The Right to Privacy

Stakeholder Report
Universal Periodic
25th Session – Kingdom of Thailand

Submitted by The Thai Netizen Network and Privacy International
September 2015

I. Introduction

1. This stakeholder report is a submission by Privacy International (PI) and Thai Netizen Network (TNN). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. TNN is a Bangkok-based organisation that works to promote human rights in Internet policy and support the work of human rights defenders in digital environment.

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

II. The right to privacy

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

4. 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.[1]

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.

6. 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.[2] A number of international instruments enshrine data protection principles,[3] and many domestic legislatures have incorporated such principles into national law.[4]

1 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

2 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).

3 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)

4 As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

III. Follow up to the previous UPR

7. There was no mention of the right to privacy, surveillance and data protection in the National Report submitted by Thailand.[5]

8. Issues raised on the right to privacy by stakeholders where in relation to the rights of child victims, and early marriage of girls.[6]

9. There were many recommendations by Members States on the need to ensure that legislation was consistent with international human rights law, particularly in relation to the Internal Security Act, the Computer Crimes Act, the Emergency Decree, the Official Information Act, and lèse-majesté provisions.[7] Some of those recommendations were accepted and others simply noted but many calling for legal reform were rejected.

IV. Domestic laws related to privacy protection

10. The previous Constitutions of Kingdom of Thailand included a right to privacy as a human right. B.E. 2540 (1997) and B.E. 2550 (2007) Constitution Article 35 used the same phrase;

> *"A person's family rights, dignity, reputation or the right of privacy shall be protected. The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public".*[8]

11. Following a military coup on 22 May 2014, all but a few provisions of the 2007 Constitution were suspended. An interim Constitution was promulgated on 22 July 2014.[9] The Interim Constitution does not explicitly uphold the right to privacy and the only provision on the protection and promotion of fundamental rights and freedoms reads as follow:

> *"Section 4. Subject to the provisions of this Constitution, all human dignity, rights, liberties and equality of the people protected by the constitutional convention under a democratic regime of government with the King as the Head of State, and by international obligations bound by Thailand, shall be protected and upheld by this Constitution."*

12. The Official Information Act B.E. 2540 (1997) protect personal information by providing exceptions (Chapter III) to to the principle of transparency in disclosure of official documents. It obligates public sector to protect the data systems and allows

5 A/HRC/WG.6/12/THA/1
6 A/HRC/WG.6/12/THA/3, para 40
7 A/HRC/19/8
8 The right to privacy was also mentioned in older constitutions, for example in the B.E. 2534 Constitution. It is also inserted in recently-dismissed B.E. 2558 Draft Constitution. Available in Thai at: http://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/download/article/article_20150429103838.pdf.
9 Constitution of the Kingdom of Thailand (Interim), B.E. 2557 (2014). Unofficial translation available at: http://lawdrafter.blogspot.co.uk/2014/07/translation-of-constitution-of-kingdom.html

individual to correct personal data maintained by government.[10] The Policy and Guidelines for Protection of Personal Information in Public Sectors B.E. 2553 (2010)[11] (combined as one document) regulate the management of personal information used or kept in public sector in electronic form which is not explicitly covered by the Official Information Act.

13. Other sectoral laws regulate personal data held by private sector, such as the Credit Information Business Act of B.E.2545 (2002) (amended in 2551) (2008),[12] Electronic Transaction Act B.E. 2544 (2011),[13] Royal Decree Prescribing the Security Procedure Presumed as a Reliable Method for Electronic Transaction of B.E. 2553 (2010)[14] enacting the provisions of Electronic Transaction Acts, Section 7 of National Health Act protects personal health information,[15] some other sets of standards has been announced by ETDA[16] and National Broadcasting and Telecommunication Commission (NBTC).[17]

V. International obligations and commitments

14. Thailand ratified[18] the International Covenant on Civil and Political Rights ('ICCPR') without any reservation on Articles 17 or Article 19, on the right to privacy and freedom of expression respectively.[19] 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 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]."*[20]

10 Official Information Act B.E. 2540, unofficial English translation available at http://www.oic.go.th/content/act/act2540eng.pdf.
11 Policy and Guidelines for Protection of Personal Information in Public Sectors B.E. 2553. Available in Thai at: https://www.etda.or.th/files/1/files/12.pdf
12 Credit Information Business Act of B.E.2545 (amended in 2551). Unofficial English translation available at: http://www.creditinfocommittee.or.th/download/creditinfo_act-engv3.pdf
13 Electronic Transaction Act B.E. 2544. Unofficial translated version available at: https://www.bot.or.th/English/PaymentSystems/OversightOfEmoney/RelatedLaw/Documents/et_act_2544_Eng.pdf
14 Royal Decree Prescribing the Security Procedure Presumed as a Reliable Method for Electronic Transaction of B.E. 2553. Available in Thai at: https://www.bot.or.th/Thai/PaymentSystems/OversightOfEmoney/Documents/%E0%B8%9E%E0%B8%A3%E0%B8%8E.%20%E0%B8%A7%E0%B8%B5%E0%B8%98%E0%B8%B5%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%81%E0%B8%9A%E0%B8%9A%E0%B8%9B%E0%B8%A5%E0%B8%AD%E0%B8%94%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%AF.pdf
15 National Health Act B.E. 2550. Unofficial English translation available at: http://en.nationalhealth.or.th/node/123.
16 ETDA Announcement on Safety Standards in Complianc with Security Procedure Presumed as a Reliable Method for Electronic Transaction, B.E. 2555. Available in Thai at: https://www.etda.or.th/files/1/files/129-191.PDF
17 NBTC Announcement on Measures to Protect Telecommunication Services Users' Personal Information, Right to Privacy and Freedom of Telecommunication B.E. 2549. Available in Thai at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2549/E/088/20.PDF.
18 UNTC, Status as at 18 September 2015 of 4. International Covenant on Civil and Political Rights https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en#EndDec
19 On 8 July 2014, the government of Thailand notified the UN Secretary-General through a letter from the Permanent Mission of the Kingdom of Thailand that the Martial Law has been invoked in Thailand and that, as a result, the government derogated from some articles of the ICCPR, including Article 19," by the prohibition of broadcasting or publishing certain content, particularly those inciting conflict and alienation in the society, false or provoking messages".
20 General Comment No. 16 (1988), para. 1

