

TECHNOLOGY AND COUNTER-TERRORISM:

Mapping the impact of biometric surveillance
and social media platforms on civic space

CASE STUDY THAILAND

This case study was researched and written by FORUM-ASIA, with ECNL's contribution being only editorial input and summarising for the purposes of the report. The Asian Forum for Human Rights and Development (FORUM-ASIA) is a network of 85 member organisations across 23 countries, mainly in Asia. Founded in 1991, FORUM-ASIA works to strengthen movements for human rights and sustainable development through research, advocacy, capacity development and solidarity actions in Asia and beyond. The FORUM-ASIA Secretariat is based in Bangkok, with offices in Jakarta, Geneva and Kathmandu.

Notable uses of biometric technology

Despite the 2019 elections, Thailand has effectively been ruled by the junta that led the coup in 2014. Since then, CSOs and human rights defenders have increasingly faced surveillance by the junta, in offline and online spaces, with the military enacting new regulation under the justification of national security.¹ The Thailand 4.0 Policy, with a stated aim of transforming Thailand into a digital government, has enabled the deployment of biometric technology supposedly for national security purposes.² This policy has enabled the collection of biometric information, such as fingerprints and face scanning, through the national digital ID card under the Digital Identification Act.³ Facial recognition systems in smart cities were also created under this policy.⁴ With an authoritarian government enforcing Thailand 4.0 policy, and with very little space for accountability or CSO participation, actions under this policy risk reinforcing the government's ongoing efforts to repress civic space, including through surveillance.

The government identified Southern Border Provinces (SBPs) as ongoing conflict areas and justified their biometric collection as a means to identify insurgents.⁵ These included SIM card registration, CCTV systems, facial recognition cameras, and DNA collection. Fingerprints and facial verification were required to purchase SIM cards in SBPs, with the government

- 1 Government Gazette. (2019, May 22). Vol. 136, Part 67a The Amendment to the Electronic Transaction Act (No. 4), B.E. 2562 (2019) on Digital Identification ("Digital ID Act") <https://www.mdes.go.th/law/detail/5100-ELECTRONIC-TRANSACTIONS-ACT-NO-4---B-E-2562-2019->; National Broadcasting and Telecommunications Commission (NBTC). (2019, April 9 & 2019, June 29). On the registration and collection of sim cards users. <http://numbering.nbt.go.th/getattachment/Announcement/Announcement-manual/447/ประกาศ-กสทช.-,เรื่องการลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่.PDF.aspx> (in Thai) and https://www.nbt.go.th/law/law_noti/nbt_notification/หลักเกณฑ์และวิธีการนำส่งข้อมูลการใช้โทรศัพท์เคลื่อนที่.aspx?lang=th-th (in Thai) - continued enforcement of Emergency Decree on Public Administration in Emergency Situation B.E.2548, the Martial Law Act B.E.2457 and the Internal Security Act B.E.2551 to authorise any faced surveillance policy in the Southern Border Provinces.
- 2 Ministry of Information and Communication Technology. (nd). Digital Thailand Pocket Book. Thailand Digital Economy and Society Development Plan. https://www.onde.go.th/assets/portals/files/Digital_Thailand_pocket_book_EN.pdf
- 3 Mansri, S. & Chumuang, P. (2019, January 10). Thai Cabinet Approves Digital ID Bill. SPI Newsletter. Siam Premier. http://www.siampremier.com/imgadmins/publications/pub_pdf/20190307140339.pdf
- 4 Burt, C. (2017, December 15). Phuket, Thailand to use Herta facial recognition for Safe City project. Biometric Update.com <https://www.biometricupdate.com/201712/phuket-thailand-to-use-herta-facial-recognition-for-safe-city-project>
- 5 Tatiyakaroonwon, C. (2020, January 8). Fact sheet: Forced DNA Collection in the Southern Border Provinces of Thailand. Research Project for Actions against Racial Discrimination in Thailand. Cross Cultural Foundation. https://crcfthailand.org/wp-content/uploads/2019/12/fact-sheet_forced-dna-collection-in-the-southern-border-provinces-of-thailand-1.pdf

alleging that sim cards were used to detonate bombs.⁶ Several Malay Muslims were asked to provide the DNA samples at checkpoints and border control with no explanation.⁷

Biometric data collection and SIM card registration supposedly aim to investigate and identify insurgents or individuals in terrorist groups in the South. The military reasoned that SIM card registration with fingerprints and facial scan would enable them to investigate perpetrators who detonate bombs.⁸ Biometrics are also used for border control by immigration police to check criminal records, including individuals identified as criminals with notice from Interpol.⁹

