Suggestions for right to privacy-related questions to be included in the list of issues on Thailand, Human Rights Committee, 117th Session, June 2016

April 2016

Privacy International and Thai Netizen Network (TNN) have concerns on the legislation and practices related to surveillance in Thailand.[1] Further, the organisations are concerned at the increasing monitoring of social media and other internet based communications services for the purpose of identifying political dissent, often in pursuant of prosecutions under the overbroad crime of lèse majesté and related crimes, which result into unlawful intrusion into people's privacy and have a chilling effect on freedom of expression.

1. Lack of protection of the right to privacy in the Thai Interim Constitution

Article 35 of the previous Constitution of Kingdom of Thailand included a right to privacy as a human right.[2] 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. The Interim Constitution does not explicitly uphold the right to privacy and the only provision on the protection and promotion 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."[3]

2. Concerns with existing legislation and policies on interception of communications

There is no specific law on interceptions of communications. Instead, communication surveillance is regulated through various laws, including Special Investigation Act B.E. 2547 (2004), Criminal Procedure Act B.E. 2552 (1999) (amended in 2015), Computer Related Crime Act B.E. 2550 (1999)

---

[1] Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. Thai Netizen Network is a Bangkok-based civil rights organisation that works to defend and promote information rights in Thailand.

[2] B.E. 2550 (2007) Constitution Article 35: "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".

[3] 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

(as of September 2015, is under amendment process) and sectorial laws such as Anti-Money Laundering and Anti- Drug laws.[4]

These laws give the permission for the authority to conduct surveillance investigation.

In particular, 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 serious criminal acts as defined in Act, 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 exceed 90 days.

Under the 2007 Computer-related Crimes Act (CCA)[5], an official 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. However, 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.

These wide surveillance powers under the Computer-related Crimes Act are of particular concerns because the Act has been used to prosecute internet users from posting any 'false information' online. Due to the vague term 'false information', the Act has been used for example to prosecute cases of lèse-majesté-like statements, to prosecute almost any comment about the Royal Family perceived as negative.[6]

The martial law introduced in May 2014 granted the military the right "to inspect message, letter, telegraph, package, parcel or other things transmitting within the area under the Martial Law."[7]

Further, on May 2014, the military government published an Order 26/2014 on "the control and surveillance of the use of social media." In this order, the government claims the right to "monitor and access the computer traffic, the use of websites, social media, photos, text, video and audio which are

---

[4] Special Investigation Act B.E. 2547. Unofficial English translation version available at: https://www.unodc.org/tldb/pdf/Thailand_Special_Investigation_Act.pdf; 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; 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; Computer-related Crime Act B.E. 2550. Unofficial English translation version available at: http://itserv.ait.ac.th/Helpdesk/announce/cc_laws_eng.pdf. 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; 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), unofficial English translation available at https://www.unodc.org/tldb/pdf/Thailand/THA_AML_2009.pdf; the Narcotics Control Act B.E.2519 (1976), Section 14 fourth paragraph 1, unofficial English translation available at http://en.oncb.go.th/document/ Narcotics%20Control%20Act%202519%20(1976)%20p1-9.pdf.

[5] The Act 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.

[6] Privacy International researched one case of prosecution under the Act. See details here: https://privacyinternational.org/node/674

[7] See unofficial English translation: http://www.thailawforum.com/laws/Martial%20Law.pdf

deemed to instigate violence and unrest, which are deemed to be unlawful and which violate the National Council for Peace and Order's (NCPO) Orders."

Despite having lifted martial law in most of the country in April 2015[8], 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 provides the Prime Minister with extensive unregulated and unchecked powers over the three branches of the government.[9]

On 29 March 2016, the Head of NCPO issued Order No.13/2559 (2016), which effectively become a law, according to Article 44 of the 2014 Interim Constitution. Articles 3 and 4 of the Order give NCPO officers power to summon and arrest people, search premises, people, and vehicles, confiscate, request for information, without warrant, if they suspect someone might doing illegal activities as specified in the List attached to this Order.[10]

3. Blanket data retention requirements and access to telecommunication networks

Section 26 of the 2007Computer-related Crimes Act requires that traffic data be retained by service providers, 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.[11]

Under Section 31 of the Telecommunication Business Act B.E. 2544 (2011), the government can request the National Telecommunications Commission to take action to provide it access to the telecommunication network, on grounds of national security, prevention of disaster that may case public harms, or public interest. This request does not require judicial authorisation as the telecommunications licensees have an obligation to comply with the order of the Commission.[12]

4. Concerns regarding draft bill on cybersecurity

The Cybersecurity Bill, one of the 8 bills proposed by the Ministry of Information and Communication Technology, 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.[13]

---

[8] 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

[9] 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." 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

[10] Order (in Thai): http://www.ratchakitcha.soc.go.th/DATA/PDF/2559/E/074/1.PDF

[11] Section 26 of the Computer-related Crime Act B.E. 2550 (2007)

[12] Unofficial translated version available at: https://www.bot.or.th/English/PaymentSystems/ OversightOfEmoney/RelatedLaw/Documents/et_act_2544_Eng.pdf

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

Among the most controversial provisions, Article 35 (3) of the Bill provides that the officials 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."

