PRIVACY INTERNATIONAL

WHO'S THAT KNOCKING AT MY DOOR?

Understanding Surveillance In Thailand

Acknowledgements

Privacy International wants to thank Victor Clark for his assistance. We also want to thank the individuals who have helped us with this investigation and who cannot be named. A handful of these individuals took significant risks to share information with us, for which we are very grateful.

WHO'S THAT KNOCKING AT MY DOOR?

Understanding Surveillance In Thailand

January 2017

PRIVACY INTERNATIONAL

www.privacyinternational.org

Table of Contents

Executive Summary

In May 2014, Thailand experienced a military coup.[1] As the army took over the country, Facebook was shut down on May 28th to eventually be restored just 30 minutes later.[2] Over the following months, a debate would ensue over what actually happened. Was the government trying to cut the main communication medium of Thai protesters? Or was it a "slight technical failure" as the army spokesperson told the New York Times?[3]

The move at first appeared typical of Thailand's long history of internet censorship, including removal of content, and social media monitoring.[4] It reflected the Thai government's desire to control what the population can see and say online, a practice dating back to the early days of the internet.[5]

However, scratch the surface and what is revealed is a complex web of online surveillance, aided by the Thai government's control of the internet infrastructure; a close relationship with internet service providers (ISP) and a 'revolving door' between government and telecommunications companies, whereby former politicians or family members hold key positions.

There is no evident impetus to formalise procedures to obtain information and support from ISPs (including removing content). Instead, as set out below and exemplified in what we know of the Facebook shut down, the Thai government relies upon informal relationships with ISPs, opting for a 'friendly knock on the door' of the telecommunications providers. Added to this is the ease of access that can result from revolving door politics, as exemplified by the fact that AIS was previously owned by former prime minister Thaksin Shinawatra, and anti-Thaksin generals subsequently being appointed as advisors to Charoen Pokphand, the corporation that owns the telecommunication company True.

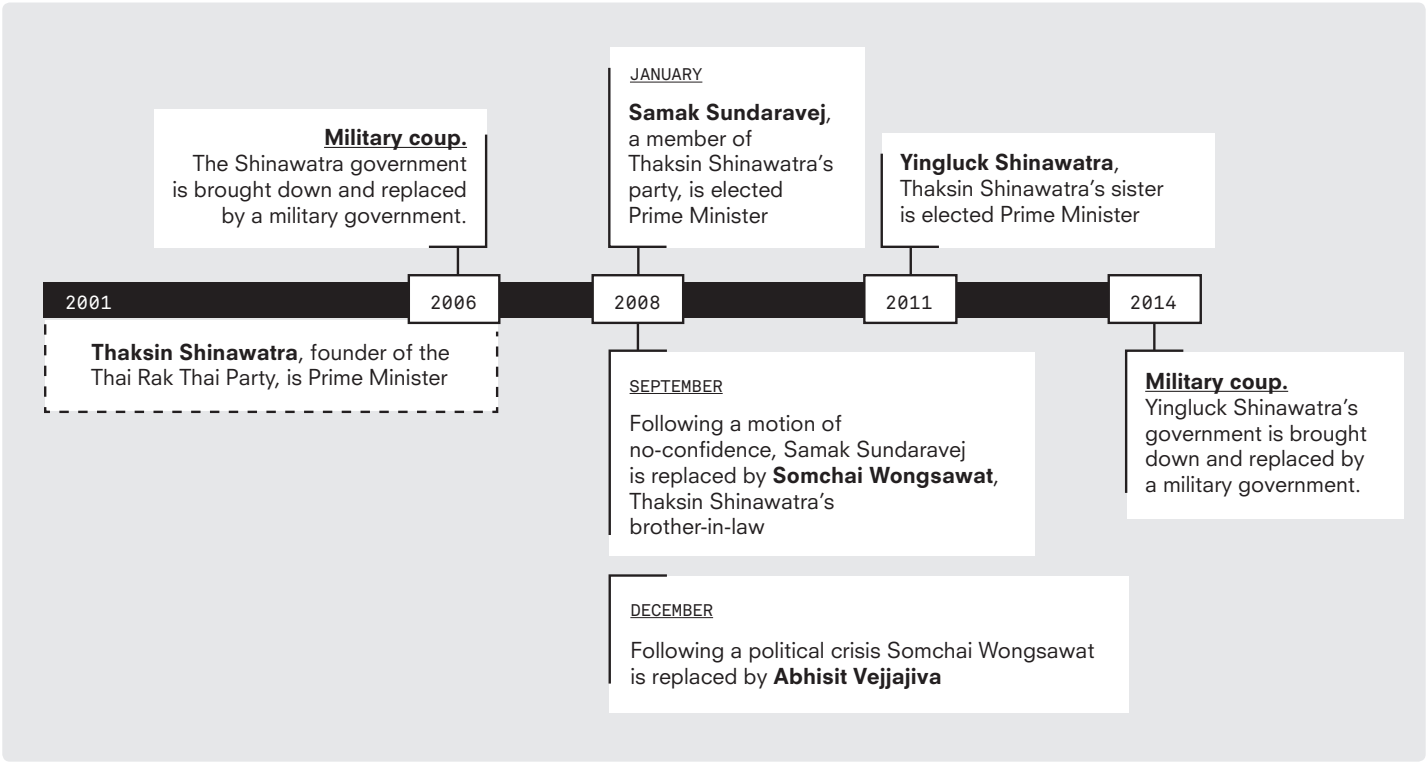
We refer to this context and the lack of a rigorous legal framework – that does not encourage or allow companies to resist or deny requests for access – as 'door-knocking surveillance'.

In the first part of this report, we examine the issues above and what was really at stake behind the Facebook shut-down: the Government's attempts to circumvent encryption.

In the second part of the report we then look at a separate aspect of control – the extent and growth of online government surveillance which does not rely upon

1 http://www.bbc.co.uk/news/world-asia-27517591
2 http://qz.com/214173/the-thai-junta-briefly-blocked-facebook-in-a-dry-run-for-a-social-media-blackout/
3 https://twitter.com/thomasfullerNYT/status/471592305011351552
4 https://www.privacyinternational.org/node/935
5 https://www.privacyinternational.org/node/967 The NECTEC is a government agency in charge of IT policy planning http://www.nectec.or.th/home/

relationships or control of ISPs, but is instead based on more direct interventions. This includes how the government is using 'downgrade attacks' to break the encryption of email communications and the purchasing of IMSI catchers to intercept phone data and communications. Just like door-knocking surveillance, many of these techniques are low cost, a form of cheap surveillance. While Thailand has also invested in expensive and sophisticated surveillance technologies, we believe it is important to illustrate another concerning reality of surveillance: governments can sometimes access content of communications with a small budget.



