# GLOBAL INFORMATION SOCIETY WATCH 2014

*Communications surveillance in the digital age*

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

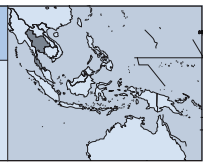
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

# THAILAND

When elephants fight: Communications surveillance on the rise in Thailand



**Thai Netizen Network**
Mishari Muqbil and Arthit Suriyawongkul
thainetizen.org

## Introduction

Thailand is presently going through a period of upheaval with the population split between two strong ideologies and those in power playing a zero sum game. Surveillance of the internet and other communication mediums has in the last decade been shown to have progressively greater importance to those in power. This can be seen by the 2007 Computer-related Crimes Act (CCA), brought into law by the previous junta; but more telling is the second version of the law, worked on by the subsequently elected civilian government, which focuses on criminal aspects but offers no safeguards to privacy and civil liberties.

The major application for mass surveillance has been in the form of logging internet use and blocking websites, but there have also been cases where law enforcement has requested cooperation from companies such as the social network company LINE in order to acquire chat transcripts to help them prosecute (non-political) criminal cases. However, recently, with the military takeover of the caretaker civilian government on 22 May 2014, surveillance has taken a more totalitarian form.

At 3:00 p.m. on 28 May 2014, people across Thailand could not use Facebook for about 55 minutes. At first it was announced by the National Council for Peace and Order (NCPO) spokesman that there was an issue with Facebook's own internet gateway.[1] But later it was revealed by the vice president and head of communications of Telenor Asia that its local subsidiary DTAC, the second-largest GSM operator in the country, "received a notification at 15:00 local time from the National Broadcasting and Telecommunications Commission of Thailand to restrict access to Facebook temporarily."[2] This incident would serve as a warning of things to come.

## Policy and political background

The CCA[3] stipulates penalties for various computer crimes including unauthorised access and spamming, but the clauses relevant to this report are Section 13, which penalises anyone who "disseminates sets of instructions developed as a tool used in committing an offence;"[4] Section 14, which penalises the spreading of vaguely defined "false computer data" (often interpreted to use for defamation charges), pornography and information that goes against national security (most notably defamation of members of the royal family); and "intermediary liability" in Section 15, which holds accountable the service provider who "supports or consents" to the crimes committed under Section 14. A service provider is broadly defined and can be anything from a satellite link provider to a coffee shop with free Wi-Fi access. Section 18 allows the authorities to demand traffic data from service providers without a court warrant. Article 25 of the Special Case Investigation Act (2004, amended 2008) also allows communication interception without notification.[5] Since 2012, every computer-related crime case is a special case under this Special Case Investigation Act.[6]

The new junta has chosen to act slightly differently. Their modus operandi seems to be the direct command of ministries and semi-governmental organisations to carry out tasks irrespective of existing legislation.

1 The Nation. (2014, May 29). No policy to block fBFB. *(2014, May). Retrieved June 13, 2014, fromThe Nation*. http://www.nationmultimedia.com/politics/%5CNo-policy-to-block-FB%5C-30234896.html.

2 Vals, M. (2014, June 9). Telenor says Thailand's recent Facebook outage was ordered by the government. *The Next Web*. thenextweb.com/asia/2014/06/09/operator-dtac-says-thailands-government-forced-shut-access-facebook

3 https://thainetizen.org/docs/thailand-computer-crime-act-2550 (original); https://thainetizen.org/docs/thailand-computer-crime-act-2550-en (English translation).

4 Under the previous section which can penalise security research as well as make dual use software illegal because the same set of computer tools that can be used to test for security flaws can also, by their very nature, be used to gain unauthorised entry.

5 Special Case Investigation Act (No. 2, amended February 2008). bit.ly/thaispecialcaseinvestigationact2008 (Thai and English translation)

6 Ministerial Regulation on Additional Special Cases according to Special Case Investigation Act (No. 2). bit.ly/morespecialcases2 (in Thai)

## Compliance with international benchmarks on surveillance

Since the military junta has taken power, there has been one high-profile arrest based on computer evidence. Sombat Boonngamanong, an activist who defied the junta, was tracked through his IP address.[7] It is of concern how this happened exactly, as Sombat's primary visible form of expression is through Twitter and Facebook. Both are HTTP Secure-enabled,[8] which should prevent any agents monitoring Thai internet traffic from tracing his account back to his address. We can only speculate that he made an error in operations security which resulted in his IP address being revealed, but we also cannot rule out the possibility of Facebook's cooperation with the junta or the existence of highly advanced surveillance capabilities.

