The Right to Privacy in the Indonesia

Stakeholder Report

Universal Periodic Review

27th Session – Indonesia

Submitted by the Institute for Policy Research and Advocacy (ELSAM) and Privacy International

September 2016

Introduction

1. This stakeholder report is a submission by Privacy International (PI) and the Institute for Policy Research and Advocacy (ELSAM). PI is a human rights organisation that works to advance and promote the right to privacy around the world. ELSAM is an Indonesian human rights group formed to actively participate in the efforts to develop, promote and protect civil and political rights and other human rights in Indonesia.

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

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

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

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.[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

6. There was no explicit mention of the right to privacy in the National Report submitted by Indonesia in 2012, nor in the stakeholder submissions and the issue was not addressed in the report of the Working Group following the consideration of the state report in 2012.[6] Since then a number of concerns relating to the right to privacy have arisen in Indonesia, making the issue to be considered particularly important.

7. Various recommendations[7] were submitted on related topics developed in this report which enjoyed the support of the government including to:

   108.30 Pursue the revision of the Penal Code to provide a more comprehensive and thorough legal basis for the implementation of Indonesia's international obligations.
   108.31 To adopt promptly the reforms of the Criminal Code.
   108.34 Continue its efforts to promote and support national human rights institutions
   108.35 Continue developing the institutional framework with respect to the promotion and protection of human rights
   108.49 Strengthen its efforts and measures to consolidate the State of law and its mechanisms on human rights protection and promotion, as stated in the recently launched Third National Action Plan on Human Rights
   108.104 *Revise any national legislation that may be in conflict with international obligations*

Indonesian domestic law related to privacy

8. Indonesia's 1945 Constitution does not explicitly mention privacy. However, Article 28G (1) protects the right to dignity and "to feel secure", concepts that are often related to the right to privacy:

   (1) Every person shall have the right to protection his / herself, family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right."[8]

9. The Constitutional Court decision in Judgement No. 5/PUU-VII/2010 affirmed the recognition of the right to privacy in Indonesia under Article 28(G). It also recognised the importance of restricting communications surveillance powers to prevent misuse and ultimately the violation of the right to privacy.[9]

10. "Law no. 39 of 1999 on Human Rights" contains in Article 32 the same language as Article 12 in the UDHR enshrining the right to privacy and contains an acknowledgement in Article 2 that human rights are "...an integral part of humans, which must be protected, respected, and upheld in the interests of promoting human dignity, prosperity, contentment, intellectual capacity and justice."

Indonesia's international obligations and commitments

11. Indonesia acceded to the International Covenant on Civil and Political Rights ('ICCPR') in 2006. Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that *"no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation"*. The Human Rights Committee has noted that state parties to the ICCPR have a positive obligation to *"adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."*[10]

12. Indonesia is also a signatory to the Association of South East Asian Nations (ASEAN) Human Rights Declaration. Article 10 affirms all civil and political rights in the UDHR and Article 21 closely resembles the language on the right to privacy found in the UDHR.

Areas of concern

I. Communications surveillance

13. A 2015 poll revealed that Indonesians consider technology to have had a mostly negative impact on privacy rights and think there is a lack of sufficient legal safeguards in the country to protect privacy.[11]

14. Indonesia has seen both high-level surveillance scandals with the government as both victim and perpetrator, and widespread reports of surveillance against activists, journalists and other public figures.

15. In 2011, Human Rights Watch revealed systematic surveillance of activists and journalists in West Papua, a highly militarised region of the country that has witnessed significant separatist activities.[12] According to leaked documents, Indonesia's Special Forces unit 'Kopassus' had been illegally surveilling "a broad swathe of Papuan political, traditional, and religious leaders, and civil society groups." Kopassus has also been accused of torture and other grave crimes.