Door-Knocking Surveillance

ISPs, the government and the internet: the revolving doors of a family business

The Thai government has exerted strong control over the internet through its ownership of the national infrastructure in the early days of the internet. In Thailand, the internet became accessible to the general population in December 1994 when the telecommunications regulator, the Communications Authority of Thailand (CAT), the incumbent operator, the Telephone Organisation of Thailand (TOT) and the National Science and Technology Development Agency (NSTDA), the legal entity of the National Electronics and Computer Technology Centre[6] (NECTEC), joined forces to create the Internet Thailand Company (ITC), a state owned ISP.[7] Both CAT and TOT are state owned companies[8] and the ITC was therefore an entirely state-owned enterprise.[9]

By August 1995, CAT, which acted as the regulator in this new industry, had approved four other private ISPs: KSC Comnet, Loxley Information (LoxInfo), Wattachak Group and Advanced Research Group.[10] CAT had defined strict rules for new ISPs, in order to both limit the number of companies deciding to set themselves up as ISP and also guarantee CAT would maintain control over them. Among other rules, ISPs were required to become joint ventures with CAT and grant it 35 per cent of their total equity. They also had to buy their leased circuit[11] from CAT, grant CAT ownership of their equipment and agree to have CAT employees working in the ISP and give them the right to veto decisions made by the board. Thus, while the ISPs were privately owned on paper, the state maintained a tight control over them via CAT.[12]

At the time, there were serious concerns regarding the control CAT had over the emerging internet sector. In particular, there were public concerns about the high price of subscribing to the internet. The conflict of interest that the situation presented was also raised by Thaweesak Koanantakool, an academic who would become NECTEC director, who in 1997 commented on the unhealthy nature of having an institution like CAT, that is at the same a time both a telecommunications regulator and a telecommunications operator.[13]

At the time, CAT also controlled the International Internet Gateway[14] and the local exchange points.[15] [16] Today, the major ISPs are AIS, True, TOT, 3BB and DTAC.

---

6 The NECTEC is a government agency in charge of IT policy planning http://www.nectec.or.th/home/

7 Palasri, S, Huter, S.G, Wenzel, Z, The History of the Internet in Thailand, 1998 ftp://ftp.cs.ait.ac.th/pub/pdf/ENPRINT.PDF

8 https://privacyinternational.org/node/740

9 https://privacyinternational.org/node/740

10 http://www.nectec.or.th/users/htk/milestones.html

11 Leased circuit: the actual physical wires

12 Palasri, S, Huter, S.G, Wenzel, Z, The History of the Internet in Thailand, 1998 ftp://ftp.cs.ait.ac.th/pub/pdf/ENPRINT.PDF

13 ftp://ftp.cs.ait.ac.th/pub/pdf/ENPRINT.PDF

14 International Internet Gateway: a device that sends internet traffic to an ISP in another country

15 Local exchange points: shared service platforms or hubs where different networks connect technology

16 ftp://ftp.cs.ait.ac.th/pub/pdf/ENPRINT.PDF

There appears to be ten exchange points run by ISPs, cloud computing services and gateway service providers.[17]

In terms of phone services, TOT was originally the first and only provider of the telecommunications network. Throughout the 1980s and 1990s private providers started emerging: thirty concessions were granted to private investors.[18] In 2002, TOT and CAT became corporations: TOT became TOT Public Company Limited[19] and CAT became CAT Telecom.[20] Despite becoming corporations, the two companies are still today part of the Ministry of Information and Communications Technology (ICT), as illustrated in the Ministry's organisational chart.

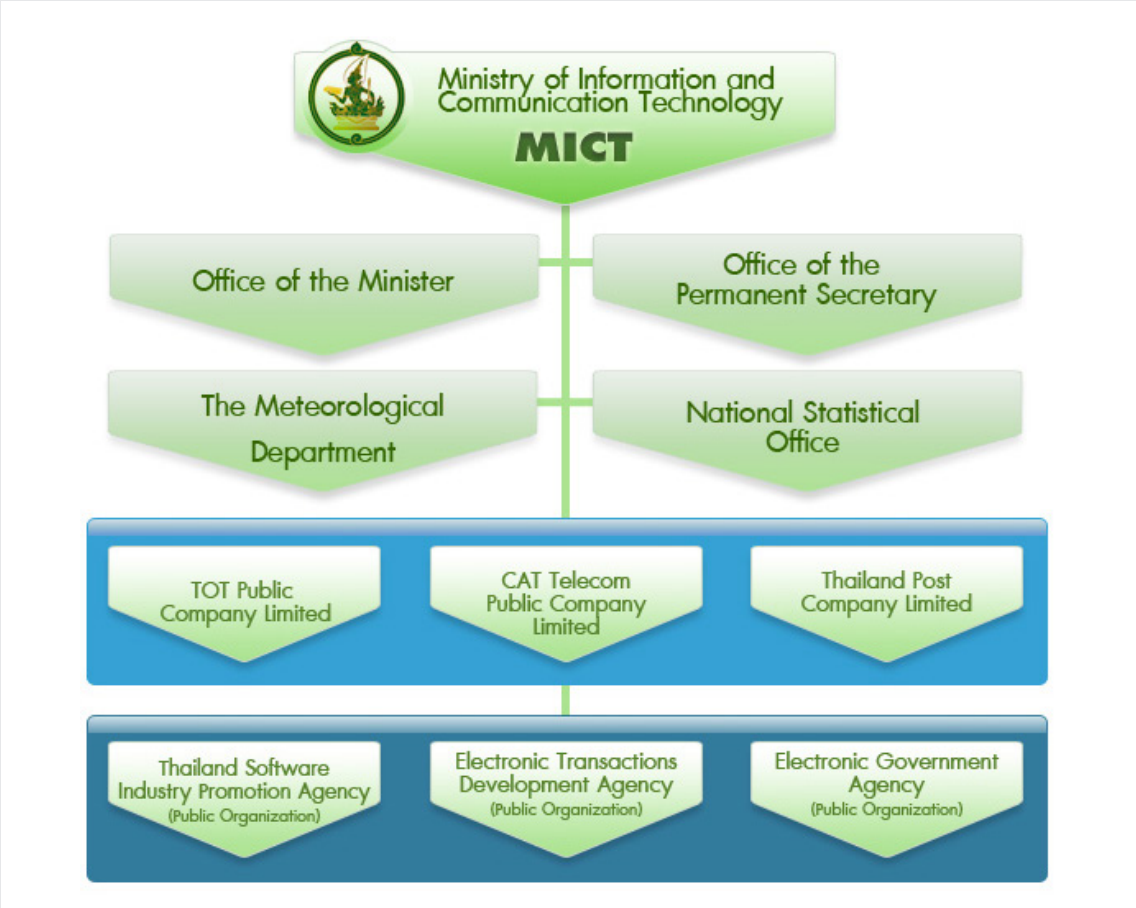


Figure 1 Ministry of Information and Communications Technology's organisational chart. Image from the Ministry of Information and Communication Technology. http://www.mict.go.th/view/10/About%20Us