If we look at this evolving situation in the context of the 13 International Principles on the Application of Human Rights to Communications Surveillance,[9] we see that Thailand has entered a precarious situation:

1. Legality – It can be argued that surveillance and intercepts are in effect legal, as laws have been written to give the state power to intercept. However, if it is implemented in such a way that citizens cannot foresee its application, then we fall short on this principle. Specifically in the case of DTAC above, the junta denied that such a block was ordered, and when Telenor's executive said otherwise,[10] the company felt threatened.[11]
2. Legitimate aim – It is arguable whether retaining logs of all internet traffic complies with a legitimate aim or not. One thing is certain: Sombat has been charged with "cyber crime as well as of inciting unrest and violating junta orders"[12] for not reporting to the junta when summoned, and for organising a flashmob.[13] This is definitely not a "legal interest that is necessary in a democratic society."[14]
3. Necessity – The provisions in the CCA require internet service providers (ISPs) to retain traffic data logs for up to three months to make them available for scrutiny by the state. The information, if requested, must be handed over to a competent officer without the requirement of any judicial oversight. Since the coup, however, it is unclear whether this applies anymore, as seen by the shutting down of Facebook with no reason provided nor an acknowledgement of the shutdown order.
4. Adequacy – Despite the blanket provisions and data logging requirements of the CCA, it does not seem to adequately fulfil all legal requirements. In 2013 Thai authorities reached out to LINE for access to online chat records.[15]
5. Proportionality – Here, it is enough to quote one analyst: "The Computer Crime Act has been criticised for its unclear provisions and harsh penalties."[16] This is by virtue of the fact that the language of the act is open to very broad interpretations, and some provisions prescribe a harsher penalty for a crime using a computer, compared to the same crime conducted without a computer.
6. Competent judicial authority – This is split into two parts: regular criminal and civil cases under the CCA, which are handled by the respective civilian courts, and national security cases, which are now handled by military courts.[17] The civilian courts have had some training and experience dealing with such cases (even though this is questionable).[18] However, it is certain that the military courts have had no experience dealing with CCA-related issues and are unlikely to base their judgements on human rights considerations.
7. Due process – Human Rights Watch (HRW) says it best: "The May 25 order [to try civilians in

7 Sawitta Lefevre, A. (2014, June 6). Thai junta tracks internet posting to capture protest leader. *Reuters*. uk.reuters.com/article/2014/06/06/uk-thailand-politics-idUKKBN0EH0KX20140606

8 HTTP Secure (HTTPS) is a standard for protecting internet traffic from intercepts, by encrypted communications using Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer protocol. More technical information can be found at www.tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html; for more information in plain English, watch this animation: youtu.be/DPYYwocbrFE

9 https://en.necessaryandproportionate.org/text

10 Vals, M. (2014, June 9). Op. cit.

11 Woodgate, E. (2014, June 11). Telenor threatened by Thai junta. *News in English.no*. www.newsinenglish.no/2014/06/11/telenor-threatened-by-thai-junta

12 Ngamkham, W., & Sattaburuth, A. (2014, June 11). Sombat now faces cyber-crime charge. Bangkok Post. www.bangkokpost.com/news/politics/414655/sombat-now-faces-cyber-crime-charge

13 Purnell, N. (2014, June). How Thai flash mobs avoid capture. *Wall Street Journal*. blogs.wsj.com/searealtime/2014/06/01/how-the-thai-flash-mobs-avoid-capture

14 https://en.necessaryandproportionate.org/text

15 Doksone, T. (2013, August 13). Thai police seek to monitor chat app for crimes. *AP*. bigstory.ap.org/article/thai-police-seek-monitor-chat-app-crimes

16 Charoen, D. (2012). The analysis of the Computer Crime Act in Thailand. *International Journal of Information and Communication Technology Research*, 2(6). esjournals.org/journaloftechnology/archive/vol2no6/vol2no6_7.pdf

