PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 24th Session, Singapore

The Right to Privacy in Singapore

Submitted by Privacy International

PRIVACY INTERNATIONAL

The Right to Privacy in Singapore

Stakeholder Report
Universal Periodic Review
24th Session - Singapore

Submitted by Privacy International
June 2015

Introduction

1. This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. PI wishes to bring concerns about the protection and promotion of the right to privacy in Singapore before the Human Rights Council for consideration in Singapore's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society.

4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

Follow up to the previous UPR

5. There was no mention of the right to privacy and data protection in the National Report submitted by Singapore nor in the final report of the Working Group.

6. However, a joint submission submitted by stakeholders raised concerns on the lack of protection of privacy laws, the extensive powers to law enforcement authorities to conduct searches on computers without judicial authorisation and raised raised concerns over the extensive unlawful practice of employers monitoring the phone calls, emails and internet usage of employees.[3]

7. Members States, including Slovenia, Czech Republic, Poland, Kazakstan, Lesotho, Finland, Jordan did however put forward recommendations for Singapore to consider the ratification of core international human rights treaties including the International Covenant on Civil and Political Rights (ICCPR).[4] Singapore accepted these recommendations, but it has yet to ratify the ICCPR.

Domestic laws related to privacy

---

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

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

3 A/HRC/WG.6?11SGP/3, para 26 and 27

4 A/HRC/18/11

8. The Constitution of the Republic of Singapore does not include a right to privacy.

9. Some laws regulate the processing of personal data,including in the public sector, such as the Computer Misuse and Cybersecurity Act which criminalises unauthorised access to data, but does not regulate or address lawful collection of data. Other safeguards for privacy and personal data are included in the Official Secrets Act, the Statistics Act, the Statutory Bodies and Government Companies (Protection of Secrecy) Act and the Electronic Transactions Act.

10. Other laws regulate data held by private sector entities including the Personal Data Protection Act, Banking Act, and the Telecommunications Act; whilst other relevant legislation include the law of confidence, which addresses misuse and publication of confidential information.

International obligations

11. Singapore has has not ratified the International Covenant on Civil and Political Rights ('ICCPR') which under 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".*

Areas of concern

I. Failure to ratify the ICCPR

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

13. 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".

14. The ICCPR has been ratified by 168 states, including many in Asia. It is urgent that Singapore ratifies and implements the ICCPR including by recognizing the right to privacy as a Constitutional right.

II. Communications surveillance

15. Despite some evidence from security researchers[5], details of the capacity of the Singaporean government to conduct surveillance and the scope of its surveillance infrastructure remains unknown. Yet, it is widely acknowledged that Singapore has a well-established, centrally controlled technological surveillance system designed to maintain social order and protect national interest and national security.[6]
16. The surveillance structure in Singapore spreads wide from CCTV, drones, internet monitoring, access to communications data, mandatory SIM card

[5] *See Section below on surveillance capabilities*
[6] Harris, S., *The Social Laboratory*, Foreign Policy, 29 July 2014. Available at: http://foreignpolicy.com/2014/07/29/the-social-laboratory/

registration, identification required for registration to certain website, to use of big data analytics for governance initiatives including traffic monitoring.[7]

17. This raises significant concerns in light of the fact that the legal framework regulating interception of communication falls short of applicable international human rights standards, and judicial authorisation is sidelined and democratic overnight inexistent.

Lawful interception

18. The law, through various pieces of legislation including the Criminal Procedure Code (amended in 2012) and the Computer Misuse and Cyber-security Act (amended in 1997), does not impose a need for prior judicial authorisation to conduct surveillance interception.

19. When authorisation is required, it can be given by the relevant Minister. For example, under Section 58 of Telecommunications Act, on grounds of public interest and national security, the Minister may give directions to the Authority (the Info-communications Development Authority of Singapore) or the licensee (telecommunication operator/provider) as necessary which may include: using and taking control of telecommunication system and equipment and stopping, delaying and censoring of messages as deemed necessary by the Minister.