In 2010, a new Act called 'Organisation to Assign Radio Frequency and Regulate the Broadcasting and Telecommunications Services'[21] set up an auction system to assign various segments of the frequency spectrum to the different providers. Within the 3G and 4G spectrum some segments offer better coverage than others and

17 http://internet.nectec.or.th/webstats/home.iir
18 http://userpage.fu-berlin.de/~jmueller/its/conf/porto05/papers/Gasmi_Recuero.pdf
19 https://en.wikipedia.org/wiki/TOT_Public_Company_Limited
20 https://en.wikipedia.org/wiki/CAT_Telecom
21 http://www.jfcct.org/files/2012/10/Frequency-Act-2010.pdf / http://www.aseanlawassociation.org/Thai_telecomm_law.pdf accessed 12.12.2016

telecommunication providers therefore compete for the best segments, to be able to offer the best services to their customers.[22]

Being originally the only telecommunications provider, TOT was a single point of contact for interceptions of communications requests.

The revolving doors of a family business

While CAT Telecom and TOT are state-owned, successive Thai governments over the past few decades have maintained close relationships with private telecommunication companies and ISPs through appointments which starkly exemplify the revolving door between the government and the private telecommunications sector.

For example, Advanced Info Service (AIS), which is now the largest GSM (Global System for Mobile Communications) cell phone operator - with 46.5% market share of the mobile network market - now belongs to TEMASEK,[23] a commercial investment company owned by the Government of Singapore.[24] However, it was founded in 1986 by Thaksin Shinawatra, who became Deputy Prime Minister nine years later and was prime minister from 2001 to 2006. His government was overthrown by a military coup but his sister, Yingluck Shinawatra, regained power from 2011 to 2014, when she was also overthrown by another military coup. Thaksin sold AIS in 2006, as he went into exile.[25] During the Shinawatra government, Thaksin's brother-in-law, Priewpan Damapong, was chief of the police.[26]

The 2006 coup revealed the use of telecommunications by government to spy on civilians and the complications that come with a new administration that was opposed to the previous Government. The interim military government claimed companies had been tapping communications of those in charge of investigating corruption cases related to the Thaksin government. They warned telecommunication companies who had been tapping customers that they could lose their licences. CAT was at the time reportedly in possession of illegal tapping equipment and another unnamed private company was also in possession of such equipment.[27]

The Ministry of ICT had specifically ordered AIS to report any tapping request they may have received from within their company hierarchy.[28]

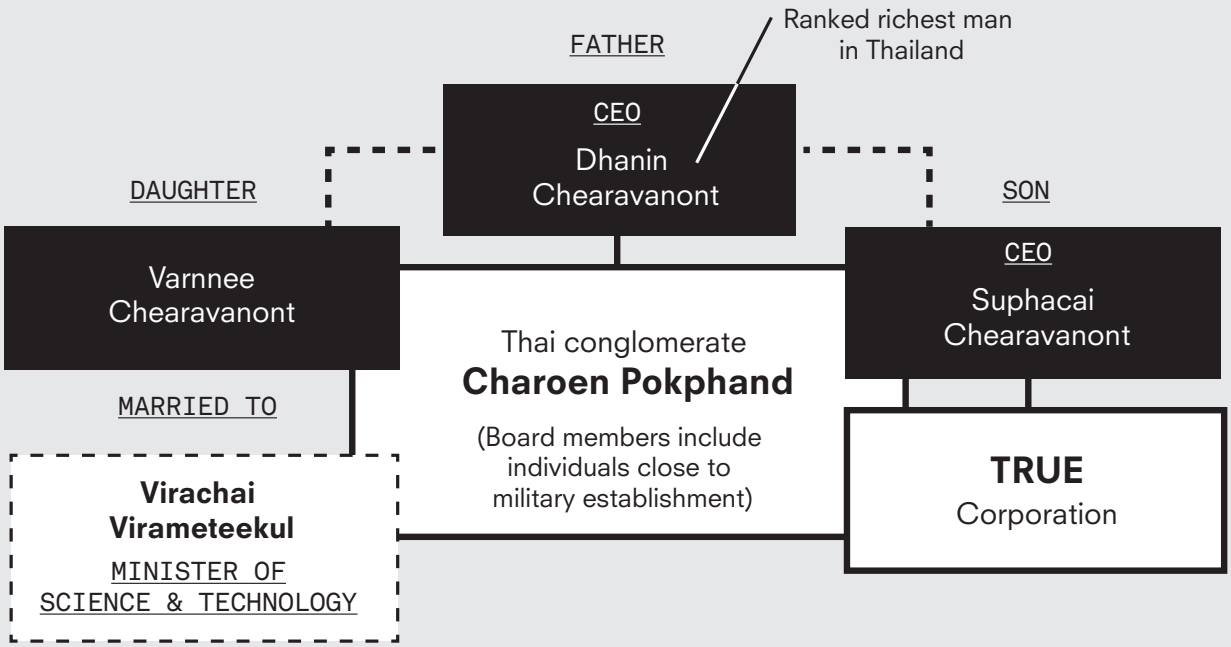
True – another major actor with 24.26% of the market – belongs to the Thai conglomerate Charoen Pokphand.[29] Charoen Pokphand is owned by the Chearavanont family. Dhanin Chearavanont is currently the Chairperson and CEO of Charoen Pokphand and his son Suphacai Chearavanont is the president and CEO of True.[30]

22 http://www.jfcct.org/files/2012/10/Frequency-Act-2010.pdf
23 https://en.wikipedia.org/wiki/Advanced_Info_Service
24 http://www.temasek.com.sg/abouttemasek/corporategovernance
25 http://web.international.ucla.edu/asia/article/37744
26 http://www.bangkokpost.com/learning/advanced/304384/police-chief-under-fire-for-hong-kong-trip
27 http://www.international.ucla.edu/asia/article/61654 (Bangkok Post)
28 http://www.international.ucla.edu/asia/article/61654 (Bangkok Post)
29 http://www.forbes.com/profile/dhanin-chearavanont/ and http://www.mobileworldlive.com/asia/asia-blogs/blog-thailands-ais-to-participate-in-uncontested-900mhz-re-auction/
30 http://www.cpgroupglobal.com/en/aboutus.php

