PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic
26th Session – Uganda

The Right to Privacy in Uganda

Submitted by Unwanted Witness Uganda, the Collaboration on International ICT Policy for East and Southern Africa, the East and Horn of Africa Human Rights Defenders Project and Privacy International

March 2016

Introduction

1. This stakeholder report is a submission by Privacy International (PI), Unwanted Witness Uganda, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) and the East and Horn of Africa Human Rights Defenders Project (EHAHRDP).

2. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. The Unwanted Witness Uganda is a Uganda based organization working for an open, free and secure internet that contributes to the realization of human rights and good governance. CIPESA is one of two centres established in 2004 under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative. CIPESA is a leading centre for research and information brokerage on ICT for improved livelihoods and ICT policy issues in the region. EHAHRDP is a regional non-governmental organization that seeks to strengthen the work of human rights defenders (HRDs) throughout the region by reducing their vulnerability to the risk of persecution and by enhancing their capacity to effectively defend human rights.

3. Unwanted Witness, CIPESA, EHAHRDP and PI wish to bring concerns about the protection and promotion of the right to privacy in Uganda before the Human Rights Council for consideration in Uganda's 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]

6. As innovations in information technology have enabled previously unimagined forms

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.

of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[3] A number of international instruments enshrine data protection principles,[4] and many domestic legislatures have incorporated such principles into national law.[5]

Follow up to the previous UPR

7. There was no mention of the right to privacy within the context of communication surveillance and data protection in the National Report submitted by Uganda nor in the stakeholders' submissions.

8. A joint stakeholder submission[6] stated that the current equality and non-discrimination legal framework reinforced the social stigma against lesbian, gay, bisexual and transgender individuals and exposed them to the risk of deprivation of liberty, life, right to privacy, physical integrity and health.[7] Additional concerns included the impact of retention of laws and the proposed enactment of new laws that further criminalize sexual relationships between same-sex consenting adults.[8]

9. Slovakia and Netherlands both raised concerns on the crackdown on civil society, human rights defenders and journalists, and urged Uganda to ensure these actors could freely exercise their work.[9]

Domestic laws related to privacy

10. The 1995 Ugandan constitution explicitly recognises the right to privacy and calls for its protection:

    Article 27 specifically notes that:

    (1) No person shall be subjected to—
    (a) unlawful search of the person, home or other property of that person; or
    (b) unlawful entry by others of the premises of that person.
    (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

11. Since this explicit recognition, Uganda has still not yet been able to adopt a data protection law. In 2014, Uganda's government through the National Information Technology Authority (NITA), the Ministry of Information Communication and Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MoJCA)

3 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)
4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)
5 As of December 2013, 101 countries had enacted data protection legislation.
See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416
6 JS8 Human Rights Network-Uganda, Uganda; Development Foundation for Rural Areas, Uganda; Education Access Africa, Uganda; Gideon Foundation against Child Sacrifice, Uganda; Good Hope Foundation for Rural Development, Uganda; Human Rights and Development Concern, Uganda; Human Rights Awareness and Promotion Forum, Uganda; Human Rights Concern, Uganda; Rule of Law Association, Uganda; Uganda Coalition on the International Criminal Court, Uganda.
7 A/HRC/WG.6/12/UGA/3, para. 21
8 JS1 SIPD-UGANDA, Uganda; TITS-UGANDA, Uganda; KULHASUGANDA, Uganda; Frank and Candy, Uganda; Queer Youth Uganda, Uganda; Icebreakers Uganda, Uganda; Sexual Minorities, Uganda; Spectrum Uganda Mission, Uganda; Freedom and Roam Uganda, Uganda; Participatory Action for Rural Development Initiative (PARDI) and Human Rights Watch
9 A/HRC/19/16, Recommendations 111.75 and 111.76

issued a draft Data Protection and Privacy Bill for public comment but there has been no progress since.

International obligations

12. Uganda has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR 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". The Human Rights Committee has noted that states party 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]."[10]

Areas of concern

I. Communications surveillance

13. In the last few years, there has been an increased concern of surveillance of political dissidents, human rights defenders, and journalists in Uganda.[11] These concerns have been heightened with the adoption of Regulation of Interception of Communications Act (RICA) in 2010 which provided broad provisions for interception of communications with limited oversight or safeguards, and on-going legislative process to adopt the Non-Governmental Organizations Bill which was gazetted in 2015 and stifles civic engagement by restricting the operations of NGOs.

