Submission on the right to privacy in Thailand, Human Rights Committee, 119th Session

February 2017

1. Introduction

Privacy International notes the written replies by the government of Thailand to the Committee's list of issues.[1]

The organisation remains concerned over the practices of surveillance by Thai authorities. National legislation governing surveillance is inadequate, unclear as to the powers, scope and capacity of state surveillance activities and thus it falls short of the required human rights standards to safeguard individuals from unlawful interference to the right to privacy.

In this submission, Privacy International provides the Committee with additional, up to date information to that contained in the briefing submitted to the Committee in advance of the adoption of the list of issues in 2016.[2] Unless otherwise stated, the concerns expressed in the 2016 submission are on going and if they are not repeated here it is solely for brevity sake.

2. Concerns about the Computer Crimes Act - Lack of safeguards related to retention and access of traffic data

As noted in the 2016 submission, Thailand does not have a comprehensive law to cover communications surveillance. Instead a range of laws apply, including most notably the Computer Crimes Act.[3] Section 26 of the Computer Crimes Act requires that traffic data be retained by service providers, for a period not exceeding 90 days.[4] This period can be extended for up to a year if requested by a competent official. Failure on the providers to retain the traffic data will result in a fine.[5]

---

[1] Replies of Thailand to the list of issues, UN doc. CCPR/C/THA/Q/2/Add.1.
[2] Available at: http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/THA/INT_CCPR_ICO_THA_23558_E.pdf
[3] The Computer Crimes Act deals with offences committed against computer systems or computer data and offences which are already crimes under the Thailand Penal Code and are committed via a computer.
[4] Traffic data is defined to include data showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.
[5] Section 26 of the Computer Crimes Act B.E. 2550 (2007).

Access to such traffic data does not require any judicial authorization. In fact, while officials must apply for court authorization to conduct certain types of communications surveillance, this is not the case for traffic data (see Section 18.)

In its replies to the list of issues, the government of Thailand noted that the Computer Crimes Act is currently being amended. We understand that the amendments to the Act were adopted in December 2016 despite significant opposition by civil society organisations, including Thai Netizen Network. The amendments fail to address concerns about protection of privacy and freedom of expression, instead they expand on the unchecked powers of surveillance, including notably allowing almost unfettered access to metadata for the investigation of any crime.[6]

On the issue of differentiation in safeguards and procedural rules between the collection and analysis of content and metadata, the UN High Commissioner for Human Rights noted that: "the aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication".[7]

More recently, the Court of Justice of the European Union confirmed and elaborated on its jurisprudence, by noting that metadata "is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them […]. In particular, that data provides the means […] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[8]

This conclusion, confirmed by other human rights experts and reflected in some conclusions of the Human Rights Committee, reflects the fact that with the advancement of telecommunications and telecommunications' interception technologies, there is no justification for making distinctions in legal protections based on the nature of the data collected.[9]

3. Social media monitoring as an interference with privacy

Privacy International is particularly 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

---

[6] An online petition by Thai Netizen Network to oppose the amendments attracted more than 370,000 signatures (link to the petition and other relevant information: https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand)

[7] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014), paragraph 19.

[8] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).

[9] See, inter alia, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015) and Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016).

related crimes, which result into unlawful intrusion into people's privacy and have a chilling effect on freedom of expression.

Social media monitoring in Thailand is conducted by police, the military and other agencies. But beyond its security agencies, the government has empowered networks of citizens whom it encourages to denounce those who post online content considered contrary to government policies.

The Thai government has deployed substantial resources in order to surveil the population over social media. The Technology Crime Suppression Division (TCSD) – the police unit that specialises in cyber-crime – has deployed a 30-person team that operates around the clock, scanning online postings and following up complaints from the public on cybercrimes, including royal defamation.[10] The military has also set up an "Army Cyber Centre" dedicated to monitoring news deemed critical of the royal family. An earlier Senate report 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.[11]

After the death of the Thai King Bhumibol Adulyadej on 13 October 2016, social media surveillance has reportedly considerably stepped up.[12] The Thai government's replies to the list of issues confirms this where it states that "at present, there has been an increasing number of defamation incidents conducted in cyber space or social media, resulting in a rise in cases filed against the accused by referring to Section 14 of Computer Crime Act in connection with Sections 326 and 328 of the Criminal Code (on offence of defamation)."[13]

Apart from the police and the military, the Thai government relies largely on Thai citizens to monitor and report on political dissent. Active encouragement includes providing financial rewards for sharing of personal information, including pictures, of those displaying opposition to the government, [14] to reactivating the cyber scout programme, encouraging students to monitor the internet and denounce anything illegal according to Thai law.[15]

Beyond active encouragement, the government can rely on the support of a range of groups of private individuals, including some ultra-royalist groups, whose activities result in the invasion of individuals' privacy in the quest to pursue the crime of lèse-majesté".