National human rights groups has called to scrap the Bill as it would allow for mass surveillance of online activities without judicial authorisation or oversight.[14] The latest analysis of the Bill by Thai Netizen Network shows how the Bill does not meet 11 of the 13 International Principles on the Application of Human Rights to Communications Surveillance.[15]

5. Concerns about surveillance and monitoring of online communications and social media

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

Just after the introduction of martial law on 20 May 2014, the Peace and Order Maintaining Command (POMC) issued twelve Orders, six of them were about media and communication control, and one of them (POMC Order No. 8/2557) was 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), which were then later followed by a number of announcements, including NCPO Announcement No. 26/2557 (online social media monitoring).[16]

Last year, plans were also put in place to establish "National Single Gateway" aimed at consolidating every international internet gateways (IIG) in Thailand into one single link, which will "make it easier to block websites and defend against cyberattacks". This poses a serious threat to the enjoyment of fundament rights and freedoms online, particularly as it would give state officials the capability to intercept internet session information over time, to control (block or permit) information flows coming through Thailand, to identify users' internet activities.[17]

Due to its popularity, social media and internet-based communication applications like Facebook, Twitter, YouTube, WhatsApp and Line have been the main target for government's surveillance. In December 2014, ICT Minister claimed that they "can monitor all the nearly 40 million LINE

---

[14] See 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/ 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

[15] See https://thainetizen.org/2016/04/cybersecurity-bill-necessary-proportionate/

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

[17] Prachatai, "Thai authorities to build state-owned internet gateway for more efficient censorship", 28 May 2014. Available at: http://prachatai.org/english/node/4045 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 Freedom House, Freedom on the Net: Thailand, 2014. Available at: https://freedomhouse.org/report/freedom-net/2014/thailand

messages sent by people in Thailand each day."[18] On 22 January 2015, it was reported that local ISPs were asked by the Ministry of ICT to install in their data centres interception equipment that can reveal username and passwords of Facebook users.[19]

The technical surveillance capabilities of the Thai agencies are not officially known. However, it is of particular concern that, according to reports by Citizen Lab of the University of Toronto in 2013[20] and leaked communications in 2015[21], Thailand may be the current or previous user of the advanced surveillance technology, Remote Control System Galileo, marketed by the Italian firm Hacking Team. The Galileo system has the ability to bypass encryption, take control of a user's device, and to monitor all activities conducted on the device, poses significant threats to the right to privacy.[22]

Apart from surveillance technology and equipment, significant human resources have been invested to monitor open source social media. According to former Minister of Information and Communication Technology in August 2015, the 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.[23]

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 majesté is found. 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 and their families found 57,958 urls/messages that were deemed to be lèse majesté, and as a response posted a combined numbers of 3,914,314 urls/messages of counter information.[24]

This monitoring of the on-line activities is of particular concern 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.

---

[18] 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/

[19] Prachachat, Against Cyber Act. Netizens buzz point violations of personal information.", 22 January 2015. Available in Thai at: http://www.prachachat.net/news_detail.php?newsid=1421922012

[20] 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

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

[22] 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

[23] 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

[24] Subcommittee for the Study of Online Social Media and Threats to National Security, Report on the Study of Online Social Media and Threats to National Security, Senate Committee on Armed Forces, 2012 http://www.senate.go.th/w3c/senate/pictures/comm/66/file_1353298809.pdf

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. For example, on 23 June 2014, Deputy police commissioner announced THB 500 (about USD 15) reward for each photo of people illegally expressing a political stance, this also include online expression.[25]

6. Unlawful searches and other measures violating the right to privacy

Following the military coup in 2014, political activists, lawyers, and journalists were increasingly subjected to unlawful searches in their homes and offices and seizures of their 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.[26]

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. These places belonged to politicians, academics, activists, people who join anti-coup demonstrations, and community radio stations.[27] 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. State officers also demanded passwords of email and social media accounts from these people after their arrest.[28]

List of issues

Based on the above observations, Privacy International and Thai Netizen Network propose the following questions for the List of Issues on Thailand:

Article 17:

- What laws, orders and procedures currently govern the interception of communications and retention of communications data? How these measures comply with the principles of legality, necessity and proportionality?
- What measures is Thailand taking to investigate reports of unlawful surveillance of journalists, political activists and human rights defenders to ensure that their right to privacy, freedom of expression, peaceful assembly and association are respected and protected? What measures to prevent violations of these rights to reoccur?
- What is the status of the Cybercrime Bill, and how does it comply with Thailand's national and international human rights obligations, in particular in relation to the right to privacy?

---

[25] 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/

[26] 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

[27] 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

[28] 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 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.