14. In addition, whilst the extent of the surveillance capabilities of the Government of Uganda is unclear and leaked documents in July 2015 failed to confirm surveillance technologies had been sold to Uganda,[12] a report by Privacy International published in October 2015 has provided evidence of the sale of intrusion malware FinFisher by Gamma International GmbH ('Gamma') to the Ugandan military. The malware was used to infect communications devices of key opposition leaders, media and establishment insiders over period between 2011 and 2013. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili).

15. This evidence in the context of a poor and inadequate legal framework raises some significant concerns of the surveillance practices of the government of Uganda.

Interception of communication

16. Communications surveillance is primarily regulated by the Regulation of Interception of Communications Act (RICA) 2010, though other acts grant the security services wide-ranging communications surveillance powers including the 2015 Anti-Terrorism (Amended) Act. The adoption of RICA three days after the twin bomb attacks in Kampala in July 2010[13] illustrates the context in which it was adopted given the fact

10 General Comment No. 16 (1988), para. 1

11 In a survey conducted in 2015 by CIPESA of human rights defenders, bloggers, journalists, editors, media rights organisations, sexual minorities and gender equality activists, 76% of the respondents thought that government agencies were monitoring and intercepting citizens' communications. See: CIPESA, State of Internet Freedom in in Uganda 2015, August 2015. pp. 9. Available at: http://www.cipesa.org/?wpfb_dl=209

12 Wikileaks, Hacking Team, dated 8 June 2016. Available at: https://wikileaks.org/hackingteam/emails/emailid/11829

13 As Ugandans gathered in bars and restaurants to watch the FIFA World Cup final on 11th July, militants linked to the Islamist group Al Shabaab detonated bombs at Lugogo Rugby Club and the Ethiopian Village restaurant, killing over 70 people and injuring many more. See: "Militants Find Symbolic Targets in Uganda", Wall Street Journal, 13 July 2010. Available at: http://www.wsj.com/articles/SB10001424052748704288204575362400675683926

that the Bill had been in discussion since 2007[14].

17. RICA requires intelligence agencies and the Police to seek judicial authorisation for the interception of communications under Section 5. The law authorises officials to apply for a warrant that is issued by a designated judge to intercept specific communications. However, the threshold for issuance of a warrant to be established is very low given that law enforcement must only demonstrate "reasonable" ground for unspecified and broad threats to national security, national economic interests and public safety. As was noted with concern by the UN Special Rapporteur on promotion and protection of the right to freedom of opinion and expression (thereafter referred to as UNSR on freedom of expression) "In such instances, the burden of proof to establish the necessity for surveillance is extremely low, given the potential for surveillance to result in investigation, discrimination or violations of human rights."[15]

18. Under Section 7 evidence obtained by interception made in excess of a warrant issued under the Act remain admissible at the discretion of the court. To determine the admissibility of the evidence, the Court is required to consider the circumstances in which the evidence was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused that may be occasioned by its admission or exclusion.

19. Furthermore, the adoption of RICA failed to provide the necessary clarity on the legal framework for the interception of communication, as it does not replace the provisions contained in the Anti-Terrorism Act 2002.

20. The 2002 Act gives almost unfettered powers for state officials to conduct surveillance, without the need to obtain judicial authorisation.[16] The powers of surveillance awarded under the 2002 Act are broad. These include the interception of phone calls, emails or other communications, 'electronic surveillance', as well as monitoring of meetings, or doing "any other thing reasonably necessary" for the purpose of surveillance as noted in Section 19(5). The justifications of such surveillance are very broad, including safeguarding public interest, and protecting the national economy from terrorism as stated in Section 19(4).

21. In April 2015, the Parliament of Uganda adopted the Anti-Terrorism (Amendment) Bill, 2015[17], aimed at revising parts of the Anti-Terrorism Act of 2002 and was signed into law by the President on 19 June 2015[18]. Members of the Parliament who wrote a dissenting minority report[19] raised their concern that some amendments "have been included with the aim to prejudice rights and freedoms of citizens contrary to the established constitutional order."[20] Whilst the aim of the bill was to define 'terrorism' in order to comply with the International Convention on the suppression of terrorist financing, the amended Act provides a broad definition of terrorism whose vagueness is concerning. Furthermore, there were concerns over the weak provision which termed "causing serious damage to property" as a definition of terrorism arguing the damage