---

[10] 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

[11] 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

[12] Prachatai, Thailand's witch-hunting culture explained by sociologist, 26 October 2016, http://prachatai.org/english/node/6672?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+pra

[13] Replies of Thailand to the list of issues, UN doc. CCPR/C/THA/Q/2/Add.1, paragraph 107.

[14] 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/

[15] See Privacy International, Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand, September 2016, https://www.privacyinternational.org/node/935

Thai authorities use the information revealed to support the prosecution of individuals exposed by such groups.[16]

Unlike most websites, social media services are spaces that require the user to create an account and log in to access the full range of social media services, for example, sharing articles or exchanging messages with other users. Each social media service is governed by terms of use set out by the private companies that provides the service as to what can and cannot be accessed when you are logged in or not logged in.

Any attempt by law enforcement agencies or security services to covertly add the targeted user as a validated contact, e.g. to use fake profiles, to obtain further information than what is publicly available, should be treated as undercover surveillance and addressed with constraints and safeguards similar to those in place for undercover activities. That is, any attempt to infiltrate person-to-person, person-to-group, group-to-group interactions is covert state action that needs to be strictly regulated by law. As it amounts to an interference with someone's privacy, it should be demonstrably necessary and proportionate to the achievement of a legitimate aim.

Further, the privacy's implications of monitoring 'publicly available' information on social networking sites should be addressed. The fact that data is *publicly available* does not suffice for unregulated and un-checked collection, retention, analysis and other processing.

In particular, the authorities' collection and use of *publicly available* social media data without informed public awareness and debate, clear and precise statutory framework and robust safeguards fall short of standards of protection of the right to privacy and of personal data protection. This is becoming increasingly concerning in light of the development of technologies that can process and aggregate a vast range of data, including personal data, creating profiles of individuals.[17]

4. Attempts to circumvent encryption in order to conduct surveillance

Beyond social media monitoring mentioned, above, Privacy International is concerned about the expansion of online surveillance methods conducted by the Thai government,

---

[16] For example the Social Sanction (SS) group became well-known with the arrest of Norawase Yotpiyasathien, a business administration student from Kasetsart University, for his blog posts deemed to contain content insulting the royal family. He was, at 23 years old, the youngest person arrested for lèse-majesté, which caused concern among students. The SS exposed Norawase and published his name, photos, personal address and phone numbers online. When he was arrested the SS wrote "another one is down." Norawase was arrested before the military coup, a time when lèse-majesté sentences were significantly more lenient and he was therefore released on bail after a few days of arrests. More information on this and other cases are contained in Privacy International, Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand, September 2016, https://www.privacyinternational.org/node/935

[17] Some national oversight bodies have expressed concerns about the privacy implications of the use these technologies. For example, To equal effect, the UK Chief Surveillance Commissioner commented in 2015 that "*perhaps more than ever, public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices. I repeat my view that just because this material is out in the open, does not render it fair game*" (Office of Surveillance Commissioners Annual Report for 2014-15, paragraph 5.72.)

in particular its effort to circumvent the encryption of many different online services by secretly undermining their security and directly impacting the privacy of internet users.

Research published by Privacy International highlights that the Thai Government's blocking of Facebook, 6 days after the military coup on 28 May 2014, may have been an attempt to circumvent the platform's encryption and spy on its users, rather than attempting to censor Facebook users as initially reported. Privacy International could not establish if the Thai Government managed to circumvent encryption. [18]

In addition, the research illustrates how the Thai military government reportedly conducted downgrade attacks. Downgrade attacks are a way for the attacker to force the user to communicate with their email service provider via an unencrypted channel. This means the security of people's email communications through mail clients such as Apple Mail, Microsoft Outlook and Thunderbird was likely compromised, and their emails re-routed through insecure channels. This weakened security may have allowed the Thai Government to access the content of the emails.

5. IMSI catcher and other surveillance technologies

The technical surveillance capabilities of the Thai agencies are not officially known. According to reports by Citizen Lab of the University of Toronto in 2013[19] and leaked communications in 2015[20], 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.[21]

More recently, government documents have revealed that Thailand purchased IMSI (International Mobile Subscriber Identity) catchers. In January 2015, the Swiss government released the list of export licences granted to companies based in Switzerland that were selling surveillance technologies.[22] The document reveals that between March 2012 and January 2013, Thailand has purchased nine items requiring an export licence under the category "Mobile telecommunications interception or jamming equipment, and monitoring equipment" and the subcategory "Interception equipment

---

[18] Privacy International (2017) Who's That Knocking At My Door?: Understanding Surveillance In Thailand

[19] 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

[20] 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

[21] 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

[22] See https://www.privacyinternational.org/node/98

designed for the extraction of voice or data, transmitted over the air interface". This is the category of licence IMSI catchers require. Likewise, in the UK, since 2015, the Department for Business, Innovation and Skills also started publishing data on export licences. Thailand obtained six different licenses for telecommunications interception equipment from the UK.[23]

IMSI catchers are devices that mimic the operation of a cell tower device in order to entice a users' mobile phone to surrender personally identifiable 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. Further, IMSI catchers are becoming increasingly cheap and these devices have been miniaturised to the point of being concealable on a person in a crowd rather than requiring a large van. But IMSI catchers are far from harmless given that their capacity to interfere with right to privacy goes beyond the person targeted. [24]

In its concluding observations on the Republic of Korea, this Committee expressed its concerns about "the operation and insufficient regulation in practice of so called 'base-station'".[25] The technology reportedly in the hands of the Thailand authorities raises similar concerns, due to the lack of specific regulations of its use. This is further exacerbated given that the deployment of IMSI catchers could contribute to the repression of freedom of expression and of peaceful assembly in Thailand.