16. Activists and journalists routinely allege covert physical and communications surveillance.[13]

Absence of communications surveillance legislation

17. Article 31(4) of Law No. 11 of 2008 on Electronic Information and Transactions (EIT) establishes that provisions on procedures for lawful interceptions of communications shall be regulated by government regulation.[14]

18. The decision by the Constitutional Court in Judgement No. 5/PUU-VII/2010 stated that there is a necessity for comprehensive and appropriate regulations to control interception powers. It found article 31(4) of the EIT insufficient to achieve this aim in that the need for effective controls on communications surveillance required control at the level of regulatory law, not by government regulation which 31(4) provided for. The decision also made a pointed criticism of the regulation of communications surveillance.[15] At the time, it existed solely upon the policies of each state agencies involved, adding further to the need for comprehensive communications surveillance legislation that would standardize the powers and limitations of those powers across these different agencies mandated to conduct surveillance.

19. Yet no further legislation has been adopted. In December 2014[16] a list of legislative priorities was released by the newly elected government which included a reference to a Draft Bill on interception procedure though no bill came within the legislative session.

20. The decision made evident that it is necessary to amend the current practice of dispersing communications surveillance powers across a number of different laws and instead to synchronise in one integrated regulation. While the decision called for regulation, it should be used as a catalyst to go further and have robust legislation passed on communications surveillance with public debate and scrutiny of the proposed legislation.

21. This would be in line with the recommendations contained in the United Nations General Assembly Resolution 68/167 on the right to privacy in the digital age, which calls upon states *"To respect and protect the right to privacy, including in the context of digital communication"* and *"To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law."*

Lack of independent oversight of intelligence agencies

22. The Indonesian government's intelligence functions are spread across various agencies, each of which has some capacity for communications surveillance. These include:
    - The Strategic Intelligence Agency ('Badan Intelijen Strategis', BAIS). It is under the command of the Indonesia National Armed Forces Headquarters which has the President as the Commander-in-Chief;

- The State Intelligence agency ('Badan Intelijen Negara', BIN): formerly BAKIN, BIN is responsible both for coordinating information sharing and operations between other intelligence agencies, and is directly answerable to the President;[17]
- The "National Crypto Agency" (Lembaga Sandi Negara): a government agency engaged in the security of state secret information, and in gathering signals intelligence. Its operations and structure are mandated by Presidential decree.[18]

23. These three agencies are under the direct authority of the President, and there exists no independent authority to review the operations of these agencies. In the current legal framework, these intelligence agencies are not being suitably held to account for their policies and practices to adhere to international human rights and adequately protect rights found in the constitution of Indonesia.

Purchase of communications surveillance technologies from surveillance companies

24. The publication by the United Kingdom's Department of Business, Innovation and Skills of export data between February 2015 and April 2016 showed that Indonesia had imported IMSI Grabber technology from companies from the United Kingdom (UK).[19] "IMSI Catchers" are devices that mimic the operation of a cell tower device in order to entice a users' mobile phone to surrender personally identificable data such as the SIM card number (IMSI). In recent years, "IMSI catchers" have become far more sophisticated and can perform interception of voice, SMS and data. They are also able to operate in a passive mode that is virtually undetectable as it does not transmit any data. In its concluding observations on the Republic of Korea, the Committee expressed its concerns about "the operation and insufficient regulation in practice of so called 'base-station'".

25. This is not the first time Indonesia have been involved in the importation of mobile phone surveillance technology. In response to a Freedom of Information request by Privacy International, Swiss authorities revealed that companies in Switzerland had received a license to export technology, most likely an IMSI catcher, to Indonesia.

26. This adds to previous purchases of surveillance technology by Indonesia. In 2013, UK-based surveillance company Gamma TSE sold the Indonesian military US$6.7 million worth of unspecified "wiretapping" equipment as part of the military's weapons modernization effort.[20]

27. These purchases by Indonesia have been carried out without a comprehensive communications surveillance law in place which reflects international human rights standards and provides sufficient regulation limiting the scope for abuse and arbitrary interference with the right to privacy.

Mandatory SIM registration

28. In August 2014, it became mandatory for all prepay SIM card users to register their personal information with mobile operators.[21]

29. Existing prepay mobile customers were given a six-month period to register their mobile line at their operator's outlets, according to the industry regulator.