14 African Centre for Media Excellence, Parliament Passes Law to Intercept Communications Following Uganda Attacks, 23 July 2010. Available at: http://acme-ug.org/2010/07/23/parliament-passes-law-to-intercept-communications-following-uganda-attacks/
15 A/HRC/23/40, para. 56
16 Anti-Terrorism Act 2002, Part VII—Interception of Communications
17 Anti-Terrorism (Amendment) Act 2015. Available at: http://parliamentwatch.ug/wp-content/uploads/2015/06/The-Anti-Terrorism-Amendment-Bill-20151.pdf
18 Ibid
19 A Minority Report on the Anti-Terrorism Amendment Bill, 2015, June 2015. Available at: http://parliamentwatch.ug/wp-content/uploads/2015/06/DIA3-15-Report-on-the-Anti-terrorism-Amendment-Bill-2015-Including-Minority-Report1.pdf
20 Ibid, pp. 2

would have to be extensive.[21] Finally, they contested that "criminalizing 'any act prejudicial to national security or public safety' as a terrorist offence without qualifying national security and public safety is unconstitutional."[22] Such a provision would allow further crackdown on civil society, journalists and political dissidents in the name of "public interest".[23]

22. The addition of "interfering with an electronic system resulting in the disruption of provision of communication, financial, transport or other essential or emergency services" as terrorist office under Part III-Terrorism and Related Offences also raises concerns. 'Interfering with an electronic system', a practice also known as hacking, has been elevated to amounting to a terrorist offence, when it has up until now been categorized as a criminal offence. The vagueness of this provision and the failure to define "interfering with an electronic system" and "disruption" raises concerns that these would be subject to broad interpretation.

No clear oversight or transparency mechanisms

23. As noted by the UN Special Rapporteur on freedom of expression in 2013, the justification of national security "acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."[24] Without adequate transparency and oversight of the powers granted under those two Acts, the Ugandan intelligence and law enforcement agencies are failing to ensure that their policies and practices adhere to international human rights standards and adequately protect the rights to privacy and freedom of expression.

24. There is no clear oversight mechanism under RICA or the Anti-Terrorism (Amended) Ac. None of the intelligence agencies with the power to conduct surveillance under these acts are subject to independent oversight however they all report to the President. Any reporting that may be conduced by the agencies to the President is not made public.

Obligations on telecommunications and internet service providers to enable interception

25. In order to ensure that law enforcement and intelligence agencies are able to conduct communication surveillance, Section 8 of RICA requires that telecommunications and internet service providers ensure that their services are technologically capable of allowing lawful interception, and in such a way that the target of the interception remains unaware of it.

Decryption of communications

26. Section 10 of RICA regulates the possibility of decrypting encrypted communications. This Section requires that a person in possession of a key must use it to disclose the encrypted information upon request by the authorised person. Failure to comply is sanctioned with a fine or a prison sentence.

21 A Minority Report on the Anti-Terrorism Amendment Bill, 2015, June 2015. Available at: http://parliamentwatch.ug/wp-content/uploads/2015/06/DIA3-15-Report-on-the-Anti-terrorism-Amendment-Bill-2015-Including-Minority-Report1.pdf

22 A Minority Report on the Anti-Terrorism Amendment Bill, 2015, June 2015. Available at: http://parliamentwatch.ug/wp-content/uploads/2015/06/DIA3-15-Report-on-the-Anti-terrorism-Amendment-Bill-2015-Including-Minority-Report1.pdf

23 See: Ian, Tough Times Ahead; Anti-Terrorism Bill Passed, The Independent, 18 June 2015. Available at: http://www.independent.co.ug/ugandatalks/2015/06/tough-times-ahead-anti-terrorism-bill-passed/; Unwanted Witness, Crackdown on social media is a threat to digital rights and internet freedoms, 23 June 2015. Available at: https://unwantedwitnessuganda.wordpress.com/2015/06/23/crackdown-on-social-media-is-a-threat-to-digital-rights-and-internet-freedoms/

24 A/HRC/23/40, para 60

27. This section of the Act does not seem to fall within the warrant regime that the Act upholds for interception of communications. The power to request the decryption of communications falls solely on an authorized person, i.e. intelligence officials including the police (see Section 4), but this decision is not required to be authorised by a judge and is not bound under any oversight regime.

28. In the words of the UN Special Rapporteur on freedom of expression, decryption "orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation is not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight."[25]

Blanket retention of communications data

29. Section 11 of RICA requires service providers to retain metadata, although the terms and conditions of the retention are not specified in the Act. As is seen in many countries, metadata is often wrongly awarded a lower level of protection than the content itself of communications (i.e. text of email). The Special Rapporteur on freedom of expression has noted that analysis of metadata "can be both highly revelatory and invasive, particularly when data is combined and aggregated."[26]

30. However, RICA does not define the terms and conditions of the retention policy but merely instructs the Minister responsible for Information and Communications Technology to issue a Directive outlining how service providers how they must comply with Section 11.