6. Application of Orders that prevent corporate transparency

While the martial law established after the 2014 coup was lifted in April 2015, the Thai military government immediately implemented the National Council for Peace and Order (NCPO) Order No. 3/2558, designed to respond to actions allegedly intending to undermine or destroy peace and national security. The order grants extensive powers to a specific category of military of officers called 'Peacekeeping Officers'.

---

[23] See https://docs.google.com/spreadsheets/d/11_TtwzbRIP9QD_aKA6ej8REFwVsS-hmB91WCTAYfP9g/edit#gid=831716195

[24] An IMSI catcher is portable equipment that allows the interception of data (phone communications, messages, location data) from phones in its surrounding environment. Inorder for a mobile phone to function it has to communicate with a cell tower. The phone then chooses the cell tower it communicates with based on the strength of the signal. An IMSI catcher pretends to be a powerful cell tower - it sends a very strong signal so that the phone in the surrounding areas connect to it instead of to an actual cell tower. Once connected to the IMSI catcher some data becomes available to the person in control of the IMSI catcher. IMSI catchers are often presented as a tool for targeted interception (one has to be geographically close to the targeted person to intercept their communications), yet IMSI catchers can capture all the data of all phones in their surrounding perimeter that connect to it. And indeed, some metadata from nearly every phone in the area surrounding it. There is also no technical barrier for the operator to intercept many phone conversations and SMS messages simultaneously. In general, each device can intercept eight phones in parallel but additional hardware can be purchased to multiply this value to the desired rate.

[25] Concluding observations of the Human Rights Committee on the fourth periodic report of the Republic of Korea, UN Doc. CCPR/C/KOR/CO/4, 3 December 2015.

Peacekeeping Officers are in charge of preventing and suppressing offences related to lèse-majesté, internal security, rearm regulations and "any violation of any other orders issued by the NCPO."[26]

After the coup, the NCPO had issued a notification (NCPO Notification No. 26/2557) establishing an online social media committee to "examine, inspect and access 'online information". The committee had the powers to suspend or close websites and social media platforms, including those accused of undermining the military government. Since Order No. 3/2558, Peacekeeping Officers are now in charge of enforcing this notification.[27]

The work of Peacekeeping Officers is not subjected to any form of judicial oversight. Order No. 3/2558 also grants the government the authority to restrict publishing any types of data which are not in the national interest. This has impacted the ability of telecommunications companies to be transparent about the government requests they receive to hand over user data, block services or take down content. The telecommunications company DTAC, part owned by the Telenor Group in Norway, stated in their government access report:

> "Ordinarily there is no legislation which prevents the publication of aggregate data relating to the use by the government of the powers described in this report. However under the expansive extrajudicial powers vested in the government under NCPO Order No. 3/2558 issued under Section 44 of the Interim Constitution, it has the authority to restrict publishing of any types of data which are not in the national interest".[28]

7. Recommendations

Based on the above observations and those contained in the 2016 Submission, Privacy International proposes the following recommendations to the Thai government:

- Review the laws governing surveillance in Thailand, notably the Computer Related Crime Act, to ensure they comply with the International Covenant on Civil and Political Rights, including article 17.
- Ensure that all communication interception activities are only carried out on the basis of judicial authorization, and that the communications interception regime complies with the principles of legality, proportionality and necessity.
- Refrain from imposing indiscriminate obligations to retain communications data on companies and ensure that request to access of communications data is authorised by a judicial authority.
- Do not impose unlawful restrictions on the use of encryption and anonymity tools. Blanket prohibitions are neither necessary nor proportionate, and thus cannot comply with human rights law. The use of encryption promotes secure, private and

[26] https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
[27] Ibid.
[28] Ibid.

free communications, facilitating the realisation of rights to privacy and expression.

- Avoid all measures that weaken the security that individuals may enjoy online, such as the use of downgrade attacks that attempt to circumvent encryption on communications tools.
- Prevent arbitrary invasion of privacy, freedom of expression and peaceful assembly through the use of IMSI catchers. Government's use of IMSI catchers must be prescribed by law and limited to what necessary and proportionate to achieve a legitimate aim.
- Remove legal restrictions that prevent telecommunications companies from being transparent in their reporting about the requests they receive regarding access to user data, or discussing security issues.