17 Thai PBS. (2014, May 25). NCPO announces cases to be tried by military court. *Thai PBS*. englishnews.thaipbs.or.th/ncpo-announces-cases-tried-military-court

18 Pananda, A. (2012, May 15). Oddities abound in Amphon's trial and jailing. *The Nation*. www.nationmultimedia.com/politics/Oddities-abound-in-Amphons-trial-and-jailing-30181989.html


*Landing page that says: "This website contains content and information that is not appropriate and has been suspended by the Ministry of ICT."*

military courts] grants the military wide-ranging powers to prosecute civilians without basic due process protections, and prohibits defense counsel and rights to appeal."[19]

8. User notification – Passive surveillance happens without any indication to the user that it is happening. However, if users try to access a blocked URL, they are greeted with a landing page. There are several different landing pages depending on which state authority is responsible for the URL being blocked. A landing page by the Ministry of ICT is shown in Figure 1. In June 2014, the Thai Netizen Network found that the blocked URL landing page that is run by the Technology Crime Suppression Division (TCSD) is trying to imitate the Facebook login screen and collecting visitors' personal information. The TCSD block page has two graphics: one is a blue "Close" button, and the other is a "Login with Facebook" icon. If the second is clicked, visitors will be redirected to a TCSD Facebook application named "Login" and asked for permission to access their personal information stored in their Facebook profile – without any indication of where that data is being sent, or for what purpose.[20]
9. Transparency – There is no official list available of websites being blocked. In the past, after the 2006 coup, Freedom Against Censorship Thailand (FACT) made the block list available by leaking information from the official list given out to ISPs.[21] In 2007, FACT and the Campaign for Popular Media Reform petitioned for the block list using the 1997 Official Information Act[22][23] but eventually failed. The Official Information Commission said that revealing the block list could harm the website owners' reputations,[24] citing the "privacy" exemption of the Act. There are also no lists available of the number of requests to share data that an ISP has received, and when DTAC acknowledged being asked by the junta to block Facebook, it was threatened with punitive measures.[25]
10. Public oversight – There is little or no public oversight. Law enforcement officials are empowered to act on their own.
11. Integrity of communications and systems – Interception can put users in danger by creating a

19 Human Rights Watch. (2014, May 28). Thailand: Halt military trials, end arbitrary arrests. *Human Rights Watch*. www.hrw.org/news/2014/05/28/thailand-halt-military-trials-end-arbitrary-arrests

20 O'Brien, D. (2014, June 24). Thai junta used Facebook app to harvest email addresses. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/06/thai-junta-used-facebook-app-harvest-email-addresses

21 facthai.wordpress.com/data

22 FACT. (2007, February 11). Information Request Letter to MICT. *FACT*. facthai.wordpress.com/2007/02/11/info-request-letter-to-mict-eng

23 FACT. (2007, April 3). FACT files Freedom of Information complaint. *FACT*. facthai.wordpress.com/2007/04/03/fact-files-freedom-of-information-complaint

24 Freedom House. (2011). *Freedom on the Net 2011: Thailand country report*. www.freedomhouse.org/report/freedom-net/2011/thailand

25 Woodgate, E. (2014, June 11). Op cit.

convenient attack point. For example, for a while the proxy for True (a major ISP) was compromised, serving pop-up ads.[26] Since the attacker could wilfully manipulate web traffic data, it is unknown what else they may have done during this period. There is also little transparency on the side of the ISPs on the issue of who has access to the traffic information and how interception is happening. There is no consideration of whether the state would refrain from compelling the identification of users. Internet usage at internet cafés requires users to provide identification, which is recorded, before access is granted and, since the coup, it has been reported that vendors have been consulted to find a way where "[e]very Thai citizen will need to authenticate an internet logon session with a smart ID card."[27]

12. Safeguards for international cooperation – When the Thai authorities were getting in touch with the LINE corporation, there did not seem to be any resistance from the Thai division of the company. In Japan, where LINE's HQ is based, they were clear that a Japanese court order is required to comply in any way with state requests.[28] More telling is a recent incident where authorities decided to seek cooperation with social media providers to block content.[29] A trip was planned to Singapore to pursue the matter, but then was abruptly cancelled.[30]
13. Safeguards against illegitimate access – The CCA stipulates in Article 24 that if information gathered by a competent official is leaked by anyone, they can face a jail term of up to two years or be fined up to 40,000 baht (about USD 1,200), which could help deter neglect on the part of the officer. However, it is unclear how many safeguards apply under the coup administration.