31. In addition, Section 3 of RICA also provides for the establishment of a Monitoring Centre under the control of the Minister – the "sole facility through which authorised interceptions shall be effected". As of late 2015, the monitoring centre was not operational though seven international firms were invited to bid for the project.[27] It has been delayed in part because service providers have contested Government orders that they pay to connect to the future system, according to sources in the technology industry. RICA requires service providers to foot the bill of connecting to the new centre or otherwise complying with the Act, a considerable cost. Current data retention capacity of the main networks, including MTN Uganda is estimated at around 6 months' worth of call metadata.

No access to redress

32. RICA does not provide a right to seek redress for individuals who are the subject of a warrant for interception of communication. This is compounded by the fact that the Act fails to also provide a right to notification following an investigation to inform an individual that they had been subject to communication surveillance.

33. Instead, the restrictions on disclosure as outlined under Section 15 hinder any process

25 A/HRC/29/32, para 45
26 A/HRC/23/40, para 15
27 Privacy International, For God and My President: State Surveillance in Uganda, October 2015. Available at: https://www.privacyinternational.org/sites/default/files/Uganda_Report_1.pdf

of transparency, including from service providers by limiting their ability to publish statistics and other relevant information on the number and nature of communication interception requests received under the Act.

34. In the case of the Anti-Terrorism Act of 2002 and the Anti-Terrorism (Amendment) Act, given that no warrant is required and there may be no evidence it had been undertaken, the subject of the interception would have no means of finding out whether their communications have been intercepted, which further hinders their right to seek redress.

Internet shutdowns and other unlawful limitation to enjoyment of fundamental rights on-line

35. The Uganda Communications Act 2013[28] awards the Uganda Communications Commission (UCC) the power to "direct any operator to operate a network in a specified manner in order to alleviate the state of emergency", as defined by the Constitution, "during a state of emergency in the interest of public safety" under Section 86. But neither of those terms are defined in the Act, and in accordance with the Constitution, it is the President who declares a state of emergency.

36. In 2011, the UCC directed all service providers to temporarily block access to certain services which included Facebook and Twitter in fear of these social media networks being used to escalate opposition protests.[29] On 18 February 2016, the day of the Presidential elections, once again the UCC blocked access to social media networks, President Museveni stated that this was done to stop people "telling lies".[30] The social media networks were inaccessible for several days. Civil society in Uganda and across the world condemned this decision.[31]

Lack of autonomy and independent oversight of intelligence agencies

37. The oversight of lawful security acts should be a combination of: executive control; parliamentary oversight; judicial review and monitoring by expert bodies.[32] However in Uganda, the legislative framework is vague and ambiguous, and there is not oversight nor accountability mechanism of the intelligence agencies.[33] It is the President who holds the role of overseeing the mandate and operations of all of the intelligence agencies.

38. The power to gather intelligence and conduct surveillance are concentrated around various institutions: the Uganda People's Defence Force (UPDF) and the Uganda Police Force (UPF). The President exercises control over sensitive intelligence operations while day-to-day spying for intelligence gathering appears less centralised.

28 Communications Act, 2013. Available at: http://www.ucc.co.ug/files/downloads/UCC%20Act%202013.pdf
29 CIPESA, Privacy in Uganda - An Overview of How ICT Policies Infringe on Online Privacy and Data Protection, CIPESA ICT Policy Briefing Series No. 06/15 December 2015, pp. 5. Available at: http://www.cipesa.org/?wpfb_dl=201
30 BBC News, Uganda election: Facebook and WhatsApp blocked, 18 February 2016. Available at: http://www.bbc.co.uk/news/world-africa-35601220
31 See: Unwanted Witness, Press Release on UCCS illegal social media shutdown, 19 February 2016. Available at: https://unwantedwitness.or.ug/press-release-on-uccs-illegal-social-media-shutdown/ ; CIPESA & al, Joint Letter on Internet Shutdown in Uganda, 24 February 2016. Available at: http://www.cipesa.org/2016/02/joint-letter-on-internet-shutdown-in-uganda/
32 European Union Agency for Fundamental Rights (2015) Surveillance by Intelligence Services: Fundamental Rights and Remedies in the EU. Mapping Member States Legal Frameworks, pp. 29. Available at: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf
33 Agaba, A. (2009) Intelligence Sector Reform in Uganda: Dynamics, Aspects and Prospects, in 'Changing Intelligence Dynamics in Africa', eds. S. Africa and J. Kwadjo, GFN-SSR and ASSN, Birmingham, UK, pp. 41-60. Available at: http://epapers.bham.ac.uk/1526/1/AfricaKwadjo_-2009-_IntelligenceAfrica.pdf

39. The 1987 Security Organisations Act[34] established the Internal Security Organisation (ISO) and External Security Organisation (ESO). These two agencies are directed by Director Generals appointed by, and accountable to, the President, and exist to collect intelligence and provide advice on Uganda's security directly to the President.