20. And under Section 15A, Chapter 50A, of the amended Computer Misuse and Cybersecurity Act of 2013, the Minister for Home Affairs can authorize the collection of information from any computer, including in real time, when satisfied that it is necessary *"for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore".*

21. Furthermore Section 40 the Criminal Procedure Code[8] reads that, for the purposes of investigating an arrestable offence, the Public Prosecutor may authorise a police officer or an authorised person to exercise to decrypt communications required for the purposes of investigating the arrestable offence.[9]

22. It has been reported that the law enforcement agencies including the Internal Security Department and the Corrupt Practices Investigations Bureau, have extensive powers to conduct surveillance which are facilitate by highly "sophisticated" technological capabilities to monitor telephone, and other digital communications. These operations not do require prior judicial authorisation.[10]

23. The lack of a requirements for a judicial warrant for communications interception is concerning. Such authorisation must be delivered by judges, and not politicians. Ministerial authorisation must be removed and be

---

7 See: Harris, S., *The Social Laboratory*, Foreign Policy, 29 July 2014. Available at: http://foreignpolicy.com/2014/07/29/the-social-laboratory/; Lee, T., S*ingapore an advanced surveillance state, but citizens don't mind*, 26 November 2014. Available at:https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind/ *;* Cushing, T, *Singapore's Precarious Surveillance State The Envy Of US Intelligence Agencies*, TechDirt, 5 August 2014. Available at: https://www.techdirt.com/articles/20140730/13443428060/singapores-precarious-surveillance-state-envy-us-intelligence-agencies.shtml

8 Criminal Procedure Code. Available at: http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=DocId%3A3b4efefc-6d61-43ac-8b1c-8ccd8b86a972%20Depth%3A0%20Status%3Ainforce;rec=0;whole=yes#pr40-he-.

9 Under Article (2) (c) of Section 40, those who obstruct the lawful exercise y the police officer or an authorised person of the powers, are liable to fines up to SGP 10,000 (USD 8,000), jail terms up to three months, or both.

10 U.S. State Department, *2013 Human Rights Reports: Singapore,* 27 February 2014. Available at: http://www.state.gov/j/drl/rls/hrrpt/2013/eap/220229.htm

replaced with an independent judicial authorisation process in order to make the process more transparent and accountable.

24. Recent incidents of unwarranted access to communication data include:
    - 1999: SingTel was revealed to have scanned its customers' computers surreptitiously following orders it has received from the Ministry of Home Affairs;[11]
    - 2008: ISPs were forced to disclose the personal details of its subscribers it held in a lawsuit involving copyright infringement, i.e. case of Odex[12]

25. In 2013, when the amendments to the Computer Misuse Act were being discussed,[13] several members of Parliament raised the need to increase accountability and appropriate checks and balances in view of the "the enormous power and wide discretion the Bill confers on the Government to affect measures and to obtain data from private companies."[14] Yet unfortunately, none of these suggestions were taken on and were not included in the amended Act.

Limits on anonymity

26. On 1 November 2005, a pre-paid SIM card regulatory regime came into force. This emerged from a joint initiative by the Infocomm Development Authority (IDA), the Ministry Home Affairs together with mobile service providers.[15] In order to buy a SIM card, a new user must provide piece of identification.[16]

27. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups. 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.