Surveillance technology and biometric collection used in SBPs are increasingly being used against protesters, and to monitor activities of human rights defenders and political dissidents. Examples include an attempt to collect DNA among Talu Fah Group protesters¹⁰ and a plan to use facial recognition and AI-driven surveillance to identify individuals on the national security watchlist.¹¹ In 2020, the police deployed around 30 CCTVs to monitor protests, raising concerns of surveillance among protesters.¹²

Notable uses of online content moderation and social media surveillance

The Thai government has pressured social media platforms to take down content critical of the monarchy, alleging that it violates the Computer Crime Act 2017¹³ and the Penal code,¹⁴ section 112 (Lèse-majesté).¹⁵ Content restrictions increased in 2020, during the height of

- 6 Anonymous. (2017, May 25). Thailand to require biometric checks for pre-paid SIM cards in troubled south. Reuters. <https://www.reuters.com/article/us-thailand-telecoms-idUSKBN18L1R2>
- 7 Anonymous. (2020, June 20). Coronavirus returnees ordered to give up DNA Samples. Khaosod English. <https://www.khaosodenglish.com/politics/2020/06/01/coronavirus-returnees-ordered-to-give-up-dna-samples/>
- 8 Anonymous. (2017, May 25). Thailand to require biometric checks for pre-paid SIM cards in troubled south. Reuters. <https://www.reuters.com/article/us-thailand-telecoms-idUSKBN18L1R2>
- 9 Devanesan, J. (2020, August 27). Thailand 4.0 — biometric e-passports arrive as part of national DX strategy. Techwire Asia. <https://techwireasia.com/2020/08/thailand-4-0-biometric-e-passports-arrive-as-part-of-national-dx-strategy/>. Biometric system procurement (as proof that the biometric system under immigration police includes integrating biometric data and matching with criminal records in the central system): <https://www.royalthaipolice.go.th/auction/590427.pdf> (in TH); Example: Thepgumpanat, P. & Wongcha-um, P. (2019, February 16). Thailand blames Australia for arrest of refugee Bahraini footballer. Reuters. <https://www.reuters.com/article/us-thailand-bahrain-refugee-idUSKCN1PV0E3>
- 10 Anonymous. (2021, April 21). combine culture point The officer tried to collect the DNA of the arrested mob through the sky reiterate the principles of human rights Everyone has the right to refuse. Matichon. (Title translated from Thai). https://www.matichon.co.th/politics/news_2653660
- 11 Nanuam, W. (2018, January 13). Push to fix, integrate security cameras. Bangkok Post. <https://www.bangkokpost.com/thailand/general/1394934/push-to-fix-integrate-security-cameras>; Royal Thai Police, Announcement of procurement: project to increase the investigation capacity and escalate the security and safety through the use of VIDEO processing, 21 Dec 2020.
- 12 Anonymous. (2020, September 17). Install cameras, set up screening points to deal with mob 19 Sept. Repeat the TU's order "Close all doors" (Title translated from Thai). Thairath.com <https://www.thairath.co.th/news/local/bangkok/1931771>
- 13 Act On Commission Of Offences Relating To Computer. B.E. 2550 (2007). Office of the Council of the State. http://web.krisdika.go.th/data/document/ext809/809768_0001.pdf
- 14 Thailand Penal Code Thai Criminal law (English Translation). <https://www.samuiforsale.com/law-texts/thailand-penal-code.html>
- 15 Facebook's own records show that there are requests from the Thai government since 2013 and the restrictions have made as related to those regulations, please see at the changelog: <https://transparency.fb.com/data/content-restrictions/country/TH/>

pro-democracy protests calling for monarchy reform.¹⁶ Twitter deleted 12% of government requests.¹⁷ It is unclear, however, whether the deleted content was related to Computer Crime Act or Lèse-majesté.