15. Thailand, with other ASEAN States adopted the ASEAN Human Rights Declaration on 18 November 2012 which upholds under Article 21 that:

> *"Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks."*[21]

VI. Areas of concern

Concerns with existing legislation on communications surveillance

16. There is no specific law on interceptions of communications. The communication surveillance is regulated through various laws, including Special Investigation Act B.E. 2547 (2004),[22] Criminal Procedure Act B.E. 2552 (1999)[23] (amended in 2015)[24], Computer Related Crime Act B.E. 2550 (1999)[25] (as of September 2015, is under amendment process[26]) and sectorial laws such as Anti-Money Laundering[27] and Anti-Drug laws[28.] These laws give the permission for the authority to conduct surveillance investigation.

17. The 2007 Computer-related Crimes Act (CCA) covers computer-related offences as outlined under Chapter 1 of the Act, which amongst others, include hacking, disclosure of access passwords to a third party, eavesdropping on computer data, as well as the dissemination of pornographic and other *harmful* Internet content.

---

21 ASEAN Human Rights Declaration. Available at: http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration

22 Special Investigation Act B.E. 2547. Unofficial English translation version available at: https://www.unodc.org/tldb/pdf/Thailand_Special_Investigation_Act.pdf

23 Criminal Procedure Act B.E. 2542. Unofficial English Translation available at: http://eng.moph.go.th/index.php/policy-advocacy/91-the-criminal-procedure-act-amendment.

24 Criminal Procedure Act B.E. 2542 (amended in 2005). Available in Thai at: http://library2.parliament.go.th/giventake/content_ncpo/ncpo-annouce115-2557.pdf.

25 Computer-related Crime Act B.E. 2550. Unofficial English translation version available at: http://itserv.ait.ac.th/Helpdesk/announce/cc_laws_eng.pdf.

26 Computer-related Crime Act B.E 2550. Available in Thai at: http://ictlawcenter.etda.or.th/de_laws/detail/de-laws-computer-related-crime-act

27 Anti-Money Laundering Act of B.E. 2542, Section 46 as amended by section 21 of the Anti-Money Laundering Act (No.2) B.E. 2551 (2008), "In the case where there is sufficient evidence to believe that any account of a financial institution's customer, communication device or equipment or computer is used or may be used in the commission of an offense of money laundering, the competent official entrusted in writing by the Secretary-General may file an ex parte application with the Civil Court for an order permitting the competent official to have access to the account, communicated data or computer data, for the acquisition thereof," unofficial English translation available at https://www.unodc.org/tldb/pdf/Thailand/THA_AML_2009.pdf.

28 The Narcotics Control Act B.E.2519 (1976), Section 14 fourth paragraph 1, "In the case where there is a reasonable ground to believe that any document or information which transmit by any post, telegraph, telephone, fax telephone, computer, tool or instrument in the communication, electronic communication or communication by information technology was used or may be used for the purpose of the commission offence relating to narcotics. The competent official who have approved in letter of the Secretary- General shall submit unilateral application to Chief Justice of the Criminal Court for having an issue to permit the competent official of obtained such information," unofficial English translation available at http://en.oncb.go.th/document/Narcotics%20Control%20Act%202519%20(1976)%20p1-9.pdf

18. The competent official, a person appointed by the Minister in the execution of this Act, must apply for authorisation to the competent Court, for conducting surveillance activities. These activities, as described under Section 18 (4) to (8), include: copying computer data, traffic data from a computer system not in the possession of a competent authority, ordering a possessor or controller of computer data and equipment to deliver that data, verify and access computer systems, computer data, traffic data or equipment storing data which is or may be used as evidence, to decrypt computer data and to seize as necessary computer system. Powers under Section 18 (1), (2) and (3) which refer to powers to summoning any person related to the offence, requesting traffic data and other information in their possession from service providers, respectively, do not require a judicial order. Furthermore, Section 26 of the Act requires that traffic data be retained by the service provider, for a period not exceeding 90 days, but this can be extended for a period of up to a year if requested by a competent official. Failure on the providers to do so will result in a fine.