28. As recently noted by the UN Special Rapporteur on Freedom of Expression, in a report presented at the 29th Session of the Human Rights Council, *"encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."* He added that because of their importance to these rights *"restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective."*[17]

---

11 Legard, D., ISP admits scanning its own subscribers, CNN, 6 May 1999. Available at: *http://edition.cnn.com/TECH/computing/9905/06/ispscan.idg/*

12 Odex Pte Ltd v Pacific Internet Ltd [2008] 3 SLR 18; [2008] SGHC 35. Available at: http://www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/free-law/high-court-judgments/13434-odex-pte-ltd-v-pacific-internet-ltd-2008-3-slr-18-2008-sghc-35

13 Lee, T., S*ingapore an advanced surveillance state, but citizens don't mind*, 26 November 2014. Available at: https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind/

14 See: Computer Misuse (Amendment) Bill, Sitting Data 14 January 2013, Available at: http://sprs.parl.gov.sg/search/topic.jsp?currentTopicID=00078404-WA&currentPubID=00078407-WA&topicKey=00078407-WA.00078404-WA_2%2Bid-2346c421-2c51-4106-afb9-0d02286db209%2B

15 Development Authority of Singapore, *Regulatory Controls on Prepaid SIM Cards from 1 Nov 2005 - Singapore Tightens Security Controls*, Press Release, 21 October 2005. Available at: https://www.ida.gov.sg/About-Us/Newsroom/Media-Releases/2005/20050705162915.
Note: This is the pink identity cards for Singaporeans, the blue identity card for permanent residents, work permit identification cards for work permit holders, SAF 11B, SPF11B or SDDF1182 National Servicemen or passports for all other foreigners.

16 See: SingTel, *Documents to bring when purchasing a hi! SIM Card*, Available at: http://info.singtel.com/personal/phones-plans/mobile/prepaid/support#documents-to-bring-when-purchasing-a-hi!card

17 A/HRC/29/32, para 56

The private sector and human rights obligations[18]

29. Online services and Internet Service Providers (ISPs) operate under the control and supervision of the government and other public entities,[19] which as noted above have broad powers to intercept, access communication data and take control and use telecommunication systems and equipment, amongst other.

30. ISPs and Internet Content Providers are obliged to comply with the Internet Code of Practice of Singapore under Section 1(1). The Code requires that all licensees "*use their best efforts to ensure that prohibited material is not broadcasted via the Internet to users in Singapore" under Section 2, and to "deny access to material considered by the Authority to be prohibited material if directed to do so by the Authority"* under Section 3(3)(4). The Code defines *"prohibited material"* is defined as *"material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws".*[20] Concerns have been previously raised by CSOs, including Human Rights Watch, that the government was using the Code to impose censorship and unlawful limitations on freedom of expression.[21]

31. As noted by the Navi Pillay, former UN High Commissioner for Human Rights, in her report on privacy in the digital age, 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.[22]

Expansive surveillance capabilities

32. In 2013, Citizen Lab of the University of Toronto found evidence that a product "PacketShaper", produced by BlueCoat[23] Systems, a US-based company, is in use in Singapore. [24] Blue Coat allows the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter, Google Mail, and Skype.[25]

33. Also in 2013, Citizen Lab found command and control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in a total of 25 countries, including Singapore.[26] FinSpy is malware – software programmes that give an operator the ability to observe and control an individual's computer or mobile device – produced by British-

---

18 As noted in the UN Guiding Principles on Business and Human Rights, the private sector has a responsibility to respect human rights. See: OHCHR (2011) *Guiding Principles on Business and Human Rights*, 2001, Available at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

19 Global Internet Liberty Campaign, Privacy and Human Rights: An International Survey of Privacy Laws and Practice. Available at: http://gilc.org/privacy/survey/intro.html

20 Media Development Authority, Internet Code of Practice. Available at: *http://www.mda.gov.sg/RegulationsAndLicensing/Licences/Documents/Properties/mobj.981.Internet_Code_of_Practice.pdf*

21 See: Human Rights Watch, Singapore: Space Narrows for Online News Media, 15 October 2014. Available at: http://www.hrw.org/news/2014/10/15/singapore-space-narrows-online-news-media; Global Voices, *Singapore Shuts Down News Website on World Press Freedom Day, 8 May 2015.* Available at: https://globalvoicesonline.org/2015/05/08/singapore-shuts-down-news-website-on-world-press-freedom-day/

22 A/HRC/27/37, para. 43-45

23 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: Citizen Lab, *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Research Brief, Number 13, January 2013. Available at: https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf

24 Citizen Lab, *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, 15 January 2013. Available at: *https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/*

25 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

26 Citizen Lab, *You Only Click Twice: FinFisher's Global Proliferation*, 13 March 2013. Available at: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

German company Gamma International. The news was covered by local media[27] but the Government denied using spy software.[28]

34. 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. Given the lack of legal framework in place to ensure the protection of the rights to privacy, the possible presence and use of such technologies is of extreme concern.

