PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 23rd Session, Myanmar

The Right to Privacy in Myanmar

Submitted by Privacy International

PRIVACY INTERNATIONAL

The Right to Privacy in Myanmar

Stakeholder Report
Universal Periodic Review
23rd Session - Myanmar

Submitted by Privacy International

March 2015

Introduction

1. This stakeholder report is a submission by Privacy International (PI).[1] 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 Myanmar before the Human Rights Council for consideration in Myanmar's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[2] 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. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals.[3]

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.[4]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[5] A number of international instruments enshrine data protection principles,[6] and many domestic legislatures have incorporated such principles into national law.[7]

---

1 For further information, please visit our website at: www.privacyinternational.org

2 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.

3 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

4 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.

5 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).

6 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)

7 As of December 2013, 101 countries had enacted data protection legislation: 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

Follow up to the previous UPR

6. There was no mention of the right to privacy and data protection either in the National Report submitted by Myanmar nor in the report of the Working Group. On the other hand, stakeholders raised widespread concerns regarding the right to freedom of expression and attacks against human rights defenders and journalists.[8] These were included in the recommendations made by the Working Group to Myanmar.[9]

Domestic laws related to privacy

7. The Constitution of the Republic of the Union of Myanmar under Section 357 reads: *"*

   The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution".

8. Article 17 of the Telecommunication Law No. 31 of Myanmar[10] requires Service Licensees to maintain securely the information and contents that are transmitted or received through its telecommunication services and confidential personal information of each individual user, and to not disclose and inform to irrelevant persons such information except where allowed in accordance with existing laws. Article 69 of the same law requires a court order for the disclosure of information kept in secured or encrypted systems, and any violation can result in a prison sentence for up to one year and/or a fine.

International obligations relating to privacy

9. Myanmar is a signatory to the Universal Declaration of Human Rights ('UDHR') but it has not ratified the International Covenant on Civil and Political Rights ('ICCPR'). 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"*.

Areas of concern

I. Failure to sign major international treaties

10. Myanmar has still not signed nor ratified many of the major international treaties, including the ICCPR, which upholds the right to privacy under Article 17.

---

8 Including Slovenia, France, Denmark, Germany, Canada, Sweden, Austria, Uruguay, Norway, the United Kingdom, and Italy.

9 A/HRC/17/9, Report of the Working Group on the Universal Periodic Review, Myanmar, 24 March 2011

10 The Telecommunication Law No. 31 of Myanmar was enacted on 8 October 2013. Available at: http://www.mcit.gov.mm/sites/default/files/Telecom%20Law%20English%20Version_0.pdf

11. In June 2013,[11] the National Human Rights Commissioner of Myanmar recommended that the government ratify the ICCPR and the International Covenant on Economic, Social and Cultural Rights ('ICESCR'). The Commission also called for the government to subsequently undertake legal reforms in order to align its national legislation with these treaties.

II. Communication surveillance

12. In the five decades of military dictatorship that Myanmar endured, state surveillance was part of a systematic policy to control citizens and monitor political dissent. Political reforms have been initiated since 2010, but since the political turmoil that occurred in Myanmar in 2013 as a result of religious unrest and legal reform pushed by the opposition, state surveillance has actually intensified.[12]

13. A recent report by the UN Special Rapporteur on the situation of human rights i n Myanmar, Yanghee Lee, which was presented at the 28th session of the Human Rights Council noted her concern about regular communications surveillance of human right defenders.[13] These reports complement the ones made in 2013.[14] when it was reported that journalist and academics had received Google notifications of state-sponsored attempts to infiltrate personal accounts on its e-mail service, Gmail.[15]

Lack of legal framework for lawful communication surveillance

14. Whilst the new telecommunication law adopted in 2013 requires a court order for the disclosure of information kept in secured or encrypted systems under Article 69, the government of Myanmar has yet to draft laws that govern the interception of communications by law enforcement. It has been reported that the government has requested support from the European Union to draft this implementation framework.[16]

---

11 Article 19, *Myanmar: National Human Rights Commission recommends ratifying key human rights treaties*, Press release, 21 June 2013. Available at: http://www.article19.org/resources.php/resource/37119/en/myanmar:-national-human-rights-commission-recommends-ratifying-key-human-rights-treaties