The government has attempted to prosecute platforms for failure to remove content critical of the monarchy. It threatened to ban Facebook in May 2017,¹⁸ and the government used Cyber Crime Law to threaten Facebook, Google and Twitter in 2020.¹⁹

In 2021, Facebook was threatened by the Ministry of Digital, Economy and Society (DES) and ordered to delete users disseminating 'fake news' and criticising the monarchy.²⁰ Following Thailand's order to Facebook to shut down the Royalist Marketplace,²¹ a Facebook group critical of the monarchy, Facebook threatened legal action against the DES. However, following the Thai government's withdrawal of its suit against Facebook, Facebook decided to not push through with their legal action.²²

Facebook and Twitter removed accounts that appeared to be linked to the Thai Military Internal Security Operations Command,²³ a military-led organisation that has been accused of conducting 'information operations' to target dissenters.²⁴ These accounts promoted messaging supporting the military and the monarchy and criticised insurgent groups and the opposition party in the SBPs. The networks used both fake and authentic accounts to manage pages and groups supportive of the military. On Facebook, these accounts had at least 700,000 followers in 2021.²⁵

16 As above, and Twitter Transparency Report Thailand <https://transparency.twitter.com/en/reports/countries/th.html>

17 Twitter Transparency Report Thailand <https://transparency.twitter.com/en/reports/removal-requests.html#2021-jul-dec>

18 New York Times. (2017, May 16). Thailand Warns Facebook After Video Seems to Show King in Crop Top. <https://www.nytimes.com/2017/05/16/world/asia/thailand-facebook-king-crop-top.html>

19 Anonymous. (2020, September 25). Thailand prosecutes Facebook, Google and Twitter over posts. BBC.com <https://www.bbc.com/news/technology-54296465>

20 Tortermvasana, K. (2021, June 25). Chaiwut threatens to sue Facebook. Bangkok Post.com <https://www.bangkokpost.com/thailand/general/2138027/chaiwut-threatens-to-sue-facebook>

21 Anonymous. (2020, August 25). Facebook blocks Thai access to group critical of monarchy. BBC.com. <https://www.bbc.com/news/world-asia-53899816>

22 Iyengar, R. (2020, August 25). Facebook prepares legal action against Thai governments order to block group. CNN Business. <https://edition.cnn.com/2020/08/24/tech/facebook-blocks-thailand-group/index.html>. New York Times. Facebook Plans Legal Action After Thailand Tells It to Mute Critics. <https://www.nytimes.com/2020/08/25/world/asia/thailand-facebook-monarchy.html>

23 Anonymous. (2020, October 9). Twitter takes down Thai army IO Network. Bangkok Post. <https://www.bangkokpost.com/thailand/general/1999463/twitter-takes-down-thai-army-io-network> ; Tanakasempipat, P. (2021, March 3). Facebook removes Thai military-linked information influencing accounts. Reuters. <https://www.reuters.com/article/us-facebook-thailand-idUSKBN2AV252>

24 Goldstein, J., Sinpeng, A., Bush, D., Ewald, R. & John, J. (2020, October 8). Cheerleading without fans: A low-impact domestic information operation by the Royal Thai Army. Stanford Internet Observatory. Stanford.edu. <https://stacks.stanford.edu/file/druid:ym245nv3149/twitter-TH-202009.pdf>

25 Tanakasempipat, P. (2021, March 3). Facebook removes Thai military-linked information influencing accounts. Reuters. <https://www.reuters.com/article/us-facebook-thailand-idUSKBN2AV252>

Relevant laws and legal precedents

The Personal Data Protection Act 2019 mandates that data controllers or data processors protect the privacy of individuals whose data they process.²⁶ It provides criminal and civil liabilities for violations. However, it allows exemptions for the collection and disclosure of data without consent if it is deemed to be used for public interest. It was enforced on 1 June 2022, after it having been delayed for two years.

While the law has provisions requiring data collectors to protect data,²⁷ it remains insufficient in addressing the systemic issues in Thailand. Within a cultural context where public interest has been broadly defined to justify violations of human rights particularly against the pro-democracy movement and defenders, there is a risk that the government will use this exception as a blanket exemption, impacts to the right to privacy of certain individuals and groups.

Unique aspects of the local surveillance landscape

In August 2021, a national security watch list or ‘enemies of the state’ list containing personal details of 183 political opponents, human rights activists and journalists was leaked.²⁸ The information included ID numbers, photos, passport numbers, and criminal records. Many of the individuals in the list were facing judicial harassment.²⁹

26 Government Gazette. (2019, May 27). Personal Data Protection Act, B.E.2562 (2019). <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>

27 Government Gazette. (2019, May 27). Personal Data Protection Act, B.E.2562 (2019). Section 22 to Section 44 under Personal Data Protection Act. <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>

28 Rojanaphruk, P. (2021, August 14). The Paranoid States Top-Secret List of Enemies. Khaosod English. <https://www.khaosodenglish.com/opinion/2021/08/14/the-paranoid-states-top-secret-list-of-enemies/>



European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

www.ecnl.org
[@enablingNGOlaw](https://twitter.com/enablingNGOlaw)