Wide powers of intelligence agencies

35. The Security and Intelligence Division (SID) operates under the Ministry of Defence and is responsible for gathering and analysing intelligence related to the country's external security. Very little information is publicly available on the function, operation but also the personnel of the SID. The SID has been reported as *"one of the best-kept secrets".*[29] It is unclear under what legal regime this agency is 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.

36. The Internal Security Division (ISD)[30] under the Home Ministry is the Singaporean domestic intelligence agency. The ISD is regulated by the Internal Security Act as well as the Criminal Procedure Code, the Official Secrets Act, and the Maintenance of Religious Harmony Act. The Internal Security Act offers a form of broad immunity: Section 8B(2)[31] notes that there shall be no judicial review in any court of any act done or decision made by the President or the Minister under the provisions of the Act except with regards to procedural requirements. Although, the Act does include under Section 13 that every order or direction made or given by the Minister under Section 8 and 10 to be reviewed by an advisory board at intervals of not more than 12 months, there is no judicial authorisation or oversight.

37. The various different agencies, their remit and operations, particularly the SID, must be reviewed to meet the international human rights standards, as articulated in the International Principles on the Application of Human Rights to Communications Surveillance.[32] The State should be transparent about the use and scope of communications surveillance techniques and powers.

Collaboration in mass communication surveillance programmes

38. In August 2013, documents published by NSA whistleblower Edward Snowden have revealed Singapore as a key "third party" providing direct and secret access to Malaysia's communication data with the Fives Eyes.[33] Whilst it remains unclear what the role and responsibilities are of 'third parties" to the

---

27 Han, K., *Online Spying in Singapore*, The Diplomat, 3 April 2013. Available at: http://thediplomat.com/2013/04/online-spying-in-singapore/

28 Tan. J., *S'pore govt denies using spy software*, Yahoo News, 15 March 2013. Available at: https://sg.news.yahoo.com/s%E2%80%99pore-among-25-govts-using-spy-software--researchers-084037882.html

29 Chuin Wei, Y., *Singapore's most secretive spy agency: The Security and intelligence divisions*, Straits Times, 19 May 2001. Published on All Singapore Stuff on 28 October 2014, Available at: http://www.allsingaporestuff.com/article/singapores-most-secretive-spy-agency-security-and-intelligence-division

30 See: Ministry of Home Affairs, ISD, *About ISD*. Available at: *https://www.mha.gov.sg/isd/pages/about-isd.aspx*

31 Internal Security Act. Available at: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A5ba26ddb-fd4c-4e2e-8071-478c08941758%20Depth%3A0%20Status%3Ainforce;rec=0;whole=yes#pr8B-he-.

32 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 www.necessaryandproportionate.org website for further details.

NSA, it has been reported that the government of Singapore, through state-owned operator, SingTel facilitated access to fibre optic cables passing through its territory.[34]

39. This access was provided through the tapping of some internet cables running through Singapore.[35] Internet monitoring is the act of capturing data as it travels across the internet towards its intended destination. [36]It can take place across any point of the infrastructure, depending on what information is trying to be collected.

40. Privacy International is concerned that such mass surveillance programmes are contrary to Article 12 of the UDHR and Article 17 of the ICCPR. The alleged role of Singapore as a third party to the Five Eyes extends far beyond principles of legality, legitimacy, proportionality, and necessity that must considered when interfering with and limiting the right to privacy. Such activities also fail to meet well-established human rights principles of transparency, accountability, due process, and the requirement independent oversight.

