6/1993
12 Media Institute of Souther African (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/
13 Vodafone, Law Enforcement Disclosure Report, Updated Legal Annexe, February 2015, pp. 96. Available at: http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf

the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order." Section 31 of Subsection 4 of this Act allows for the use of any communications intercepted, including from outside of the country, to be admissible in proceedings for any offence under the Act.

20. The Tanzania Intelligence and Security Service Act of 1996[14], which established the Tanzania Intelligence and Security Service (TISS), the national intelligence and security agency of Tanzania, as a department of the Government within the office of the President, also provides for surveillance powers.

21. Section 5(2) notes that the TISS shall not institute surveillance of any person or category of persons by reason only of his or their involvement in lawful protest, or dissent in respect of any matter affecting the Constitution, the laws or the Government of Tanzania."

22. However, Section 14 gives the TISS power to collect, and analyse, retain "information and intelligence respecting activities that may on reasonable grounds be suspected of constituting a threat to the security of the United Republic or any part of it." Whilst the terms "security" and "threats to the security of the United Republic" a defined by the Act[15], their broadness is highly concerning and provides the TISS with extensive powers with minimal provisions for oversight of the agency.

23. The 1996 Act also directs the minister responsible for intelligence and security to make "regulations which shall constitute the code of conduct for all officers and employees of the Service in relation to the conduct, discipline, presentation, considerations, ethical standards and general directions to be adhered to in the carrying out of the functions and exercise of the powers conferred on the service." These regulations "shall be published only to members of the Service" or as the minister sees fit.[16]

24. In her June 2014 report on the right to privacy in the digital age, the former UN High Commissioner for Human Rights, Navi Pillay, noted the "disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability."[17] It is essential that Tanzania rectify the deficit in transparency and oversight of surveillance.

25. This lack of transparency and oversight of the TISS is compounded by the fact that there is no requirement of judicial authorisation for interception of communications. Section 18 outlines the powers to investigate and conduct interception of communications which permit the Tanzanian intelligence service to enter into arrangements with various other actors including any person, local government or

14 Available at: http://www.parliament.go.tz/polis/PAMS/docs/15-1996.pdf
15 "Security" means the protection of the United Republic from acts of espionage, sabotage and subversion, whether or not it is directed from or intended to be committed within the United Republic;'threats to the security of the United Republic'' means- (a) espionage, sabotage or other activities which are against Tanzania or are detrimental to the integrity, sovereignty or other interests of Tanzania or activities directed toward or in support of such espionage or sabotage. (b) foreign influenced activities within or relating to Tanzania that are detrimental to the interests of Tanzania, are clandestine or deceptive or involve a threat to any person. (c) activities within or relating to Tanzania directed toward or in support of the threat or use of acts of serious violence- against persons or property for the purpose of achieving a political objective within Tanzania or a foreign state; and (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Tanzania, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d)
16 Tanzania Intelligence and Security Service Act (1996), section 9(3) and 9(4).
17 A/HRC/27/37, para. 48.

other authority, any police force or other policing organisations as well as government of foreign states or an international organisations of states with the sole authorisation of the Minister made responsible for the TISS, as well as the Minister of Foreign Affairs in the case of engagement with foreign governments and organisations.

26. On 8 May 2015, the government of Tanzania announced[18] that the President had signed the Tanzanian Cybercrimes Act 2015.[19] However after strong criticism within Tanzania, from both the opposition and civil society organisations, but also international human rights groups, the government had committed to review the Act before the end of the parliamentary session.[20] The Cybercrime law is in operation since 1 September 2015 with no major changes except for section 20 of the Cyber crime law.

27. THRDC we have filed the Constitutional Petition in National court challenging the Cyber crime Act.[21] Focusing on two main grounds. Firstly that the provisions of sections 31, 32, 33, 34, 35 and 37 of The Cyber Crimes Act give powers to law enforcers to search and seize computer systems, data and information without court order thus can infringe right to privacy as provided for under the Constitution of United Republic of Tanzania.

28. Secondly, THRDC will argue that the provisions of sections 6, 7, 8, 9, 10, 11, 14, 19, 21 and 22 of The Cyber Crimes Act contain undefined phrases which are likely to be subjected to subjective interpretation by law enforcers and thereby risking arbitrary arrests thus contravening the right to liberty as provided for under The Constitution of United Republic of Tanzania of 1977 as amended.