Charoen Pokphand contains some of the largest companies in Thailand: both True and Charoen Pokphand Foods are featured in the SET50 Index of the biggest Thai companies.[31] Dhanin Chearavanont was ranked the richest man in Thailand by Forbes in 2015.[32]

According to a Capital Profile report, the Chearavanont family is close to the military government that has been in power since the 2014 coup. Their report reveals that the board of Charoen Pokphand contains people affiliated with the military establishment. Anti-Thaksin generals have been appointed as advisors. Dhanin Chearavanont's daughter was married to Virachai Virameteekul, an anti-Thaksin politician who was Minister of Science and Technology from 2010-11.[33]

Chareon Pokphand does not just dominate the telecommunications sector. In July 2016, Charoen Pokphand announced they would work with the government to invest in the 'digital economy' and in particular the development of high speed railway. Charoen Pokphand was invited to build the railway by the Prime Minister. The group is also working with the Ministry of Science and Technology to develop biotechnology projects.[34] The government also announced that Charoen Pokphand had expressed interest in investing in sectors including food innovations, agricultural research and robotics.[34] In 2015, True paid a record price of $3 billion to purchase blocks of 4G spectrum at the auction.[36]



http://www.cpgroupglobal.com/en/aboutus.php

31 http://aseanup.com/top-50-companies-from-thailand-set50/
32 https://web.archive.org/web/20160321050316/http://www.forbes.com/thailand-billionaires/gallery
33 http://www.mergermarket.com/pdf/CapitalProfileSpecialReport_ThaiFamilyPoliticalAffiliations%20(2).pdf
34 http://www.asianews.network/content/thailands-cp-group-sees-future-high-tech-industry-21394
35 http://nwnt.prd.go.th/CenterWeb/NewsEN/NewsDetail?NT01_NewsID=WNECO5907010010008
36 http://www.forbes.com/profile/dhanin-chearavanont/ and http://www.mobileworldlive.com/asia/asia-blogs/blog-thailands-ais-to-participate-in-uncontested-900mhz-re-auction/

Those deals illustrate the extent of the relationship between Charoen Pokphand and the government, with the latter relying on the former to finance its projects. This proximity is another example of revolving door politics in Thailand.

Freedom of expression, auction and encryption: the truth about the Facebook shut down

The shut down of Facebook reveals both the carrot and stick approach to controlling the internet.

As of October 2015, there were 86 million mobile phone subscriptions in a population of 67 million people. Of the total handsets sold in the first quarter of 2015, 75.5% were smartphones.

Six days after the military coup, on May 28th 2014, Facebook was shut down for 30 minutes at 15.35.[37] A the time Thailand counted 28 million Facebook users. Speaking to Reuters, Surachai Srisaracam, the permanent secretary of the Ministry of ICT, said: "We have blocked Facebook temporarily and tomorrow we will call a meeting with other social media, like Twitter and Instagram, to ask for cooperation from them. Right now there's a campaign to ask for people to stage protests against the army so we need to ask for cooperation from social media to help us stop the spread of critical messages about the coup."[38]

However, the government quickly changed the narrative. An army spokesperson told a New York Times reporter the very same day that Facebook had been down due to a "technical glitch."[39] A representative of the military government also made an announcement on state television to deny they had anything to do with the shut down and blamed technical problems.[40]

Sirichan Ngathong, another spokesperson for the military government, also said to the media: "We have no policy to block Facebook and we have assigned the ICT Ministry to set up a supervisory committee to follow social media and investigate and solve problems. There's been some technical problems with the internet gateway." She added they were working with ISPs to fix the problem.[41]

Surachai Srisaracam, who had originally announced that the Government had blocked Facebook backtracked on his announcement and said: "blocking social media is usually the best way to get people to start talking about the ban, usually on social media itself."[42]

The military government may indeed have tried to ban Facebook to shut down dissent. However, our sources suggest that the strategy was not a simple Facebook shut down, but an attempt to circumvent SSL (Secure Socket Layers) encryption.

37 https://www.techinasia.com/thailand-social-media-stats-28-million-facebook-45-million-twitter-17-million-instagram
38 http://in.reuters.com/article/thailand-politics-facebook-idINKBN0E80U520140528
39 https://twitter.com/thomasfullerNYT/status/471592305011351552
40 https://news.vice.com/article/thailands-military-denies-briefly-banning-facebook
41 http://in.reuters.com/article/thailand-politics-facebook-idINKBN0E80U520140528
42 https://news.vice.com/article/thailands-military-denies-briefly-banning-facebook

In addition to the use of the door-knocking strategy to request that ISP's block access to Facebook, a source from the telecommunications sector we have spoken to was approached by the military government and asked if they could get in touch with Facebook to ask them to route the traffic over http instead of the more secure https,[43] in order to circumvent the encryption. The information was confirmed by a person close to the ministry of ICT.

As no evidence suggesting the Thai government had managed to circumvent encryption at that time, we assume the attempt was not successful.

The use of the door-knocking strategy to shut down Facebook transpired from a rare instance of outspokenness by DTAC, the telecommunication company owned by the Norwegian Telenor Group. DTAC went public on June 9th 2014 and released a press statement admitting that they had been requested to restrict access to Facebook:

"Telenor Group can confirm that on Wednesday 28 May DTAC received a notification at 15:00 local time from the National Broadcasting and Telecommunications Commission of Thailand to restrict access to Facebook temporarily.

"This restriction, which was implemented at 15:35, potentially had impact on DTAC's 10 million Facebook-using customers."[44]

Press release from DTAC

The statement provoked the ire of the government and especially the National Broadcasting and Telecommunications Commission (NBTC). "Now Thailand is under martial law, [...] so everyone needs to respect the martial law," said Settapong Malisuwan, chairman of NBTC's telecom committee two days later. Settapong denied the existence of any such notification.[45] Talking about Telenor, Settapong said: "It is inappropriate and disrespectful. If Thailand has such great problems, Telenor should invest in another place"[46] and "If they want to continue investing in Thailand, it should respect Thai law."[47]

Settapong also called for Telenor to be placed under greater scrutiny and hinted at the ownership regulations that ban foreign firms from owning more than 49% of a telecommunications company. As of 2014, Telenor owned 42% of DTAC's shares.[48]

43 HTTPS: secure protocol that delivers web traffic encrypted by SSL/TLS
44 http://thenextweb.com/asia/2014/06/09/operator-DTAC-says-thailands-government-forced-shut-access-facebook/
45 http://www.nationmultimedia.com/news/business/corporate/30236007
46 http://www.independent.co.uk/news/world/asia/leading-telecoms-firm-apologises-to-thai-junta-after-facebook-blocked-9543096.html
47 http://www.nationmultimedia.com/news/business/corporate/30236007
48 http://www.independent.co.uk/news/world/asia/leading-telecoms-firm-apologises-to-thai-junta-after-facebook-blocked-9543096.html