12 Freedom House, *Freedom on the Net 2014: Myanmar*. Available at: https://freedomhouse.org/sites/default/files/resources/Myanmar.pdf

13 A/HRC/28/72, para. 9, which reads as follows, *"Human rights defenders informed the Special Rapporteur of regular surveillance through phone calls, monitoring and inquiries of their movements and activities. She highlights the obligation of the Government to demonstrate the necessity and proportionality of such measures, including in relation to the right to privacy, and to establish judicial and parliamentary oversight over the executive's use of surveillance powers."*

14 Freedom House, *Freedom on the Net 2013: Burma.* Available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Burma.pdf, pp. 14

15 Fuller, T., *E-Mails of Reporters in Myanmar Are Hacked*, New York Times, 10 January 2013, Available at: http://www.nytimes.com/2013/02/11/world/asia/journalists-e-mail-accounts-targeted-in-myanmar.html?_r=3&; Crispin, S., *As Censorship Wanes, Cyberattacks Rise in Burma,* CPJ Internet Channel, 11 February 2013. Available at: http://www.cpj.org/internet/2013/02/as-censorship-wanes-cyberattacks-rise-in-burma.php.

16 Purdon, L., *Rights, safety at risk without lawful interception rules,* The Myanmar Times, 26 January 2015. Available at: http://www.mmtimes.com/index.php/opinion/12900-rights-safety-at-risk-without-lawful-interception-rules.html

15. This legal void is concerning given that government has expansive powers under Article 76 to *"*enter and inspect" telecommunication services" for the matters relating national defense and security or public interest" and under Article 77 to "intercept... when an emergency situation arises"*.*

16. It is urgent that Myanmar adopts a robust legal framework to govern lawful interception that upholds principles of legitimacy, proportionality and necessity to ensure that any interference with privacy is targeted and not arbitrary, as well as legislate for prior judicial authorisation, independent oversight, user notification, and access to remedy in case of violations.[17]

Access to communications data

17. Whilst Article 75 of the 2013 Telecommunication Law reads that, *"The Union Government may, as may be necessary, direct to the relevant organization for enabling to obtain any information and telecommunications which causes harm to national security and prevalence of law without affecting the fundamental rights of the citizens",* the law fails to include any privacy protections.[18] This provision is very broad and fails to specify which government agents have the authority to do this.

18. Article 77 of the 2013 Telecommunication Law says that:
    "The Ministry may, when an emergency situation arises to operate for public interest, direct the licensee to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments".

19. As noted by Human Rights Watch during the drafting phase of the law, the law fails to provide adequate guidance as to what constitutes *"national security"*, *"national defense"*, *"public interest"* or *"emergency situation"*.[19]

20. In 2011, it was reported[20] by Reporters without Border (RSF) that the Ministry of Communications, Posts and Telegraphs (MCPT) had issued new expansive rules for owners of public access centres (i.e. Internet cafes) to require them to keep and share with the authorities personal data such as name, National Registration Card number, passport number (if the user is a foreigner), contact address, and telephone number, as well as a log of the internet websites they visited. As noted by Frank LaRue, former UN Special Rapporteur on Freedom of Expression, *"Such laws are particularly problematic in countries where personal computer ownership is low and individuals rely heavily on publicly available computers".*[21]

---

17 See: https://necessaryandproportionate.org/

18 Freedom House, *Freedom on the Net 2014: Myanmar*. Available at: https://freedomhouse.org/sites/default/files/resources/Myanmar.pdf

19 Human Rights Watch (2013) *Reforming Telecommunications in Burma: Human Rights and Responsible Investment in Mobile and the Internet,* pp. 13. Available at: http://www.hrw.org/sites/default/files/reports/burma0512_ForUpload.pdf

20 Reporters Without Borders, *Surveillance of the media and the internet stepped up under new civilian president*, 17 May 2011. Available at: http://en.rsf.org/burma-surveillance-of-media-and-internet-17-05-2011,40296.html

21 A/HRC/23/40, para. 68

The private sector and human rights obligations

21. As noted in the UN Guiding Principles on Business and Human Rights, the private sector has a responsibility to respect human rights.[22]

22. With the ICT industry booming in Myanmar,[23] it is important for a robust legislative regime protecting the right to privacy and freedom of expression to accompany the development of the telecommunication infrastructure.[24] The legal void in which the industry is developing raises concerns that citizens may be exposed to increased government surveillance and control.[25]