29. Among the main concerns, the Act gives extensive surveillance powers to the police, including to use intrusive surveillance methods such as keylogging devices or software that records every keyboard stroke of personal computers in real time, without strictly requiring judicial prior authorisation or oversight. Other concerns relate to the lack of protection of whistleblowers.[22]

30. The aforementioned requirements are essential to ensure that the Cybercrime Act is in compliance with Tanzania's national and international human rights obligations, and in particular the principles of necessity, proportionality, judicial authorisation, and oversight in relations to communication surveillance.[23]

31. Furthermore, Sections 39-44 on the liability of ISPs and the powers conferred on them to monitor communications, remove information, terminate or suspend services, and notify law enforcement agencies of any alleged illegal activity, given the ISP the full discretion to determine what constitutes an illegal activity.

32. As noted in the UN Guiding Principles on Business and Human Rights, the private

18 Statement by Hon. Prof. Makame Mbarawa (MP), Minister of Communication, Science and Technology, 8 May 2015. Available at: http://www.mst.go.tz/index.php/78-news/126-taarifa-ya-mhe-prof-makame-mbarawa-mb-waziri-wa-mawasiliano-sayansi-na-teknolojia-kuhusu-sheria-ya-makosa-ya-mtandao-ya-mwaka-2015-kwa-waandishi-wa-habari

19 Available at: http://www.parliament.go.tz/polis/PAMS/docs/1-2015-4.pdf

20 Article 19, Tanzania: Cybercrime Act 2015, Legal Analysis, May 2015. Available at: https://www.article19.org/data/files/medialibrary/38058/Tanzania-Cybercrime-Bill-TO.pdf

21 http://www.thecitizen.co.tz/News/Parts-of-Cybercrime-Act-opposed-in-court/-/1840340/2867400/-/559hn2/-/index.html

22 See: Article 19, Tanzania: Cybercrime Act 2015, Legal Analysis, May 2015. Available at: https://www.article19.org/data/files/medialibrary/38058/Tanzania-Cybercrime-Bill-TO.pdf; Marari, D., Of Tanzania's cybercrimes law and the threat to freedom of expression and information, AfricaLaw, 25 May 2015. Available at: http://africlaw.com/2015/05/25/of-tanzanias-cybercrimes-law-and-the-threat-to-freedom-of-expression-and-information/#more-930; CIPESA, Tanzania Cybercrime Bill Should Safeguard Citizens' Right on the Internet, 2 April 2015. Available at: http://www.cipesa.org/2015/04/tanzania-cyber-crime-bill-should-safeguard-citizens-rights-on-the-internet/

23 See: https://necessaryandproportionate.org/

sector has a responsibility to respect human rights. Furthermore, as noted by the Navi Pillay, former UN High Commissioner for Human Rights, in her report on privacy in the digital age, "*There is a strong evidence of a growing reliance by Government on the private sector to conduct and facilitate digital surveillance*".[24] She requested that companies must have their own internal policies in place, as well as due diligence policies to "*identify, assess, prevent and mitigate any adverse impact*" on the human rights of users. When requested to provide data or access that fails to meet international human rights standards, they should interpret the these demands as narrowly as possible, as well as request clarification on scope and legal premise for request, a court order and be transparent with users when they received such requests.[25]

Mandatory SIM Card Registration and National Database

33. The 2010 Electronic and Postal Communications Act (EPOCA)[26] mandates the Communication regulatory authority to maintain a database of all subscriber information. Under Section 89 of the Act calls for all subscriber information to be kept by the Tanzania Communications Regulatory Authority (TCRA) maintains a database of subscriber information. The service providers are required by Section 91 to submit all subscriber information to the TCRA once a month.

34. Under Section 93 of the EPOCA, "Every person who owns or intends to use detachable SIM card or built-in SIM card mobile telephone shall be obliged to register SIM card or built in SIM card mobile telephone" and para (2) and (3) outlines the information that must be registered for natural and legal persons respectively.

35. Failure on the part of the operator to register a subscriber, and a user's use of an unregistered SIM card are both subject to fines and/or imprisonments.

36. The ECOPA Consumer Protection Regulations 2011[27] and the EPOCA Licensing Regulations 2011[28] establish a mandatory SIM card registration policy. Section 10(2) of the ECOPA Consumer Protection Regulations 2011 requires all persons who intend to use a SIM card to register the SIM card with the service provider, giving their full name, identity card number, and registered address. If the user is a business, it must also provide its business license and taxpayer number. Section 33 of the EPOCA Licensing Regulations 2011 requires that, "Any person who sells or , in any other manner provides detachable SIM card or built-in SIM card mobile telephone to any potential subscriber shall register subscribers using Form as provided in the Third Schedule to these Regulations."

37. Mandatory SIM card registration facilitates the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location-tracking, and simplifying communications surveillance and interception.