19. Section 25 of the Special Case Investigation Act addresses the interception of postal, digital and telephonic communications. When there is a suspicion that a communication of any sort was used or may be used to commit a criminal acts as defined in the Act under Section 21[29], the Special Case Inquiry Official from the Department of Special Investigation may ask to the Chief Judge of the Criminal Court for an authorisation to obtain the information. When granting the permission the Chief Judge has to justify the decision to prove that there is reasonable ground that the person whose communication is being intercepted will or has committed a crime and that there is no other appropriate investigative method. The interception must never exceeds 90 days.[30]

20. Furthermore, it is important to note that the Telecommunication Business Act B.E. 2544 (2011), and related laws like Computer-related Crime Act B.E. 2550 (2007), sets various obligations on telecommunications operators. Set out by various regulations, these obligations include the retention of communications data of service users for a period of up to 3 months, and for the same period following the termination of the service.[31] Under Section 31, for the benefit of national security, or for the prevention of disaster that may case public harms, or for public interest, the

29 See: Section 21 Special Cases required to be investigated according to this Act are the following criminal cases:
(1) Criminal cases according to the laws provided in the Annex attached hereto and in the ministerial regulations as recommended by the BSC where such criminal cases shall have any of the following natures: (a) It is a complex criminal case that requires special inquiry, investigation and special collection of evidence. (b) It is a criminal case which has or might have a serious effect upon public order and moral, national security, international relations or the country's economy or finance. (c) It is a criminal case which is a serious transnational crime or committed by organized criminal group ; or (d) It is a criminal case in which influential person being a principal, instigator or supporter. This however shall be in line with details of the offence provided by the BSC.
(2) Criminal cases other than those stated in (1) where the BSC resolves by no less than two-thirds votes of its existing Board members. In a case of a single offence against various legal provisions and a particular provision is handled by Special Case Inquiry Official according to this Act, or in a case of several related or continuous offences and a particular offence is handled by the Special Case Inquiry Official according hereto, such Special Case Inquiry Official shall have a power to investigate offences against such other provisions or other matters and such case shall be considered as Special Case. Any case which the investigation has already been completed by Special Case Inquiry Official shall be considered as Special Case Investigation according hereto. This provision shall also apply to person who becomes a principal, instigator or supporter of an offence.

30 Available at: http://thailaws.com/law/t_laws/tlaw0294_2.pdf

31 See: Section 26 of the Computer-related Crime Act B.E. 2550 (2007)

government can request the National Telecommunications Commission to take action to provide it access to the telecommunication network. This request does not require judicial authorisation as the telecommunications licensees have an obligation to comply with the order of the Commission.

21. Under the Martial law [32], in accordance with its Article 6[33] "*the military authority shall have superior power over the civil authority in regard to military operation, desistence or suppression, or keeping public order".* It provided the junta, know as the National Council for Peace and Order (NCPO), extensive powers including to conduct surveillance. Under Section 9[34] (2) ,the military authority has the power "*to inspect message, letter, telegraph, package, parcel or others transmitting within the area under the Martial law."*

22. Despite having lifted martial law in most of the country in April 2015[35], there are still on-going concerns as to whether the procedures and safeguards contained in the national laws described above are currently in force and applied in practice. These concerns are compounded by the fact that, after lifting the martial law that had been in place since May 2014, Prime Minister Prayuth invoked Article 44, a special security measure, of the interim Constitution. Article 44[36] provide the Prime Minister with extensive unregulated and unchecked powers over the three branches of the government.[37]

23. The UN High Commissioner for Human Rights, Zeid Ra'ad Al Huseein has expressed his concern regarding the decision to bestow wide-ranging powers to the Prime Minister, the leader of the military coup, and concluded by urging "*the Thai Government to comply with its obligations under international human rights law and promptly restore normal civilian rule of law, as it pledged to do after the coup in May last year"*.[38]

Concerns regarding draft bill relating to privacy and surveillance

32 Martial Law B.E. 2457 (1914). Unofficial translation available at: http://www.thailawforum.com/laws/Martial%20Law.pdf

33 As amended by the Announcement of the Revolutionary Council No. 303 dated 13th December B.E. 2515 (1972)

34 As amended by the Announcement of the Revolutionary Council No. 303 dated 13th December B.E. 2515 (1972)

35 The order to abrogate the martial law published in Royal Gazette on 1 April B.E. 2558 (2015). Available in Thai at: http://library2.parliament.go.th/giventake/content_ncpo/ncpo-annouce010458.pdf. Also see: Sawitta Lefevre, A., *Thai Junta lifts martial law, but retains broad powers as it is,* Reuters, 1 April 2015. Available at: http://www.reuters.com/article/2015/04/01/us-thailand-politics-martiallaw-idUSKBN0MS4NI20150401

36 Section 44 reads as follows: *"In the case where the Head of the National Council for Peace and Order is of opinion that it is necessary for the benefit of reform in any field and to strengthen public unity and harmony, or for the prevention, disruption or suppression of any act which undermines public peace and order or national security, the Monarchy, national economics or administration of State affairs, whether that act emerges inside or outside the Kingdom, the Head of the National Council for Peace and Order shall have the powers to make any order to disrupt or suppress regardless of the legislative, executive or judicial force of that order. In this case, that order, act or any performance in accordance with that order is deemed to be legal, constitutional and conclusive, and it shall be reported to the National Legislative Assembly and the Prime Minister without delay."*