## Conclusions

There is an African proverb that says, "When elephants fight, the grass gets trampled." The proverbial grass in this case is the right to access and distribute information, which is the scenario that is unfolding now in Thailand. It is doubtful that the situation will get better any time soon as this conflict intensifies; and if the current trend is any indication, it has the potential to get worse.

Based on the pattern of the junta making regular announcements for key individuals to report to them,[31] in combination with "Big Data's" ability to combine cross-referenced usage data from the logs retained from ISPs under the CCA, Prime Minister Yingluck's one million CCTV cameras in Bangkok,[32] and some form of Wi-Fi tracking[33] (possibly using government-sponsored free Wi-Fi access points),[34] it is not difficult to see how if left unchecked, Thailand can turn into a pervasive surveillance society.

## Action steps

The best strategy is to have a three-pronged approach:

- Educate – Inform the public about what criminal laws such as the CCA and surveillance mean for them. Give examples so that they can see what they stand to gain and lose from a surveillance society; then give them tools to protect their privacy and train them how to use them so that they may preserve their privacy if they choose to. This, however, should be done with care, as it is uncertain if the junta will consider such actions to be illegal in the future.
- Collaborate – At present there is no end in sight to the political conflict. However, it may be possible to convince the junta that if they had publicly released block lists and block orders, then their denial of the Facebook block would have been much more credible.
- Advocate – Activists must continue to advocate for strict controls over surveillance in Thailand and in the region, but it is unlikely that there will be the political will to do so any time in the near future.

26 Sambandaraksa, D. (2014, January 13). True Internet's proxy compromised. *Telecom Asia*. www.telecomasia.net/content/true-internets-proxy-compromised

27 Sambandaraksa, D. (2014, June 10). Thai junta holding the mother of all garage sales. *Telecom Asia*. www.telecomasia.net/blog/content/thai-junta-holding-mother-all-garage-sales

28 Leesa-nguansuk, S. (2014, May 31). LINE data request faces legal hurdles. *Bangkok Post*. www.bangkokpost.com/news/local/412749/line-data-request-faces-legal-hurdles

29 The Nation. (2014, May 29). Junta to seek cooperation from Facebook, LINE, YouTube to block 'inappropriate content'. *The Nation*. www.nationmultimedia.com/breakingnews/Junta-to-seek-cooperation-from-Facebook-LINE-YouTu-30234955.html

30 Purnell, N., & Chaichalearmmongkol, N. (2014, June 2). Thai junta says Facebook, Google meetings called off. *Wall Street Journal*. online.wsj.com/articles/thai-junta-says-facebook-google-meetings-called-off-1401689775

31 The Nation. (2014, May 24). Military junta summons 114 more to report today. *The Nation*. englishnews.thaipbs.or.th/military-junta-summons-114-report-today; The Nation. (2014, May 24). Junta summons 35 more figures. *The Nation*. www.nationmultimedia.com/breakingnews/Junta-summons-35-more-figures-30234505.html; Prachatai. (2014, June 5). Junta summons activists-lèse majesté suspects in exile. *Prachatai*. www.prachatai.com/english/node/4092

32 Thai PBS. (2013, November 5). Yingluck to open Miracle Eye project in Bangkok today. *Thai PBS*. englishnews.thaipbs.or.th/yingluck-open-miracle-eye-project-bangkok-today

33 Cunche, M. (2013). I know your MAC address: Targeted tracking of individual using Wi-Fi. *International Symposium on Research in Grey-Hat Hacking - GreHack (2013)*. hal.archives-ouvertes.fr/docs/00/85/83/24/PDF/Wi-Fi_Stalking.pdf

34 Government Public Relations Department. (2012, September 1). Opening over 20,000 free WiFi hotspots in Bangkok. Press release. thailand.prd.go.th/view_news.php?id=6070&a=4