38. Concerns have been expressed that the ECOPA fails to provide a justification as to why subscribers' data is collected.[29] And whilst the two regulations requires

24 A/HRC/27/37, para. 42
25 A/HRC/27/37, para. 43-45
26 This Act replaced the Tanzania Communications Act No.18/1993 and Tanzania Broadcasting Services Act No.6/1993
27 Available at: https://www.tcra.go.tz/images/documents/regulations/consumerProtection.pdf
28 Available at: https://www.tcra.go.tz/images/documents/regulations/licensing.pdf
29 CIPESA, State of Internet Freedoms in Tanzania 2014: An Investigation Into the Policies And Practices Defining Internet Freedom in Tanzania, May 2014. Available at: http://www.cipesa.org/?wpfb_dl=182 wpfb_dl=182

employees of service providers to maintain the confidentially of customer information and requires the protection against improper or accidental disclosure of consumer information, the lack of a provisions as to how the database is managed, maintained and its security protected to guarantee individuals' rights to privacy and data protection particularly given the lack of a data protection framework established in Tanzania.

Lack of Comprehensive Data Protection Law

39. Tanzania currently lacks a comprehensive data protection and privacy law. A bill has been in progress since 2014 when the Ministry of Communications, Science and Technology announced that a bill was being developed as part of its cybersecurity initiative.[30]

40. Without these legal protections and procedural safeguards in place, the government has few restrictions on how to handle personal data collected through data processing initiatives which include:

41. Biometrics voter registration: GenKey, a Dutch company, working as a subcontractor for South Africa-based Lithotech Exports, has been developing and implementing its Automated Biometrics Identification Solution (ABIS), its SpiRE Voter ID Management Solution, and its Adjudication Solution.[31] The registration system commenced earlier in 2015 using registration kits provided by China[32] which saw the registration of 24 million eligible voters. While recognising that biometric technology is not harmful per se, it must be regulated and data collected only for limited, specific purposes. Without appropriate safeguards, biometric data can be used as a tool for surveillance through profiling, data mining and big data analysis. The use of biometric technology in various African countries in recent year for the elections illustrated that the functionality of biometric systems is not always reliable and resulted in the need to resort to manual methods.[33] Furthermore, the lack of data protection framework in Tanzania in view of the involvement of foreign companies in the processing of personal data of citizens is highly concerning.

42. Disclosure of information on persons living with HIV: The Canadian HIV/AIDS Legal Network and Women's Legal Aid Centre have previously raised concerns about lack of adequate guidelines for the disclosure of information on individuals living with HIV with a third party in Tanzania.[34] The disclosure of such information could lead to stigmatisation and discrimination, and it is thus essential that the right to privacy of individuals living with HIV be upheld and protected through the adoption of guiding principles for health care professionals and other relevant actors processing such sensitive data such as the International Guidelines on HIV/AIDS and Human Rights.

30 Data Guidance, Tanzania: Data protection bill announced as part of the cybersecurity initiative, 18 May 2014. Available at: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2415
31 Genkey, Lithotech uses Genkey's solutions for Biometric Voter Registration in Tanzania, 7 September 2015. Available at: http://www.genkey.com/en/news-archive/lithotech-uses-genkeys-solutions-biometric-voter-registration-tanzania
32 Planet Biometrics, Biometric voter registration launches in Tanzania, 24 February 2015. Available at: http://www.planetbiometrics.com/article-details/i/2740/
33 Wrong, M., Africa's Election Aid Fiasco, The Spectator, 20 April 2013. Available at: http://www.spectator.co.uk/features/8890471/the-technological-fix/
34 See: Submission by Canadian HIV/AIDS Legal Network , Toronto, Canada, and Women's Legal Aid Centre, Dar es Salaam, Tanzania. Available at: http://lib.ohchr.org/HRBodies/UPR/Documents/session12/TZ/JS7-JointSubmission7-eng.pdf

III. Recommendations

We recommend that the government of the United Republic of Tanzania:

1. Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards and respect the right to privacy;

2. Ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted.

3. Strengthen effective oversight over the surveillance practices of its state security and intelligence agencies;

4. Review the Cybercrime Act to ensure its compliance with Tanzania's national and international human rights obligations, and in particular the principles of necessity, proportionality, judicial authorisation, and oversight in relations to communication surveillance;

5. Investigate reported unlawful communications surveillance activities by state agencies, and take necessary measures to ensure access to redress in case of violations;

6. Revoke mandatory SIM card registration policy established by ECOPA Consumer Protection Regulations 2011 and the ECOPA Licensing Regulations 2011, and the provision under the 2010 Electronic and Postal Communications Act (ECOPA) requesting the maintenance of all subscriber information;

7. Adopt a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority;

8. Ensure that data processing of personal data is conducted in compliance with national and international standards and obligations, particularly with regards to the processing of sensitive personal information, and any violations are investigated and redress provided to victims.