30. Mandatory sim registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalized groups. As was noted by the 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."[22]

Lack of investigation into reports of unlawful foreign government surveillance

31. In February 2014, The New York Times reported that Australia's signals intelligence agency, DSD, infiltrated an Indonesian mobile phone company and stole nearly 1.8 million encryption keys used to protect communications.[23]

32. In 2015, documents released by Edward Snowden dating from 2009 revealed that New Zealand's Government Communications Security Bureau (GCSB) had been spying on communications of neighboring countries, including Indonesia.[24]Despite these reports of grave and widespread violations of individual's privacy, there has been no independent investigations by Indonesian authorities.

II. Data protection.

33. Indonesia lacks a comprehensive framework for the protection of personal data. At the moment there are at least 30 different laws in Indonesia that relate to data privacy.[25] These stretch from the powers of the Anti-Corruption Commission Law (KPK) to the protection of data of medical personnel. In the absence of overarching protections, the scattered nature of privacy provisions means legislation in some cases overlap while leaving gaps in other areas. For example, the Population Administration Law and the Archival Law are two separate pieces of legislation detailing protection and procedures for archiving and political administration yet there is no recognition of personal data under the Anti-Terror Law, or the State Intelligence Law.

34. A draft regulation, the Bill on Personal Data was circulated in 2015 and consultations closed on 31 July 2015.[26] Since 2015, no further action has been taken by the Indonesian government.

35. Article 17 paragraph (2) of the ICCPR states that everyone as the right to the protection of the law against arbitrary or unlawful interference or attacks. The concept of "protection of the law" must be given directly through effective procedures and adequate institutional resources. Over 100 countries around the world have enacted comprehensive data protection legislation and several other countries are in the process of passing such laws.[27]

36. The practice in a number of countries shows that specialized, independent regulatory agencies are established for the management of personal data by third parties. The absence of a comprehensive law on data protection means there is no data protection authority to receive complaints regarding the misuse of personal data

37. With a growing number of Indonesians accessing the internet, 72 million active social media accounts and 308.2 million mobile connections[28], it is of great importance that data protection regulation reflect and respond to maintain the trust and security of Indonesian users.

38. A survey from 2015 conducted by Microsoft which included, among other countries, Indonesian respondents found that most internet users think personal technology has had a negative impact on privacy. 30% of Indonesian internet users felt this way.[29]

39. Indonesia has been increasing its data driven initiatives such as biometrics-based ID card e-KPT[30] which requires a photograph, a digital signature, ten fingerprints, iris images and biographical information, including religion. In December 2014, the government announced that Jakarta will invest $2.4 million called Smart City Jakarta. The government plans to integrate government units – transport, public utilities, health, sanitation, tax and local government – to the operation centre.

40. With an increasing emphasis on data driven initiatives it is important to see a recognition of the need for up to date and comprehensive data protection to maintain the protection of Indonesian's right to privacy and also see the benefits of these new initiatives.

Recommendations

41. We recommend the government of the Republic of Indonesia:

    1. Ensure a comprehensive data protection law is passed, with policies and practices that adhere to international human rights law and standards;

    2. Ensure that its communications surveillance laws, policies and practices adhere to international human rights law and standards including the principles of legality, proportionality and necessity;

    3. Provide effective and independent oversight of surveillance by intelligence and law enforcement agencies ensuring adherence to international human rights laws and standards;

    4. Provide effective oversight over the data handling practices of private entities and provide to citizens an individual complaints mechanism to log complaints of misuse;

    5. Undertake a review of domestic legislation and improve protections of the right to privacy found in the legislation in line with international human rights standards.

[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] 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] A/HRC/21/7 Report of the Working Group on the Universal Periodic Review, Indonesia, 5 July 2012

[7] *ibid,* at para 108, pg. 14.