A week after releasing the statement, DTAC was forced to publicly apologise, although it is interesting that their statement did not actually withdraw the claim that they had received an order to shut down Facebook:

"Earlier this week, Telenor Group released information to both international and Thai media in relation to an incident that occurred on the 28th May. These actions damaged the public image of the National Broadcasting and Telecommunications Commission (NBTC) and the National Council for Peace and Order (NCPO), which regulate the telecommunication industry and oversee the security of the nation as a whole, respectively. The executives of Telenor Group and Total Access Communication (DTAC) regret what happened. [We realise that] Thailand is currently under the administration of the NCPO. Thailand requires unity among its people and its many foreign friends who are operating in the country. The executives of Telenor Group and DTAC would like to take this opportunity to apologize to the NBTC and NCPO. We will continue to strengthen our dialogue with the people of Thailand for the betterment of the country."[49]

Press release from DTAC

Spectrum auctions

A source within the NBTC explained to Privacy International how the spectrum auctions are another way to keep telecommunication companies that provide both mobile and wired services under control: "Some segments of the spectrum work better than others so companies want to be in the good books of the government. Thai corporations are used to respecting the government, DTAC is probably a bit different but if they were completely independent they would be blacklisted. Right now, True has more negotiating power. Dhanin Chearavanont is a billionaire and he supports every government financially."

In June 2014, the Thai government postponed the 4G auction that was planned for August that year.[50]

49 http://www.nationmultimedia.com/news/breakingnews/aec/30236306

50 http://www.developingtelecoms.com/business/regulation/5335-thai-4g-auctions-suspended.html

The auction was eventually held on December 2015. True turned out be the winner of the auction, having bet the equivalent of three billion dollars for an extra 4G spectrum licence.[51] [52]

It is clear that there are many loose ends in this story. What the limited information we do know demonstrates is that the government will be ready to go to a company such as Facebook to request the removal of encryption, and they will go to ISPs to shut down access to social media more widely. And where an ISP, such as DTAC speaks out publicly, they will face threats and consequences.

Google, YouTube, Facebook and Line on the Thai government's shopping list

Thai governments past and present have not limited their activities solely to domestic ISPs and instead looked to target international social media platforms directly.

Pisit Pao-in – deputy chairman in charge of media reform, who was at the time commander of the Technology Crime Suppression Division (TCSD) – was public about his attempts (and failures) to get international social media platforms based in the West to cooperate with the TCSD.

"We have been talking to them the operators of social media a lot, but they do not want to cooperate...I won't let them go if they make any mistakes."[53]

Since 2013 the Japanese messaging application Line has been the focus of the Thai governments' attention. The Shinawatra government was trying to obtain access to communications on Line,[54] which is used by 33 million Thai people.[55]

Pisit Pao-in has also asked Line Corporation to assist him with obtaining communications of Thai citizens. It is unclear what the outcome of the request turned out to be. While Pisit Pao-in claimed he had spoken to Line and announced that the company was willing to cooperate with Thai authorities, Line on the other hand said they had received no official requests from the Thai police and that they neither collect nor store any user's information or messages. Pisit Pao-in argued that they had made that announcement to escape criticism from their customers.[56]

Facebook has also been a core target of the military government, which is trying to hunt for lèse-majesté content (speaking ill of the monarchy).[57] In December 2014, they attempted to meet with representatives from Facebook to discuss lèse-majesté and how the California-based social network could help them to track 'undesirable content'. However, Facebook at the time reportedly turned down the invitation, claiming no representatives were available.[58]

51 http://www.reuters.com/article/thailand-telecoms-4g-idUSL3N14752C20151218

52 While DTAC was eventually allowed to participated their bid turned out too low for them to win any licence.

53 http://www.nationmultimedia.com/news/politics/aec/30212462

54 https://privacyinternational.org/node/967

56 http://www.bangkokpost.com/print/1007253/

57 http://www.bangkokpost.com/tech/world-updates/364593/government-denies-all-social-network-chat-logs-will-be-monitored

58 https://privacyinternational.org/node/935

The death of the Thai King Bhumibol Adulyadej on 13 October 2016 has, however, marked a new period in the fight against lèse-majesté discourse online. The social surveillance described in a previous Privacy International analysis[59] has considerably stepped up.[60] The government has set up an "Army Cyber Centre" dedicated to monitoring news deemed critical of the royal family, and the army chief asked the Thai people to "be cautious before sharing news and online contents."[61]

The military government has also turned once again to international companies, asking them to monitor lèse-majesté content. The day after the King's death, Takorn Tantasith, secretary-general of the NBTC, announced he had sent ISPs and web-administrators of social media (including Facebook, Twitter, YouTube and Line) an order to monitor "inappropriate content" on their channels and remove it as soon as possible. Takorn Tantasith threatened to prosecute any ISP that did not comply.[62]

Unlike on previous occasions, companies have – for the most part – appeared willing to cooperate. According to the Nation, Facebook executive Alvin Sheng Hui Tan allegedly sent two letters to the Minister for Digital Economy and Society saying they were willing to collaborate with Thai authorities regarding lèse-majesté content. "Government entities can submit reports to Facebook about content that is believed to violate local law. If, after careful legal review, we find that the content is illegal under local law, we will restrict such content as appropriate," Tan said in the letter.[63]

Prajin was not as successful with Line. He announced they had agreed to set up a steering committee to investigate reports of lèse-majesté, which would cooperate with the Thai embassy in Japan, the NBTC and INTERPOL. However, after Prajin's announcement Line denied being able to monitor or block user content, arguing the content is encrypted and cannot be viewed by Line.[64] Line has in fact implemented end-to-end encryption in September 2015 and have made it a default setting.[65]

Meetings between the Ministry for Digital Economy and Society, the TCSD, the NBTC[66] and Ann Lavin, Director of Public Policy of Google's Southeast Asia and Greater China office was also held at the Government house to discuss ways of blocking websites and video clips deemed defamatory or offensive to the Thai monarchy. Google allegedly agreed to set up an ad hoc team in the US to monitor alleged lèse-majesté content. The team would include Thai nationals. Google also allegedly agreed to adjust their complaint form in Thai to make it easier for Thai people to report content.[67]