37 Associate Press in Bangkok, *Thailand 'still in the same boat' after martial law lifted,* 1 April 2015. Available at: http://www.theguardian.com/world/2015/apr/01/thailand-lifts-martial-law-coup

38 UN News Centre, *Thailand: UN rights chief warns against Government's 'draconian' powers,* 2 April 2015. Available at: http://www.un.org/apps/news/story.asp?NewsID=50495#.Vf7j3J1Viko

24. Over the course of December 2014 and January 2015, the Ministry of Information, Communication and Technology proposed ten Bills that will profoundly change the regulations of media and information in Thailand. The various proposed bills have been criticised for providing expansive powers to the Minister of Digital Economy and Society, while falling short of international human rights law and standards, particularly in relation to the right to privacy and freedom of expression.[39]

25. The Cybersecurity Bill[40], one of the 10 bills proposed, will provide the National Cybersecurity Committee (NCSC) with wide ranging powers to conduct communication surveillance, without adequate safeguards and limitations in accordance with the principles of legality, necessity and proportionality.

26. National human rights groups such as the Thai Netizen Network[41] and others such as the Committee to Protect Journalists [42]has called to scrap the Bill as it would allow for mass surveillance of online activities and would permit for the extensive surveillance powers currently awarded and performed under the Martial Law Order No. 29 to became law. Another major flaw in the Bill is that there are no check and balance mechanism. The NCSC will operate under the supervision of the Minister of Digital Economy and Society.

27. According to Article 33 and 34 in the current draft, the NCSC can order state agencies, private bodies, and individuals to take certain actions or refrain from taking action *"upon the occurrence of an emergency or danger as a result of cyber threat that may affect national security,".* This is similar to the current powers under the Martial Law and raises concerns for the protection of privacy of individuals.

28. Article 35 (3) of the Bill provides that the officials entrusted by the Secretary under this Act, have the power to "*to gain access to information on communications, either by post, telegram, telephone, fax, computer, any tool or instrument for electronic media communication or telecommunications, for the benefit of the operation for the maintenance of Cybersecurity."*

29. The Bill does not provide for the judicial authorisation of these powers but merely notes that the powers under section 35(3) would be specified by the Rules issues by the Council of Ministers..[43]

30. Dhiraphol Suwanprateep, Partner in Baker & McKenzie's Bangkok office said that *"There is no balance in this section between national security interests and data privacy of Thailand's citizens."* And on 24 January 2014, the Electronic Transactions

---

39 Pornwasin, A., *Digital economy bills 'need to be amended,* The Nation, 19 January 2015. Available at: *http://www.nationmultimedia.com/politics/Digital-economy-bills-need-to-be-amended-30252168.html*

40 Unofficial translation available at: https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf

41 Global Voices, *Thailand's Digital Economy Bills Could Worsen Media Repression,* 3 February 2015. Available at: https://advox.globalvoices.org/2015/02/03/thailands-digital-economy-bills-could-worsen-media-repression/

42 Committee to Protect Journalists, *Cyber security bill threatens media freedom in Thailand,* 20 January 2015. Available at: https://cpj.org/2015/01/cyber-security-bill-threatens-media-freedom-in-tha.php

43 The same warrantless search power is found in Article 14 of Incitement Bill (Dangerous Behavior Prevention and Suppression Bill) proposed by Ministry of Social Development and Human Security. See: Prachatai, *Thai junta's new censorship bill the first to define right/wrong sexual acts*, 10 February 2015. Available at http://prachatai.org/english/node/4772

Development Agency, which drafted the Bill acknowledged that the drafting had been rushed, and the Section 35 would be revised.[44]

31. One further worrying proposal is that the National Broadcasting and Telecommunications Commission (NBTC) will cease to be an independent regulator and will come under a Committee chaired by Prime Minister[45], which in turn could negatively affect policies on free and fair communication resources allocation, media and telecommunication operators licensing, content restrictions, and protection of personal data transmitted over communication networks.[46]

32. If Thailand's current government is committed to ensuring a return to democracy for Thailand and its people, the Cybersecurity Bill pending before the Council of State, must be reviewed to ensure its compliance with international human rights law and standards, particularly for the protection of the right to privacy.

Development of surveillance and monitoring of online communications and social media

33. There had been many attempts to upgrade Thailand's communication surveillance capabilities in the past decade, which increasingly focus on social media and internet based communication applications. These attempts coincided with major political changes and conflicts.[47]

34. In the evening after the announcement of Martial Law on 20 May 2014, the Peace and Order Maintaining Command (POMC) immediately issued twelve Orders, six of them are about media and communication control, and one of them (POMC Order No. 8/2557) is specifically about social media monitoring. On 21 May 2014, POMC demanded internet service providers to monitor and block content that may cause conflicts and threats to public order. On 22 May 2014, when National Council for Peace and Order staged a coup d'état, they immediately issued four announcements about media control (NCPO Announcement No. 12, 14, 17, and 18/2557)[48], which were then later followed by a number of announcements, including NCPO Announcement No. 26/2557 (online social media monitoring)[49].