Surveillance capabilities

40. Whilst the Ugandan government is unwilling to provide information on their surveillance programs, research published by Privacy International and other sources in the last few years has provided further information which has allowed the mapping of Uganda's surveillance capabilities.

41. Communications Monitoring Centre: RICA provides for the establishment of a Monitoring Centre. As of late 2015, the monitoring centre was not operational though seven international firms were invited to bid for the project.[35] These seven firms included: ZTE and Huawei (China), Verint Systems Ltd and NICE Systems (Israel), Macro System (Poland), RESI Group (Italy) and Gamma Group International (UK). The monitoring centre project has been delayed in part because telecommunication service providers have contested Government orders that they pay to connect to the future system, according to sources in the technology industry. NICE Systems is reported to have obtained the monitoring centre contract in November 2015.[36]

42. Forensic analysis: In recent years the security services have invested heavily in cyber defence. In 2013, a new forensic lab for the analysis of computer crime was opened in Kampala[37] and the UCC launched a Computer Emergency Response Team to investigate cybercrime.[38] Despite these developments, the Police's ability to actually conduct forensic analysis on devices and trace cybercrimes is rudimentary. The Police and investigating agencies often turn to private forensic companies to assist in complex investigations, according to an October 2015 investigation by Privacy International.[39]

43. Intrusion malware: In late 2011, officials of the Chieftaincy of Military Intelligence (CMI) and Uganda Police Force (UPF), acting on presidential orders, used an intrusion malware, short for malicious software, to infect the communications devices of key opposition leaders, media and establishment insiders. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili), according to documents acquired by Privacy International.[40] The tool chosen as the 'backbone' of the operation, FinFisher, is intrusion malware at the time manufactured by the Gamma Group of companies, headquartered in the UK.

34 1987 Security Organisations Act. Available at: http://www.ulii.org/ug/legislation/consolidated-act/305
35 Privacy International, For God and My President: State Surveillance in Uganda, October 2015. Available at: https://www.privacyinternational.org/sites/default/files/Uganda_Report_1.pdf
36 Africa Intelligence, Museveni commits $85.5 million to monitor the Web, 6 November 2015. Available at: http://www.africaintelligence.com/ION/politics-power/2015/11/06/museveni-commits-dollars85.5%C2%A0million-to-monitor-the-web,108110202-ART
37 Otage, S., Forensics lab for computer crime opened in Kampala, The Daily Monitor, 11 March 2013. Available at: http://www.monitor.co.ug/News/National/Forensics-lab-for-computer-crime-opened-in-Kampala/-/688334/1716526/-/1590cm1z/-/index.html
38 Mwesigwa, A., UCC launches response team to curb cyber crime, The Observer, 12 June 2013. Available at: http://www.observer.ug/business/38-business/25817-ucc-launches-response-team-to-curb-cyber-crime
39 Privacy International, Uganda's grand ambitions of secret surveillance, 15 October 2015. Available at: https://www.privacyinternational.org/node/656
40 Privacy International, For God and My President: State Surveillance in Uganda, October 2015. Available at: https://www.privacyinternational.org/sites/default/files/Uganda_Report_1.pdf

44. The Police also attempted to procure further technologies from intrusion malware supplier and rival to Gamma Group, Hacking Team, in mid-2015.[41] The local contact for the Hacking Team potential deal was Kin Kariisa, a business executive considered among Museveni's close contacts, according to documentation obtained by Privacy International. Kariisa was the President's special advisor on ICT from 2000 to 2009.

45. Media monitoring: In 2014, the UCC opened a media monitoring centre with "digital logger surveillance equipment",[42] though it appears to be targeted at recording and analysing public radio, television and print media rather than private communications. Police have also signed an accord with the UCC to cooperate more closely on the investigation of cybercrime.[43]

II. Lack of comprehensive data protection law

46. There is no specific law or regulation that regulates data protection in Uganda. However, in late 2014, Uganda's government through the National Information Technology Authority (NITA), the Ministry of Information Communication and Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MoJCA) issued a draft Data Protection and Privacy Bill for public comment.[44] The Bill is yet to be tabled before Parliament. It seeks to protect the privacy of the individual and personal data by regulating the collection and processing of personal information. It outlines the rights of individuals whose data is collected and the obligations of data collectors and data processors; and it regulates the use or disclosure of personal information.