23. Telecommunications company Telenor has said that it will not launch its services until the government had finalised its laws on communication interception.[26] Ooredoo, which launched its services in August 2014, has not announced how it will respond to government request for interferences with communications.[27]

24. 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"*.[28] 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.[29]

Surveillance and monitoring systems

25. In 2011, the Citizen Lab of the University of Toronto published research documenting[30] the use of Blue Coat Systems' commercial filtering products in

---

22 See: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

23 Igoe, M., I*s Myanmar ready for a telecommunication revolution?*, DevEx, 16 May 2014. Available at: *https://www.devex.com/news/is-myanmar-ready-for-a-telecommunications-revolution-83498*

24 Calderaro, A., *Digitalizing Myanmar: Connectivity Developments in Political Transition*, Internet Policy Observatory, pp. 3. Available at: http://www.global.asc.upenn.edu/app/uploads/2014/12/Digitalizing-Myanmar.pdf

25 Ibid, pp. 3

26 Telenor Group, *Telenor in Myanmar: Privacy & Freedom of Expression*. Available at: http://www.telenor.com/media/in-focus/telenor-in-myanmar/sustainable-business-in-myanmar/privacy-freedom-of-expression/

27 Purdon, L., *The Challenges and Opportunities of Myanmar's new ICT Networks*, Institute for Human Rights and Business, Commentary, 16 September 2014. Available at: http://www.ihrb.org/commentary/challenges-and-opportunities-myanmar-new-ict-networks.html

28 A/HRC/27/37, para. 42

29 Ibid, para. 43-45

30 The research findings were based on the following evidence, (i) ISP hostnames matching Blue Coat add-on names, (ii) network error pages found were generated by Blue Coat's ProxySG system, and (iii) strong correlation between Blue Coat's categorization of these URLs and those URLs found blocked by the researchers.

Myanmar.[31] Blue Coat[32] allows the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter, Google Mail, and Skype.[33] Given that Myanmar was subject to U.S. Sanctions,[34], it is concerning that as a US-based company, Blue Coat, were allowed to sell their products to the government.

26. There have also been reports of internet service providers ('ISPs') in Myanmar acquiring censorship equipment and hardware from the Chinese subsidiary of Alcatel-Lucent, a Franco-America company. Although the company denied this claim following a letter it received from RSF and Sherpa Association in March 2010, further investigation revealed that a spokesman for Hanthawaddy, a state-controlled ISP, confirmed in 2008 that the Alcatel's Chinese subsidiary did indeed provide a website filtering and surveillance system.[35]

27. Whilst such tools can be used for legitimate aims, such as controlling bandwidth costs, they also have the functionality to permit filtering, censorship, and surveillance, also given the poor human rights record of the government of Myanmar and the lack of legal framework in place to ensure the protection of the rights to privacy and freedom of expression of its citizens, the presence of such technologies is of extreme concern.

Lack of transparency of agencies conducting surveillance

28. In 2002, the intelligence apparatus of Myanmar was re-structured into the Office of Chief of Military Intelligence (OCMI). The National Intelligence Bureau (NIB), the Directorate of Defense Services Intelligence (DDSI), and the think tank Office of Strategic Studies (OSS) became sub-divisions of the OCMI. The NIB, which included the Bureau of Special Investigation (BSI) and Special Branch (SB) dealing with political, economic and criminal matters, was dismantled in 2004,[36] but it is unclear which agency took over its mandate. In the last decades, there have been numerous reports of corruption in the OCMI leading to power struggles internally but also with other agencies.[37]

29. There are various other agencies operating in Myanmar. To support its mission, the Burmese Police created the Special Branch and later a Criminal Investigation Branch. There is also the Myanmar Police Force which in 2004 was given further powers and increased responsibility for monitoring internal security issues.[38]

---

31 CitizenLab, *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*, 9 November 2011. Available at: https://citizenlab.org/2011/11/behind-blue-coat/

32 Blue Coat is a company specialised in online security but it is well know for having sold Deep Packet Inspection (DPI) technology based equipment to an array of countries. See: https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf

33 Blue Coat, *Applications that Blue Coat PacketShaper Classifies and Controls*. Available at: http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf

34 U.S. Department of the Treasury, Office of Foreign Assets Control, *Burma Sanction Program*. Available at: http://www.treasury.gov/resource-center/sanctions/Documents/burma.pdf

35 Reporters without Borders, *Internet Enemies: Burma,* 11 March 2011. Available at: http://en.rsf.org/burma-burma-11-03-2011,39754.html

36 Promulgation of Law Repealing National Intelligence Bureau Law and Dissolution of the National Intelligence Bureau, 22 October 2004. Available at: http://www.burmalibrary.org/docs15/2004-SPDC_Law2004-07-Law_Repealing_National_Intelligence_Bureau_Law-en.pdf

37 Bahroo, L., *A Family at War: Myanmar's Power Struggles and Purge*, Security Research Review, Volume 13. Available at: http://www.bharat-rakshak.com/SRR/Volume13/bahroo.html#9

38 Selth, A., *Burma's police forces: Continuities and contradictions*, Griffith Asia Institute, Regional Outlook Paper, No. 32, 2011, pp. 5. Available at: http://www.griffith.edu.au/__data/assets/pdf_file/0008/372761/Selth-

30. It is unclear under what legal regime these agencies are operating, with what remit and powers, and how their policies and practices adhere to international human rights obligations to protect the rights to privacy and freedom of expression. The various different agencies, their remit and operations must be reviewed to meet the international human rights standards, as articulated in the soft law instrument the International Principles on the Application of Human Rights to Communications Surveillance.[39] The State should be transparent about the use and scope of communications surveillance techniques and powers.

III. Lack of data protection framework

31. Myanmar does not have a law regulating the protection of personal data. A consumer protection law was reported to be in drafting and it was hoped to be published for comments in 2013, but this has not been the case.

32. As Myanmar continues with its efforts towards political and legal reforms as a democratic state of government accountable to the rule of law, it is essential that issues related to data protection be addressed. In addition, the lack of a data protection authority means there are limited or no opportunities for individuals to seek information on their right to privacy and the protection of their personal data, nor to seek redress, or compensation in case of a violation of these rights.

33. Current issues of concern in the area of data protection include:

- In 2013, the government announced that it would replace the paper National Registration card[40] with a smarter digital identification card to include biometric data.[41] Whilst it seems plans have been put on hold for such a change because of financial constraints, it is an issue that must be closely monitored as if digitised the data stored will have privacy implications which will need to be considered to ensure that the right to privacy of citizens and their personal data are protected.
- Whilst some ICT companies, such as Telenor, have developed and adopted their own data retention policies, the lack of national legislation regulating data retention, means that such internal policies may not be strong enough to protect the privacy of users and secure the freedom of services.[42]

Regional-Outlook-Paper-32.pdf

39 Launched in September 2013 following a year of consultation, the International Principles on the Application of Human Rights to Communications Surveillance a set of standards that interpret States' human rights obligations in light of new technologies and surveillance capabilities. The Principles are endorsed by 410 civil society organisations around the world, over 40 leading experts, academics and prominent individuals, as well as 4 elected officials. The Principles set for the first time an evaluative framework for assessing surveillance practices in the context of international human rights law. Please refer to the www.necessaryandproportionate.org website for further details.

40 The current card already includes he holder's photo, signature, a fingerprint of the left thumb and other personal data such as an ID number, the holder's date and place of birth, the holder's father's name, religion, height, blood type, and any obvious facial markings.

41 Kha, K., *Foreign Know-How Called Upon as Burma Gears Up for Smart ID Card Program,*, The Irrawaddy, 11 April 2013. Available at: http://www.irrawaddy.org/burma/foreign-know-how-called-upon-as-burma-gears-up-for-smart-id-card-program.html

42 Calderaro, A., *Digitalizing Myanmar: Connectivity Developments in Political Transition*, Internet Policy Observatory, pp. 10. Available at: http://www.global.asc.upenn.edu/app/uploads/2014/12/Digitalizing-Myanmar.pdf

Recommendations

34. We recommend that the government of Myanmar:

- Ratify the International Covenant on Civil and Political Rights and ensure relevant domestic legislation is adopted to domesticate the rights established by the Covenant;
- 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;
- Ensure there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses;
- Immediately enact data protection legislation that complies with international standards and establishes the creation of an independent data protection authority to monitor, investigate and sanction violations.