35. In the same week of the coup, Permanent-Secretary of Ministry of ICT (MICT) announced a "National Single Gateway" plan to consolidate every international

---

44 DataGuidance, *Thailand: Data protection bill may 'hamper' foreign investmen*t, 28 January 2015. Available at: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3184

45 Waring, J., *Thai junta's dangerous steps to neuter telecoms regulator,* Mobile World Live, 12 January 2015. Available at: http://www.mobileworldlive.com/asia/asia-blogs/thai-juntas-dangerous-steps-neuter-telecoms-regulator/ ; Porwasin, A., *Group wants 'digital economy' bills scrapped, rewritten by affected parties,* 15 January 2015. Available at: http://www.nationmultimedia.com/homeGroup-wants-%5Cdigital-economy%5C-bills-scrapped-rewri-30251904.html

46 Pornwasin, A., *Digital economy bills 'need to be amended,* The Nation, 19 January 2015. Available at: http://www.nationmultimedia.com/national/Digital-bills-will-affect-media-reform-30252412.html

47 See also: Thai Netizen Network, *Thailand Chat App surveillance timeline*, 1 July 2015. Available in Thai at: https://thainetizen.org/2015/01/thailand-chat-app-surveillance-timeline/

48 Thai Netizen Network , *The Junta Digital Agenda: 60 Days Later* and *Changes and trends in Thailand's national information and communications policy after the 2014 coup – a 60 days observation*. Available in Thai at: https://thainetizen.org/2014/08/the-junta-agenda/

49 The Announcement of National Peace Keeping Council No. 26/2557. Available at: http://library2.parliament.go.th/giventake/content_ncpo/ncpo-annouce26-2557.pdf

internet gateways (IIG) in Thailand into one single link, which will *"make it easier to block websites and defend against cyberattacks"*.[50] In September 2015, the Ministry of ICT was ordered at a Cabinet meeting to establish this gateway.[51] Under the plan, MICT will oversee the construction of this new internet gateway.[52] This poses a serious threat to the enjoyment of fundament rights and freedoms online.[53] This is because the state would have the capability to intercept internet session information over time, to control (block or permit) information flows coming through Thailand, it would permit them to identify users' internet activities habits, and therefore the user themselves possible.

36. Since at least 2013 and more systematically since the coup in May 2014, the government has reportedly tried to control popular social media such as Facebook as well as limiting the capacity of internet users to communicate anonymously, including by using encryption.[54]

37. On 28 May 2015, Facebook was blocked for up to an hour (from around 15:40 to 16:20). Sources from local internet industry said it is a consequence from some equipment test at the gateway. Telenor Asia reported that Thai military government had requested that they do so and whilst the company later apologised for referring to the government but did not retract the claim.[55] This occurred in the aftermath of the coup, and the government warnings that it would monitor social media communications such as Line and Facebook.[56]

38. On 15 December 2014, Ministry of ICT issued an order No. 163/2557 to appoint a working group (comprised of military and civilian officials) to test a circumvention equipment to bypass Secure Sockets Layer (SSL) web encryption, a standard security technology for establishing an encrypted link between a server and a client. The working group is to work with internet service providers to test the online surveillance.[57] A report from TelecomAsia, with information from a virtual private network operator using the services provided for by CAT Telecom, suggested that it may involve the use of fake SSL certificates and targeting Facebook users[58] On 22 January 2015, it was reported that local ISPs were asked by the Ministry of ICT to

---

50 Prachatai, *Thai authorities to build state-owned internet gateway for more efficient censorship*, 28 May 2014. Available at: http://prachatai.org/english/node/4045

51 The Prime Minister Order on 27 August 2015, which includes the introduction of National Single Gateway. Available in Thai at: http://www.cabinet.soc.go.th/doc_image/2558/993152581.pdf

52 Prachachat, "□□□□□□"□□□□□□□□□"□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"□□□□□□□□□□□□□□□□□□□□-□□□□□□"□□□□□□-□□□", 27 May 2014. Available in Thai at: http://www.prachachat.net/news_detail.php?newsid=1401184718

53 Freedom House, *Freedom on the Net: Thailand*, 2014. Available at: https://freedomhouse.org/report/freedom-net/2014/thailand

54 Committee to Protect Journalists, *Thai junta expands media controls,* Alerts, 21 July 2014. Available at: https://www.cpj.org/2014/07/thai-junta-expands-media-controls.php

55 Buncombe, A., *Leading telecoms firm apologises to Thai junta after Facebook 'blocked'*, !7 June 2014, Available at: http://www.independent.co.uk/news/world/asia/leading-telecoms-firm-apologises-to-thai-junta-after-facebook-blocked-9543096.html

56 Davidson, H., and Weaver, M., *Thailand army delcares martial law, denies coup,* The Guardian, 20 May 2014, last updated on 3 June 2014. Available at: http://www.theguardian.com/world/2014/may/20/thailand-army-declares-martial-law-denies-coup-live

57 Information and Communication Technology Ministerial Regulation No. 163/2557. Available in Thai at: https://www.facebook.com/thainetizen/photos/a.10150109699603130.289409.116319678129/10153052852963130/