47. During the consultation, Privacy International with Unwanted Witness and separately the Collaboration on International ICT Policy Centre for East and Southern Africa (CIPESA)[45] submitted comments on the draft bill.

48. Observations included the broad justifications for collecting personal data – namely "proper performance of a public duty by a public body" and "national security" – were overly broad and vulnerable to misinterpretation. There was a lack of clarity as to whether the Act would apply to public and private institutions. Moreover, the retention of data for national security purposes was concerning for the security and use of personal data because the term national security had not been defined.

49. Furthermore, further concerns related to poor provisions on consent, specific purpose, and quality of data, the transfer of data to third countries unless there are adequate laws in these third countries to protect this data. The lack of definition of the term "reasonably practicable" with reference to exemption from having to seek consent from the individual for collection of their data. As well as the lack of a provision establishing a data protection authority that is administratively and financially independent of any public authority and is given adequate resources to conduct its activities.

41 Privacy International, For God and My President: State Surveillance in Uganda, October 2015. Available at: https://www.privacyinternational.org/sites/default/files/Uganda_Report_1.pdf

42 Nakabugo, Z., Report facts only, Kayihura tells journalists, The Observer, 11 January 2015. Available at: http://www.observer.ug/index.php?option=com_content&view=article&id=35887:report-facts-only-kayihu-%20ra-tells-journalists&catid=34:news&Itemid=114

43 Unwanted Witness, Uganda Police signs a secret MOU with Uganda Communication Commission, 12 January 2015. Available at: https://unwantedwitness.or.ug/uganda-police-signs-a-secret-mou-with-uganda-communication-commission/

44 CIPESA, Reflections on Uganda's Draft Data Protection and Privacy Bill, 2014, 9 February 2015. Available at: http://www.cipesa.org/2015/02/reflections-on-ugandas-draft-data-protection-and-privacy-bill-2014/

45 CIPESA, Reflections on Uganda's Draft Data Protection and Privacy Bill, 2014, CIPESA ICT Policy Briefing Series, Available at: http://www.cipesa.org/?wpfb_dl=185

50. Since the open consultation, little progress has been made on the bill in 2015 but the Bill has now been gazetted and will be tabled in Parliament.[46]

51. Concerns around the lack of a data protection framework have been heightened in view of the deployment of data-driven and reliant initiatives including:

52. Identification and registration of subscribers: Compulsory SIM card registration and the retention of information about mobile phone users in a centralised database threaten the right to privacy in Uganda. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups.[47] It can have discriminatory effect by excluding users from accessing mobile networks. As was noted by the UN Special Rapporteur on freedom of expression in 2015, "compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest". The UN Special Rapporteur recommended that "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."[48]

53. In Uganda, these concerns compound due to the absence of data protection legislation to appropriately regulate the collection and processing of personal information including among government departments.

54. Registration of SIM cards has been mandatory in Uganda since March 2012, following a campaign of the Uganda Communications Commission, which cited the Regulation of Interception of Communications Act (2010) as justification for the exercise.[49] RICA under Section 9.2 requires that telecommunication service providers ensure that existing subscribers register their SIM-cards within the period of six months from the date of commencement of the Act. The UCC stated that SIM registration information would be kept confidentially by telecommunications operators in a secure data base.

55. UCC justified the initiative as necessary to "[h]elp law enforcement agencies to identify the mobile phone SIM card owners", "[t]rack criminals who use phones for illegal activities", "[c]urb other negative incidents such as; loss of phone through theft, nuisance/hate text messages, fraud, threats and inciting violence", and "[h]elp service providers (network operators) know their customers better."[50]

56. In 2015, the Ministry of Security reportedly ordered the UCC to verify information provided by telephone users in the SIM card registration exercise by matching data collected during the National Identity card registration exercise with that gathered in the SIM card registration exercise.[51]

57. The cut-off date for the exercise was March 2013. Nevertheless, as of 2016 it is still possible to buy a functional unregistered SIM card in Uganda.