III. Data protection

41. In 2012, Singapore's Parliament approved a data protection law which took effect on 2 January 2013. The Personal Data Protection Act 2012 (PDPA) establishes a regulatory framework which governs the collection, use, disclosure and care of personal data.[37] The PDPA mandated the establishment of a Data Protection Commission under Section 5.

42. The PDPA is a welcomed step in ensuring the right of individuals to protect their personal data but the scope, some of the principles, and numerous exemptions raise concerns.[38]

43. The PDPA does not apply to the police as well as any public agency or organisation. These exemptions are concerning when considering initiatives such as the one announced in January 2015 by the Neighbourhood Police Centre (NPC) raise serious concerns as to what privacy safeguards will be applied. The NPC announced it would begin trials of body-word cameras for police forces. The cameras will be kept on record mode during the entirety of an officer's shift, with the possibly of being turned off when judged necessary by the officer.[39]

44. Other exemptions provisions of concern include the exemption of 'business contact information', a broad list of uses for an 'evaluative purpose' which will exempt personal data linked to employment, education, etc.,. Furthermore,

---

[33] Lee, T., S*ingapore an advanced surveillance state, but citizens don't mind*, 26 November 2014. Available at: https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind/. For information on the Five Eyes, please visit: https://www.privacyinternational.org/?q=node/51

[34] http://news.asiaone.com/news/singapore/spying-spotlight-now-singapore?page=0%2C0

[35] These included the SEA-ME-WE-3 internet cable, which is runs from Japan passing through Singapore, Djibouti, Suez and the Straits of Gibraltar all the way to Northern Germany, and the SEA-ME-WE-4, from Singapore to Southern France. See: Dorpling, P., *Singapore, South Korea revealed as Five Eyes spying partners*, The Sidney Morning Herald, 25 November 2013. Available at: http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html

[36] See: Privacy International. Privacy 101: Internet Monitoring. Available at: https://www.privacyinternational.org/?q=node/12

[37] See: Personal Data Protection Commission, *Legislation and Guidelines: Overview.* Available at: https://www.pdpc.gov.sg/legislation-and-guidelines/overview

[38] Greenleaf, G., *Singapore's Personal Data Protection Act 2012: Scope and principles*, Privacy Laws & Business International Report, Issue 120, December 2012, pgs 1, 5-7. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2212608

[39] Lim, J., *"Police to start wearing body cameras from Friday"*, The Straits Times, 29 January 2015. Available at: http://www.straitstimes.com/news/singapore/courts-crime/story/police-start-wearing-body-cameras-friday-20150129

unless expressly provided in the Act, provisions of other 'written laws' will supersede the PDAC if these provisions are inconsistent with any parts of the Act under Section III to VI, news organisations collecting for news activities (both undefined) do no require consents, data intermediaries are exempt but controllers are liable.

45. The broad scope of exemptions allow for collecting of personal data without consent are further extended by regulations or Ministerial decisions.

46. Finally, the Act fails to provide specific protection for sensitive personal data, which is commonly defined as data consisting of information to a person's race or ethnicity, politics, health, religion, sexual life, and criminal record. Such data requires additional protection and thus should only be held and used where strictly necessary.

Recommendations

47. We recommend that the government of Singapore:

- 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;
- Make clear the basis and limits of any intelligence sharing arrangements their intelligence agencies have with foreign intelligence agencies in order to ensure that intelligence sharing arrangements are in accordance with the law by providing to Singaporean citizen's with a clear understanding of the legal nature of the relationships;
- Ensure there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses;
- Review the data protection legislation to bring it into line with international and regional standards;
- Investigate and take necessary measures to address security breaches of personal data which directly threaten the right to privacy of its citizens, and ensure those those responsible are sanctioned and case of recognised violations, victims have access to redress.