58 Sambandaraska, D., *Thai Government to test SSL surveillance,* Telecomasai.net, 26 January 2015. Available at: http://www.telecomasia.net/content/thai-government-test-ssl-surveillance

install in their data centres an interception equipment that can reveal username and passwords of Facebook users.[59]

39. Due to its popularity, social media and internet-based communication applications like Facebook, Twitter, YouTube, WhatsApp and Line are the main target for surveillance. Thai government tried in 2013 to get access to Line's users data but Naver, owner of Line, said they never received any request.[60] In December 2014, ICT Minister claimed that they *"can monitor all the nearly 40 million LINE messages sent by people in Thailand each day."*[61] Secretary-general of NBTC has asked Facebook, YouTube and Line to remove content critical of the Thai monarchy.[62]

40. In 2013, Citizen Lab of the University of Toronto published its findings on a computer spyware called Remote Control System (RCS), marketed and sold exclusively to governments by Hacking Team, an Italian company. Hacking Team presents their RCS as *"a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable."* Thailand was one of the countries the CitizenLab suspected of being a current or previous user of the RCS.[63]

41. According to Hacking Team's communications leaked in 2015, in September 2012, Hacking Team representatives met officers from Thai government agencies, including Government House, National Intelligence Agency, Internal Security Operational Center, Ministry of Defence, Royal Thai Army and Department of Correction[64] Six months later, National Security Council specifically asked Hacking Team if their product could target LINE, WeChat, and WhatsApp.[65] In April 2014, email exchanges confirmed that Hacking Team product could be used for all of them.[66] In July 2015, documents showing email exchanges revealed that a Hacking Team product, the Remote Control System Galileo, had been ordered and was to be del Thailand.[67] The Galileo system has has the ability to bypass encryption, take

---

59 Prachachat, □□□□□□□"□□□.□□□□□□□" □□□□□□□□□□ □□□□□□□□□-□□□□□□□□□□□□□□□, 22 January 2015. Available in Thai at: http://www.prachachat.net/news_detail.php?newsid=1421922012

60 Franceschi-Bicchierai, L., *Thai Police Want to Mine Popular Japanese App for Chat Records*, Mashable UK, 13 August 2014. Available at: http://mashable.com/2013/08/13/thai-police-line-app/

61 Russel, J., *Thailand's Government Claims It Can Monitor The Country's 30M Line Users*, Tech Crunch, 23 December 2014. Available at: http://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/

62 Gosh, Ni., *Thailand agency defends mass surveillance*, The Straits Times, 12 February 2015. Available at www.asianewsnet.net/Thailand-agency-defends-mass-cyber-surveillance-71690.html, Office of the National Broadcasting and Telecommunications Commission, *Thailand agency defends mass cyber surveillance,* 12 February 2014. Available at: www.nbtc.go.th/wps/portal/NBTC/Home/NewsActivi/PubNews/Detail/!ut/p/z0/fYxLDoIwFACv4oZl8x7QlrL0kxAMK9lAN-ZRi6maAqGixxcu4HImkwENDWhPi7tTcIOn18qtltc4F2WRK6yK8nLEveT1QWKN1SmFM-j_wXpwj2nSe9Bm8MF-AzS-C2Y3u2AjRO7tZyYT3OI2wnh8d5uKkKTNenUjllhBjGcmY3mSWpbEXIreiFSpDsanbn9WrF6B/

63 Marczak, Bi., Guarnieri, C., Marquis-Boire, M, and Scott-Railton, J., *Mapping Hacking Team's "Untraceable" Spyware*, The CitizenLab, University of Toronto, February 2014. Available at: *https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team%E2%80%99s-_Untraceable_-Spyware.pdf*

64 Wikileaks files published 8 July 2015, *Hacking Team, Thailand Project.* Available at: https://wikileaks.org/hackingteam/emails/emailid/445474

65 Wikileaks files published 8 July 2015, *Hacking Team: LH for Thailand National Security Council.* Available at: https://wikileaks.org/hackingteam/emails/emailid/445665

66 Wikileaks files published 8 July 2015, *Hacking Team: Japanese Messaging App Line Gian Traction Abroad*. Available at: https://wikileaks.org/hackingteam/emails/emailid/112497

67 Wikileaks files published 8 July 2015, *RE: (Draft) End User Statement.* Available at:
See also: TIKIT Delivery Preparation, Available at
https://ht.transparencytoolkit.org/FAE%20DiskStation/5.%20SWAP/TIKIT%20%28Thailand%29/TIKIT_Delivery_Preparatio

control of a user's device, and to monitor all activities conducted on the device, poses significant threats to the right to privacy.[68] AsiaSentitel, a web-based independents Asian regional publication focused on news, business, arts and culture, said Thailand had spent USD 466,482 in total for products and services provided by Hacking Team.[69]

42. Apart from surveillance technology and equipments, significant human resources have been invested to monitor open source social media. According to former Minister of Information and Communication Technology Pornchai Rujiprapa in August 2015, Technology Crime Suppression Division (TCSD) has a longstanding 30-person team that operates around the clock, scanning online postings and following up complaints from the public on cyber crimes, including royal defamation.[70]

43. A study report from Armed Forces Committee under the Senate of Thailand confirmed 60-70 officers from Royal Thai Army alone participated in the Army's "Information Warfare" and "Information Operations" to read online content and respond if content potentially falling under the crime of lèse majestéis founded. While the full scale of monitoring is unclear, these numbers can reveal the size of the efforts: in 2011 fiscal year alone, Royal Thai Army officers found 57,958 urls/messages that were deemed to be lèse majesté.