46 CIPESA, CIPESA Convenes Journalists to Discuss Uganda's Data Protection Bill, 6 January 2016. Available at: http://www.cipesa.org/2016/01/cipesa-convenes-journalists-to-discuss-ugandas-data-protection-bill/
47 A/HRC/23/40, para 70; A/HRC/29/32, para 51
48 A/HRC/29/32, para 60
49 UCC, SIM Card Registration: Q&A, Available at: http://www.ucc.co.ug/data/smenu/23/SIM-Card-Registration.html
50 Ibid
51 Bambino, R., Government to synchronize both SIM card and National ID registration data, TechJaja, 13 February 2015. Available at: http://www.techjaja.com/government-to-synchronize-both-sim-card-and-national-id-registration-data/

58. CCTV: The Ugandan government has been investing more heavily in CCTV; the number of cameras in the capital Kampala appears to have increased over several years. In 2014, it was reported that a Chinese telecommunications technology company, Huawei, had donated a multi-tracking system worth US$ 750,000 to the Kampala Capital City Authority of the Ugandan government.[52] In February 2015, the Ugandan Parliament reportedly spent UGX 28 billion (over US$ 9.8 million) on CCTV cameras and other security measures provided by Chinese technology firm ZTE.[53]

59. Biometrics: As a means of combatting terrorism, fraud and securing its border management systems, Uganda has undertaken a process to procure biometric passports.[54] As well, in 2008 in order to tackle fraud and corruption, the government launched Uganda's Biometric and Smart Card Financial Card System.[55] Furthermore, for the 2016 Presidential elections, Uganda decided to make use of a biometric verification system at every polling station across the country.[56] The fingerprint scanners were provided by Suprema, Inc. and the delivery of the biometric verification system was made by Zetes,[57] raising concerns over the role of non-Ugandan third-parties in a process which results in the processing of a sensitive personal data of Ugandans. The biometric verification system was used but not at every polling station with some having to resort to printer paper registration documents. It was reported that this was due to human errors with wrong codes, staff unable to use the machines, and late arrival of the machines at some polling stations.[58]

III. Crackdown on civil Society

60. The Non-Governmental Organisation (NGO) Bill was adopted by Parliament on 26 November 2015[59] and was signed into law by the president on 30th January 2016[60]. It is now in force since 10th March 2016 as the NGO Act, 2016.

61. The Act retained provisions that are likely to limit civic space and were criticised for negatively impacting the ability of NGOs in Uganda to operate independently and free from government monitoring and interference.[61] Provisions include limiting activities of NGOs and their ability to express any criticism of the government. Furthermore, with the criminal penalties that the Act provides could result in the criminalisation of legitimate activities and behaviour that constitute the very mandate of civil society organisations.

52 Chimp Reports, Huawei Donates shs1.8bn Security Equipment to Uganda, 28 July 2014. Available at: http://www.chimpreports.com/huawei-donates-shs1-8bn-security-equipment-to-uganda/

53 Kahill, P., KCCA receives donated Multi Media Tracking System, 29 July 2014. Available at: http://news.ugo.co.ug/kcca-receives-donated-multi-media-tracking-system/

54 Mayhew, P., Biometric identification news from Uganda, Kenya and Nigeria, 6 November 2014. Available at: http://www.biometricupdate.com/201411/biometric-identification-news-from-uganda-kenya-and-nigeria

55 Uganda's Biometric and Smart Card Financial Card System, the 2013 AFI Global Policy Forum: Driving Policies for Optimal Impact. Available at: http://www.afi-global.org/sites/default/files/publications/01_2_can_biometrics_advance_financial_inclusion_uganda.pdf

56 Clottey, Uganda to Use Biometric Verification Machines for Elections, 15 January 2016. Available at: http://www.voanews.com/content/uganda-biometric-verification-machines-elections/3147994.html

57 Vrankulj, A., Suprema to supply biometric live scanners for 2016 Ugandan elections, Zetes to deliver, 23 April 2014. Available at: http://www.biometricupdate.com/201404/suprema-to-supply-biometric-live-scanners-for-2016-ugandan-elections-zetes-to-deliver

58 Reported by Rindai Chipfunde Vava, the director of the Zimbabwe Election Support Network (Zesn) and was an observer in the recently-held Ugandan elections. See: Biometric voter registration: Lessons from Ugandan polls, The Zimbabwe Independent, 8 March 2016. Available at: http://www.theindependent.co.zw/2016/03/04/zanu-pf-not-sincere-in-re-engaging-world-bank-imf/

59 ICNL, NGO Law Monitor: Uganda, 2 January 2016. Available at: http://www.icnl.org/research/monitor/uganda.html

60 Jjuuko, A., Museveni's assent to NGO Act will cost us all, The Observer, 26 February 2016. Available at: http://www.observer.ug/viewpoint/42802-museveni-s-assent-to-ngo-act-will-cost-us-all