59 http://www.prachatai.com/english/node/4644
60 https://privacyinternational.org/node/935
61 http://prachatai.org/english/node/6672?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29
62 http://prachatai.org/english/node/6685?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29
63 http://prachatai.org/english/node/6655?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29
64 http://www.nationmultimedia.com/news/national/30298930
65 http://prachatai.org/english/node/6690?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29
66 https://linecorp.com/en/pr/news/en/2016/1464
67 http://prachatai.org/english/node/6677?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29

Successive transparency reports from Google have shown Thailand has been requesting users' data since 2013 but the company has never granted any of those requests.[68] Requests to remove content were on the other hand agreed in 85% of cases.[69]

A legal framework for the door-knocking policy

The government's activities are assisted by a permissive legal framework. 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 officer called 'Peacekeeping Officers'. In their government access report, which includes DTAC, Telenor hints at the issues that arise from these powers, in particular as the law remains vague.[70]

Peacekeeping Officers are in charge of preventing and suppressing offences related to lèse-majesté, internal security, firearm regulations and "any violation of any other orders issued by the NCPO."[71]

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.[72] This mention is particularly relevant when it comes to the type of information Telenor can include in its transparency reporting on Thailand.[73]

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.[74]

At the time of writing martial law is still in place in the Southern regions of Thailand (Pattani, Yala, Narathiwat and Songkhla),[75] where there have been ongoing tensions since 1958, relating to the Muslim populations demanding their independence.[76] Thus, the military government "may require from any person or company any conveyance, beast of burden, provisions, arms, instruments and tools for use in military service at

68 http://prachatai.org/english/node/6668?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+prachataienglish+%28Prachatai+in+English%29
69 https://www.google.com/transparencyreport/userdatarequests/TH/
70 https://www.google.com/transparencyreport/removals/government/TH/?hl=en
71 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
72 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
73 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
It is worth noting that DTAC does not provide any data on government request for communication data, lawful interception network shutdowns, content restrictions and content distribution in both their 2014 and 2015 Authority Requests Disclosure Report.
74 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
75 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
76 http://uca.edu/politicalscience/dadm-project/asiapacific-region/thailandmalay-muslims-1948-present/

that time."... It may also "cause provisional seizure of all things so as to prevent the enemy from using them or for the benefit of military service".[77] Applied to the context of telecommunication providers this suggests the military government may obtain easy access to their infrastructure in order to surveil communications in the region.

While the military coup seems to have marked a new era of even stricter control over telecommunication companies, regulations in place prior to the coup were already enforcing strong government control. An example of this was the Telecommunications Business Act B.E. 2544 (TBA), which was introduced in 2001. In cases of emergency the TBA grants the NBTC wide powers to "maintain public order, national security or economic stability or to protect public interests." As part of those powers the NBTC can "take possession of and use the devices and equipment of the licensed telecommunications provider, or authorise a state agency to temporarily take charge of a telecommunications provider's services, or order the telecommunications business or his/her employees to take a specific action until the end of such emergency or necessity." This regulation is still in place.[78]

77 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf
78 https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf

Low-Budget Surveillance

We have observed in the first part of this report how successive Thai governments were using their personal connections with telecommunications companies and service providers – as well as a legal framework favourable for them – to potentially gain access to communications. However, Thailand has developed other ways to surveil its population cheaply.

Circumventing encryption: a not so trustworthy root certificate

Despite their best efforts to inspect packets and tap cables, the Thai government are still faced with the challenge of trying to access encrypted communications, as demonstrated through the failed attempts to get staff at Line to hand over data from the encrypted messaging app. One way the Thai government may have tried to address the issue would have been misusing their root certificate and impersonating the intended website to intercept the communications and passwords.

A root certificate is the most trusted certificate issued by a "certificate authority".

A certificate authority's role is to vouch for the authenticity of the purported domain holder. The certificate issued is signed by the CAs own key to demonstrate they have conducted a review of the owner.

The certificate authorities that control root certificates and the certification process are often companies but they may also be nation states or branches of the state.

When a root certificate issues a certificate for a third party who is not the owner or operator of the domain, it can lead to security problems for all those who visit the site because the invalidly issued certificate will be trusted. This is particularly problematic when an entity that controls access to the internet is using the maliciously issued cert. This allows for interception of the content of apparently secure communications and/or the injection of false or malicious content such as malware.

Some governments, such as the regime of Ben Ali in Tunisia, have used this method to spy on citizens. It is known as a

man-in-the-middle attack, using impersonation of the intended site and the falsified cert.[79]

The reason the redirection toward a malicious website is not detected is because a user's computer trusts the root certificate. Operating systems like Mac or Windows come with a series of trusted root certificates by default. As long as your operating system trusts a root certificate it can be impossible to detect a malicious use. In addition, web browsers can have their own independent certificate stores that may not match that of the operating system. This can be good and bad. If an OS does not trust a given certificate but the browser does, the user will be unlikely to be given a warning about an untrustworthy site. However, the more likely scenario is that a browser will trust a subset of those certs trusted by the OS. Of course, other services, such as email and VPN may rely on the OS trust store and therefore be vulnerable to attacks that SSL web traffic may not.

Privacy International has noticed Mac OS X does not include the Thai national root certificate by default. On the other hand, Windows does include it.