44. This monitoring of the on-line activities is of particular concerns since expression of political dissent and other forms of legitimate freedom of expression are object of increased repression, while lèse majesté provisions continue to be used to prosecute and convict individuals in violation of applicable international human rights standards.

45. Monitoring of on-line activities and the chilling effect that accompany it has increased since the military coup in 2014. Citizen surveillance is encouraged by the State. On 23 June 2014, Deputy police commissioner General Somyot Poompanmoung has announced THB 500 (about USD 15) bounty for each photo of people illegally expressing a political stance, this also include online expression.[71]

Unlawful searches and other measures violating the right to privacy

46. Following the military coup in 2014, political activists, lawyers, and journalists were increasingly subjected to searches in their homes and offices and seizures of their

---

n.txt, Delivery Certificate https://ht.transparencytoolkit.org/FAE%20DiskStation/5.%20SWAP/TIKIT%20%28Thailand%29/TIKIT_Delivery_Certificate.pdf

68 Galileo is a remote control system which allows to take control of a target and to monitor them even if they are using encryption. Hacking Team sells it as a tool to *"bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain."* For more information: https://www.hackingteam.it/images/stories/galileo.pdf

69 Berthelsen, J., *How Asia's government Spy on Their Citizens*, Asia Sentinel, 13 July 2015. Available at: http://www.asiasentinel.com/society/asia-governments-spy-citizens/

70 Belford, A., *Special Report: Thai junta hits royal critics with record jail time*, Reuters, 3 September 2015. Available at: http://www.reuters.com/article/2015/09/04/us-military-convictions-thailand-special-idUSKCN0R400X20150904

71 Saiyasombut, S., *Thailand's junta offers $15 reward for info on dissidents*, Asian Correspondent, 24 June 2014. Available at: http://asiancorrespondent.com/124071/thailands-junta-offers-15-reward-for-info-on-dissidents/

computer under the extensive and unregulated powers provided to the authorities under the Martial law in ways that unlawfully interfered with their right to privacy.[72]

47. Based on documentation from iLaw released in 17 June 2014, in the two months following the coup, 183 homes and business in Bangkok but also across the country were searched. Six places had been raided twice in the time frame. 53 people were arrested after the raids.[73] These places belonged to politicians, academics, activists, people who join anti-coup demonstrations, and community radio stations.[74]

48. Confiscation of computer and communication devices of people who were arrested, both in their homes or offices or on the site of demonstration, became common.[75] State officers also demanded passwords of email and social media accounts from these people after their arrest.[76]

49. On 25 May 2014, three days after the coup, troops raided the house of Somyot Prueksakasemsuk, a labor and political activist and a magazine editor who was accused of Section 112 of the Criminal Code (lèse majesté provision)[77], and imprisoned without bail since 2011. Officers arrested Sukanya Prueksakasemsuk and Panitan Prueksakasemsuk, Somyot's wife and son, and confiscated two laptop computers belonging to them.[78] No charges were brought against either Sukanya or Panitan.

50. On the night of 26 June 2015 (00:30 27 June), police officers tried to search, without warrant, a car belonging to Thai Lawyers for Human Rights's lawyer. The car was parked in front of Military court as the lawyer assisted her clients (New Democracy Movement activists who were arrested that evening). After obtaining a warrant in the next afternoon (15:05 27 June -- 14½ hours after the first attempt) the officers searched laptop computers, tablets and mobile.

Data protection

51. Thailand does not have yet a comprehensive data protection law despite some protections under the Official Information Act of 1997, the Thai Civil and Commercial Code, and other sectoral laws. For the private sector, there is no general law to

72 Amnesty International, *Thailand: Attitude adjustments: 100 days under Martial Law*, ASA 39/011/2014, pp Available at: http://www.amnesty.org.uk/sites/default/files/asa390112014en_0.pdf,

73 It is unclear how many people were ordered to report and/or arrested following the raids, but in August 2014 the Office of the High Commissioner for Human Rights reported that some 700 people had been ordered to report and/or arrested under Martial Law powers. See: UN News Centre, *UN rights office urges probe of alleged torture of 'Red Shirt' activist,* 5 August 2014. Available at: ttp://www.un.org/apps/news/story.asp?NewsID=48413#.U-1b3vldWcE.

74 ilaw reports on the trespassing private property, available at: http://ilaw.or.th/node/3207 and The Statistics on the trespassing: private property by the military after Coup d'etat, available in Thai at: http://ilaw.or.th/node/3141

75 See: Prachatai article on the detention by National Peace Keeping Council published on 20 June 2014. Available in Thai at: http://prachatai.org/journal/2014/06/54125

76 The Junta Digital Agenda: 60 Days Later. Changes and trends in Thailand's national information and communications policy after the 2014 coup – a 60 days observation. Available in Thai at: https://thainetizen.org/2014/08/the-junta-agenda/ Page 10-12.