61 Human Rights Watch, Uganda: Bill Threatens Rights, Independent Groups, 20 April 2015. Available at:https://www.hrw.org/news/2015/04/20/uganda-bill-threatens-rights-independent-groups

62. Specific concerns have been expressed by organisations working with marginalised groups particularly those working with lesbian, gay, bisexual, transgender and intersex (LGBTI), as well as sex workers. The most problematic sections retained in the Act are sections 44 (d) and (f) and section 30(1). According to these sections an organisation shall not engage in 'any act which is prejudicial to the security, laws and interest of Uganda and dignity of the people of Uganda'. Given the position of the Government on these issues, and the criminalisation of any person who "promotes homosexuality," under Section 13 of the Anti-Homosexuality Act, which may have been interpreted to include NGOs that advocate for gay rights, there are serious concerns that the work undertaken by these group may be interpreted as prejudicial to the security, dignity and interest of Uganda and may result into a justification for surveillance of the organisation under the provisions of the RICA.

63. This new law comes within a context in which in recent years have seen a worrying attempt from the Ugandan government to limit, regulate and monitor the activities of civil society.[62] In the last few years, NGOs have experienced break-ins and robberies of their offices. According to an umbrella body the NGO Forum over 15 offices of human rights organizations have been broken into under similar circumstances. They include: ACCU, FHRI, EHAHRDP, AGHA, HRNJ-Uganda, AFODE, among others.[63] The above constitute some of the factors for the shrinking civic political space, notwithstanding that political officers have continuously made re-assurances about the safety and security of NGOs in Uganda.[64]

Recommendations

64. We recommend that the government of Uganda:

- Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards including the principles of legality, proportionality and necessity; and take the necessary measure to ensure that all interception activities – including access to stored communications – are subject to prior judicial authorisation;

- Establish an independent and effective oversight mechanism (such as a Surveillance Commission) with a mandate to monitor all stages of interceptions of communications under the revised Regulation of Interception of Communications Act to ensure they are compliant with Uganda's domestic and international commitment to the right to privacy and other human rights;

- Reform Uganda's intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and

62 See: East and Horn of Africa Human Rights Defenders Project (EHAHRDP), Overview of the Human Rights Situation in the East and Horn of Africa April 2015- October 2015, Report submitted to the 57th Ordinary Session of the African Commission on Human and Peoples' Rights (ACHPR), Banjul, The Gambia, November 201. Available at: https://www.defenddefenders.org/wp-content/uploads/2015/11/ACHPR-57th-Session-report.pdf; CIPESA, How Recently Enacted Laws Undermine Ugandan Citizens' Rights, CIPESA ICT Policy Briefing Series April 2014. Available at: http://www.cipesa.org/?wpfb_dl=158; http://www.theguardian.com/law/2015/aug/26/ngos-face-restrictions-laws-human-rights-generation; Unwanted Witness, Shrinking Civic Political Space, 8 January 2016. Available at: https://unwantedwitness.or.ug/shrinking-civic-political-space-government-seeks-to-amend-the-anti-terrorism-act-to-target-civil-society-foreign-funding/

63 Human Rights Network of Journalist, Ugandan human rights office vandalised in latest crackdown on civil society, IFEX, 7 May 2014. Available at: https://www.ifex.org/uganda/2014/05/07/hrnj_uganda_alert_civil/

64 Uganda National NGO Forum, NGOs should not be threatened – Gen. Aronda assures NGO Leaders, 19 May 2014. Available at: http://ngoforum.or.ug/ngos-should-not-be-threatened-gen-aronda-assures-ngo-leaders-3/

operations in accordance with international human rights standards;

- Ensure that the Parliament conducts an inquiry into the use of intrusion software to assess their compliance with Uganda's domestic and international human rights obligations and make publicly available any findings related to the above inquiry;

- Halt all procurement of intrusion malware and other hacking tools pending the results of the Parliamentary inquiry and ensure there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses;

- Abolish mandatory SIM card registration and review the data retention requirements placed on telecommunications companies;

- Pass comprehensive data protection legislation that meets international standards and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress;

- Re-evaluate the use of biometric technologies in voting systems and biometric passports in order to ensure compliance with international human rights standards;

- Review the Non-Governmental Organisation (NGO) Act 2016 to ensure that it does not curtail the ability of NGOs to freely and securely conduct their mission and conduct their activities, and in particular provide definitions for "the security, laws and interest of Uganda" and "dignity of the people of Uganda".