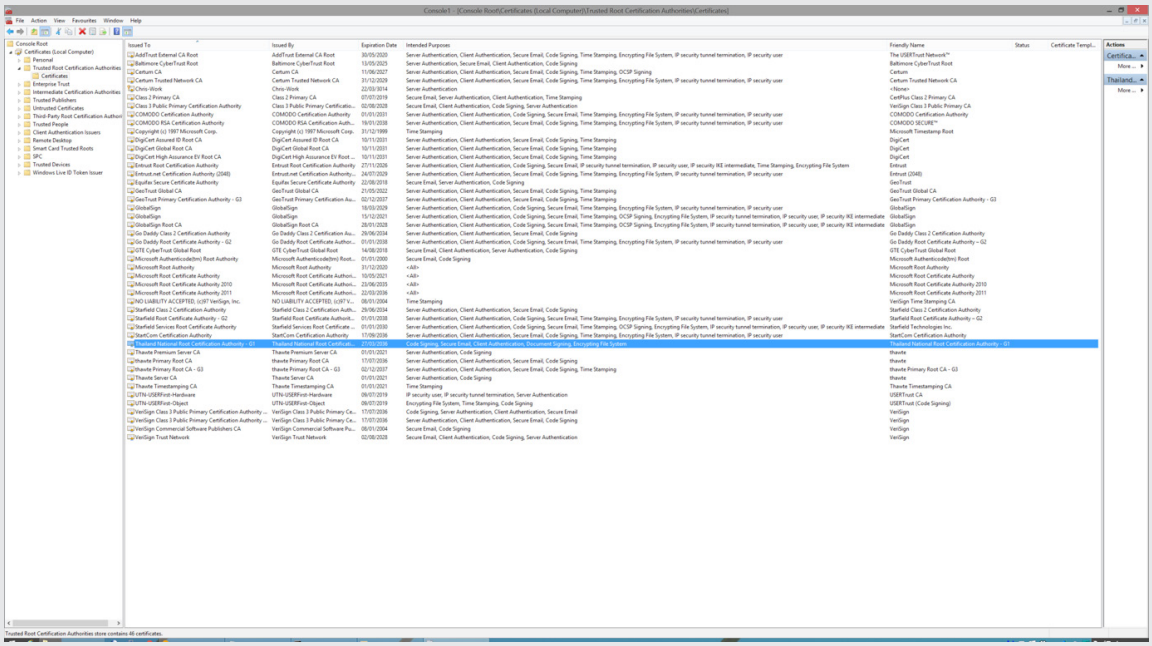


Figure 2 Thai national root certificate is trusted by default. The image above shows its intended purposes. Screen capture by Privacy International.

[79] The Ben Ali regime in Tunisia famously did so when the Arab Spring protest started. Websites that looked exactly like Facebook, Gmail and Yahoo were created to steal the username and passwords of Tunisian users who entered their credentials thinking they were accessing the 'real' Facebook, Gmail and Yahoo.

This discrepancy raises obvious concerns and illustrates how not all users are equal when it comes to security. If the Thai government were to attempt to use their certificate maliciously a Mac user would be more likely to get an alert from the browser or OS that the connection is untrusted, while a Windows user on the other hand would be more exposed. Windows users can of course remove certain certificates and use a different browser to avoid being redirected to malicious sites.

It is also worth noting that Microsoft is the only company that provides an operating system that has trusted this certificate. Neither Firefox nor Chrome – nor any certificate authority entitled to sign a root certificate – have trusted it.[80]

Purpose	Context (Version) Shortest Path						
	Apple (2016-09-22)	Microsoft (2016-09-16)	Mozilla (NSS 3.27)	Chrome	Java (8u101)	Adobe AATL	Adobe EUTL
Server Authentication	No	Valid [2]	No	Defer to OS	No	n/a	n/a
Client Authentication	n/a	Valid [2]	n/a	n/a	n/a	n/a	n/a
Secure Email	No	Valid [2]	No	n/a	n/a	No	No
Code Signing	No	Valid [2]	No	n/a	No	No	No
Time Stamping	No	Valid [2]	n/a	n/a	n/a	n/a	n/a
OCSP Signing	n/a	No	n/a	n/a	n/a	n/a	n/a
Document Signing	n/a	Valid [2]	n/a	n/a	n/a	No	No
Encrypting File System	n/a	Valid [2]	n/a	n/a	n/a	n/a	n/a
IP security end system	n/a	No	n/a	n/a	n/a	n/a	n/a
IP security IKE intermediate	n/a	No	n/a	n/a	n/a	n/a	n/a
IP security tunnel termination	n/a	No	n/a	n/a	n/a	n/a	n/a
IP security user	No	No	n/a	n/a	n/a	n/a	n/a
Adobe Authentic Document	n/a	n/a	n/a	n/a	n/a	No	No

Figure 3 Screen capture from crt.sh showing the Thai national root certificate is only trusted by Windows. Image from crt.sh https://crt.sh/?caid=13888

Server side techniques to mitigate against this threat have also been developed, such as OCSP stapling, HTTPS Strict Transport Security HSTS and Certificate Pinning to name a few.

Circumventing encryption: using downgrade attacks

One reason to be concerned about the Thai military government misusing their root certificate is that it has a history of tampering with SSL-type encryption.[81] Indeed, test data obtained by Privacy international reveals that the military government was conducting downgrade attacks in September 2014. 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 that without other protection, such as PGP encryption or S/MIME, the email metadata and content will be visible to any party between the user and the provider.

[80] https://crt.sh/?caid=13888

[81] SSL: secure socket layer (SSL), a secure internet protocol that encrypts communication over a network

Without these extra protections, it is vital that the communication link between user and service provider is secure and this is in general indicated by the use of ports 993, 465 or 587. There is however no guarantee that encryption is in place, even when these ports are in use. An attacker can deny connection via these known ports, which causes the email client to resort to the default port 25 to send email. This is unencrypted by default, although most email providers do use encryption even on this known cleartext port. This attack would only work on mail clients (such as Apple Mail, Microsoft Outlook and Thunderbird) because webmail is just standard web traffic that happens to contain an instruction to send or display an email.

Figure 4 Terminal window showing connection to Gmail from Thailand (downgrade attack). Image obtained by Privacy International from a confidential source.

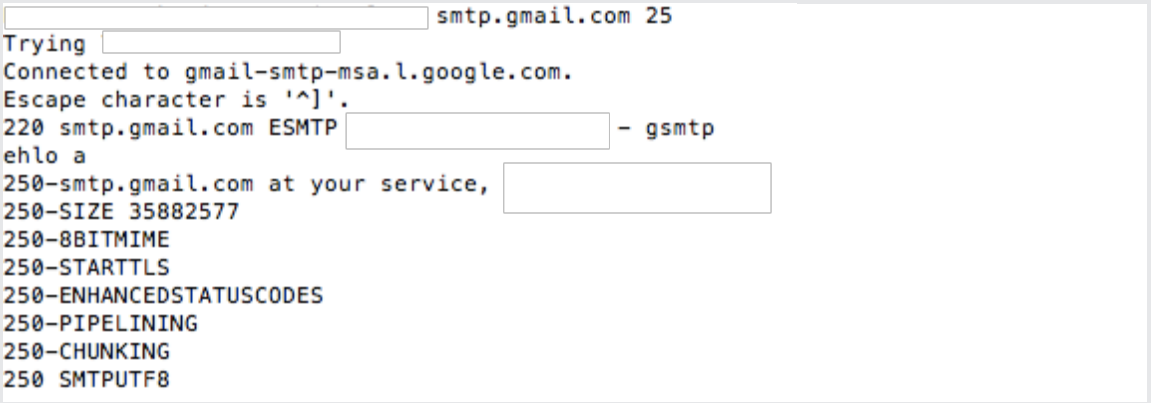


Figure 5 Terminal window showing connection to Gmail from the United Kingdom (note STARTTLS). Screen capture by Privacy International.

The attached screenshot received this year by Privacy International shows that connecting to gmail on port 25 would not offer STARTTLS[82] to be used. This would trigger an email client to send emails unencrypted to Gmail and increase the chances of them being read by a third party. Furthermore, additional data received by PI indicates that many IP addresses seemed to accept connections on port 25 even when the IP address was known not to provide email capabilities. These tests were conducted within Thailand and may indicate a blanket attempt to intercept all email communications, not just those of known providers.