[8] The 1945 Constitution of the Republic of Indonesia (unofficial translation). Available at: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_174556.pdf

[9] Judgement No. 5/PUU-VII/2010. Available at: http://hukum.unsrat.ac.id/mk/mk-5-puu-viii-2010.pdf

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

[11] Penn, M., *Views from around the globe: 2nd Annual Report on How Personal Technology is Changing our Lives*, Microsoft blog, 19 January 2015. Available at: http://blogs.microsoft.com/blog/2015/01/19/views-around-globe-2nd-annual-report-personal-technology-changing-lives/

[12] Human Rights Watch, *Indonesia: Military Documents Reveal Unlawful Spying in Papua: End Monitoring of Civil Society, Uphold Free Expression*, Human Rights Watch blog, 14 August 2011. Available at: https://www.hrw.org/news/2011/08/14/indonesia-military-documents-reveal-unlawful-spying-papua

[13] *Taming the untameable: Indonesia's effort to control the growing tide of digital communications*, published in in 'Global Information Society Watch 2014: Communications surveillance in the digital age', published by Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Available at: https://giswatch.org/en/country-report/communications-surveillance/indonesia

[14] Law No. 11 of 2008 Electronic Information and Transactions, pg. 26. Available at: https://www.bu.edu/bucflp/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf,

[15] See footnote 8 at 3.21.

[16] Institute for Criminal Justice Reform, *ICJR calls for more Progressive Regulatory Plan and Urges the GoI to Settle Outstanding Liabilities on Criminal Regulations*, 17 December 2014, http://icjr.or.id/icjr-calls-for-more-progressive-regulatory-plan-and-urges-the-goi-to-settle-outstanding-liabilities-on-criminal-regulations/

[17] See: Ingo, W. *Indonesia's new Intelligence Agency How?, Why?, and What for?* Watch Indonesia, 1 November 2000. Available at: http://www.watchindonesia.org/11776/indonesias-new-intelligence-agency-how-why-and-what-for?lang=en

[18] See: http://www.lemsaneg.go.id/

[19] Cox, J., *British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes*, Motherboard, 26 August 2016, http://motherboard.vice.com/read/the-uk-companies-exporting-interception-tech-around-the-world. Database can be found here: https://docs.google.com/spreadsheets/d/11_TtwzbRIP9QD_aKA6ej8REFwVsS-hmB91WCTAYfP9g/edit.

[20] Vit, J., *TNI Surveillance Purchase Triggers Concern in Indonesia*, Jakarta Globe, 25 September 2013, http://jakartaglobe.beritasatu.com/news/tni-surveillance-purchase-triggers-concern-in-indonesia/

[21] Telecompaper, *Indonesia prepay SIM registration mandatory starting August*, 17 July 2014. Available at: http://www.telecompaper.com/news/indonesia-prepay-sim-registration-mandatory-starting-august--1026014

[22] A/HRC/29/32, para 60.
[23] Risen, J., and Poitras, L., *Spying by N.S.A. Ally Entangled U.S. Law Firm*, New York Times, 15 February 2014, http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html
[24] Reuters, *New Zealand spying on Pacific neighbors and Indonesia: Snowden documents*, 4 March 2015. http://www.reuters.com/article/us-newzealand-spying-pacific-idUSKBN0M104R20150305#KhTB6jJyG2TPpvcu.97
[25] Please see Annex A.
[26] Lee. R., *Indonesia data privacy regulation is on its way*, Simmons & Simmons elexica, 31 July 2015. Available at: http://www.elexica.com/en/legal-topics/data-protection-and-privacy/31-indonesia-data-privacy-regulation-is-on-its-way
[27] Banisar, D., *National Comprehensive Data Protection / Privacy Laws and Bills 2016 Map*, Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416
[28] Lukman, E., *The latest numbers on web, mobile, and social media in Indonesia*, Tech In Asia, 21 January 2015. Available at: https://www.techinasia.com/indonesia-web-mobile-data-start-2015
[29] Penn, M., *Views from around the globe: 2nd Annual Report on How Personal Technology is Changing our Lives*, Microsoft presentation in Davos, Switzerland, 19 January 2015, pg. 25. Available at: http://mscorpmedia.azureedge.net/mscorpmedia/2015/01/2015DavosPollFINAL.pdf
[30] Planet Biometrics, *Indonesia ID project makes stunning progress*, 19 September 2012. Available at: http://www.planetbiometrics.com/article-details/i/1261/