77 Section 112 reads as follows: *"Whoever defames, insults or threatens the king, queen, heir-apparent, or regent shall be punished with imprisonment of three to fifteen years."*

78 See: Article on Military invades Somyot Prueksakasemsuk's House and detained his family. Available in Thai at: http://www.matichon.co.th/news_detail.php?newsid=1401014048

protect personal data. Under the wrongful act principle of Thai Civil and Commercial Code,[79] unauthorised collection, use or disclose of data are considered to be wrongful only if it causes damage to the data owner.

52. The drafting of the data protection bill has been in process for more than 10 years.[80] But in a worrying recent development, a Personal Data Protection Bill[81] was presented as part of a series of bills announced in December 2014 and January 2015 which form part of the digital economy agenda.[82]

53. The current text of the bill contains some concerning provisions which departs from previous drafts. Concerns about the current bill include:

    1) Broad and vaguely defined exemptions to data protection, which will leave significant loopholes;
    2) Failure to define the role and responsibilities of data processor and data controllers;
    3) Failure to establish an independent data protection authority, proposing instead the creation of a Committee composed of part time individuals and depending, for its functions and secretariat, on the Office of National Cybersecurity committee.

54. The Personal Data Protection Bill has been edited by Council of State and has now been sent back to Cabinet. We urge the government of Thailand to review once again the Bill to ensure its compliance with international data protection standards.

55. The current lack of a comprehensive data protection law is of particular concern in view of the following:

Mandatory SIM card registration

56. In 2015 the Thai government's Office of The National Broadcasting and Telecommunications Commission (NBTC) introduced a requirement that all mobile phone users register their numbers, by declaring identification card for Thai citizens, passports for foreigners, by 31 July 2015.[83] After the date, the unregistered numbers were disconnected from services.

57. 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.

---

79 Thai Civil and Commercial Code, Section 420. Unofficial English translation available at: http://www.samuiforsale.com/law-texts/thailand-civil-code-part-1.html.

80 Various governmental agencies involved in this drafting process, including the Ministry of Information and Communication Technology, the Office of Official Information and the Electronics Transaction Development Agency (ETDA).

81 Unofficial translation available at: https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf

82 Personal Data Protection Bill. A version approved by Council of State (August 2015) available in Thai at http://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act. Unofficial English translation of a cabinet approved version on 6 January 2015 at: https://thainetizen.org/2015/01/digital-economy-cyber-security-bills-en/

83 The Announcement of National Broadcasting and Telecommunications Commission on the pre-paid SIM card compulsory registration. Available in Thai at: http://www.nbtc.go.th/wps/wcm/connect/NBTC/b968e883-b220-46c9-9944-c28931385e32/img-121143318.pdf?MOD=AJPERES&CACHEID=b968e883-b220-46c9-9944-c28931385e32

Smart identification card

58. On 10 September 2004, the Cabinet started the Smart identification card project by issuing the Ministerial Regulation No.21 B.E. 2547[84] subject to the Identification Card Act B.E. 2526 of 1983.[85] The objectives of the project are to facilitate and to standardize all public services. On 3 September 2007, the Minister of Interior announced another Ministerial Regulation No.22 B.E.2550[86] to mandate collecting fingerprints of left and right thumbs when Thai citizen issue the ID cards.

59. The collection of biometric information, such as the fingerprints, is obligatory to all Thai citizen over the age of 7.[87]

60. Without a comprehensive data protection law , this regulation can lead to the misuse and abuse of the personal data, including facilitating unlawful surveillance. Furthermore, there this is particularly concerning given that it is about the processing of sensitive data and the data of minors.

III. Recommendations

We recommend that the government of the Kingdom of Thailand to:

61. Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards and respect the right to privacy;
62. Ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted;
63. Strengthen effective oversight over the surveillance practices of its state security and intelligence agencies;
64. Review all bills related to communication and media currently pending and in particular the Cybercrime Bill, to ensure they comply with Thailand's national and international human rights obligations, and in particular the principles of necessity, proportionality, judicial authorisation, and oversight in relations to communication surveillance;
65. Investigate reported unlawful communications surveillance and monitoring activities by state agencies, and take necessary measures to ensure access to redress in case of violations;
66. Revoke mandatory SIM card registration policy established by B.E. 2558 of 2015;
67. Adopt a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority;
68. Ensure that data processing of personal data is conducted in compliance with national and international standards and obligations, particularly with regards to the

84 Ministerial Regulation No.21 B.E.254. Available in Thai at: http://law.longdo.com/law/351/sub20403#_ftn1
85 Identification Card Act B.E.2526. Available in Thai at: http://www.musisaket.go.th/dow-load/nt3.pdf. (See also; current Identification Card Act B.E.2556. Available in Thai at: http://www.audit.psu.ac.th/data/cop_doc/group_201_0019.pdf.
86 Ministerial Regulation No.22 B.E.2550. Available at: http://www.koomuesorb.com/private_folder/PDFlaw2/koomuesorb733.4.pdf
87 Ministerial Regulation No.23 B.E.2554. Available at: http://www.library.coj.go.th/info/data/M5-04-023.PDF.

processing of sensitive personal information, and any violations are investigated and redress provided to victims.