[82] STARTTLS: Opportunistic encryption over a plaintext communication channel without requiring a separate port - generally used by email

IMSI catchers

Government documents have revealed that Thailand has purchased IMSI (International Mobile Subscriber Identity) catchers.

> 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.

In January 2015, following pressure from Privacy International, the Swiss government released the list of export licences granted to companies based in Switzerland that were selling surveillance technologies.[83] 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 designed for the extraction of voice or data, transmitted over the air interface'. This is the category of licence IMSI catchers require. The purchases range from CHF 170 ($172) to CHF 380,900 ($385,713). We believe that the low end of the cost range may pertain to trial period costs.

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.[84] The purchases ranged from £ 125,000 ($154,508) to £1M ($1,2M), an unusually expensive purchase for this type of licence. This licence was granted for "accessories/spare parts. Law enforcement agency end use."[85]

83 https://www.privacyinternational.org/node/98

84 https://docs.google.com/spreadsheets/d/11_TtwzbRIP9QD_aKA6ej8REFwVsS-hmB91WCTAYfP9g/edit#gid=831716195

85 https://www.caat.org.uk/resources/export-licences/licence?item=telecommunications+interception+equipment&order=desc&n=0&index=region

A worrying aspect of IMSI catchers is how little they normally cost. IMSI catchers have now become a common and well-known tool for law enforcement agencies and police forces all over the world, who are attracted by the low cost and ease of use. In fact they can be implemented using a standard software defined radio[86] and free and open source software. Furthermore, 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 and their damage to the right to privacy go far beyond the person targeted.

Activities that restrict the right to privacy, such as surveillance and censorship, and the use of intrusive technology such as IMSI catchers, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. It is unclear whether the legal framework in Thailand specifically regulates the use of IMSI catchers, and whether it is therefore open to abuse.

[86] Standard software defined radio: single piece of hardware that utilizes software to listen on different frequencies

Concluding Remarks: Resisting a Political System

Privacy International has conducted previous investigations into the Thai government's surveillance of social media as a tool of intimidation.[87] This report demonstrates how the practice is not only expanding, but the government is also experimenting with other forms of surveillance.

Privacy International is concerned about the increasing monitoring of social media and other internet-based communications services for the purpose of identifying political dissent. Often, monitoring is conducted in pursuance of prosecutions under lèse majesté offences and related crimes. This results in unlawful intrusion into people's privacy and has a chilling effect on freedom of expression.

In addition, this report has shown that a brief shutdown of Facebook around this time, which could have easily been overlooked, may demonstrate the government's intention to step up its surveillance regime by attempting to undermine user security and remove encryption.

Surveillance in Thailand is not necessarily carried out using expensive and highly technical infrastructures. Instead it is sometimes conducted with low-tech and affordable techniques such as misusing root certificates, employing downgrade attacks in order to circumvent encryption online, and using IMSI catchers in order to intercept content and other data from mobile phones. More profoundly, it is also achieved by establishing a political system and a legal framework that allows informal and easy access to communication service providers. The government can therefore force companies to 'behave', for example by threatening exclusion from spectrum licence auctions.

The evidence of the revolving door between the corporate sector and the government means that those at the head of communication service providers are always in close contact with the government, thus enabling softer forms of political influence to surveil people and ultimately erode people's privacy.

87 https://www.privacyinternational.org/node/935

Recommendations to the government of the Kingdom of Thailand:

- The government must uphold international obligations and Constitutional commitments to protect the right to privacy. International obligations are outlined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 21 of ASEAN Declaration on human rights. The latter states:
  "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."[88]
- Section 32 of the new Constitution of Thailand, adopted in 2016 via a referendum, states:
  "A person shall enjoy the rights of privacy, dignity, reputation and family. An act violating or affecting the rights of a person under Paragraph One, or the use of personal information for benefit by any means shall not be permitted, except by virtue of the provisions of the law specifically enacted as deemed necessary for the public interest."
- The government must 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.[89]
- The government should not restrict encryption and anonymity. Blanket prohibitions are neither necessary nor proportionate, and thus cannot comply with human rights law. The use of encryption promotes secure, private and free communications, facilitating the realisation of rights to privacy, expression and opinion.
- The government should avoid all measures that weaken the security that individuals may enjoy online, such as the malicious use of root certificates and the use of downgrade attacks.
- The government must prevent arbitrary invasion of privacy, freedom of expression and assembly through the use of IMSI catchers. Government use of IMSI catchers must be prescribed by law and limited to what should be strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion. It should be subject to periodic review by means of a participatory legislative process.
- The government should 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 such as root certificate authorisation.

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

89 https://necessaryandproportionate.org/

Recommendations for ICT Companies:

- ICT companies should support secure technologies for websites and communications and develop widespread default end-to-end encryption.[90]
- This report demonstrates that even a brief disruption of services could be part of a wider effort to undermine user privacy, such as attempting to remove encryption or interfering with root certificate authorities. All relevant companies must regularly review the status of root certificates, including companies that manufacture operating systems. In the case of Thailand, based on the refusal of other companies to trust the root certificate, Microsoft in particular should do the same as a precautionary measure.
- ICT companies should collaborate in an open and transparent manner on security issues such as root certificate authorisation. Transparency efforts can include sharing information about the status of root certificates, including any information that may impact on the trustworthiness or integrity of the root certificate authority in properly issuing certificates.
- Companies providing operating systems, browsers and mail clients must give adequate warning to users that a connection is untrusted, which could result in interception of content of apparently secure communications and/or the injection of false or malicious content such as malware. A connection is considered untrusted when a third-party attempts to bypass security processes, which could include misusing root certificates or forcing the user to communicate with their email service provider via an unencrypted channel.

90 See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/29/32 22 May 2015 https://www.privacyinternational.org/node/600. See also, Privacy International, the Harvard Law School's International Human Rights Law Clinic and ARTICLE 19 (2015) Securing Safe Spaces Online: Encryption, online anonymity and human rights https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf

Annex 1: Microsoft Response

Privacy International question to Microsoft

14 November 2016:

My question was regarding root certificates. I noticed Microsoft was the only company that trusts the Thai National Certificate by default (https://crt.sh/?caid=3D23349) so I was curious to hear what the process is at Microsoft to decide which root certs get included?

Microsoft response

25 January 2017:

Microsoft does not disclose its internal decision making process, but the overall process can be found on our website, http://aka.ms/rootcert. Generally speaking, Microsoft looks at the CAs Certificate Policy, Certificate Practices, and then consider the benefits and risks to Microsoft's customers.