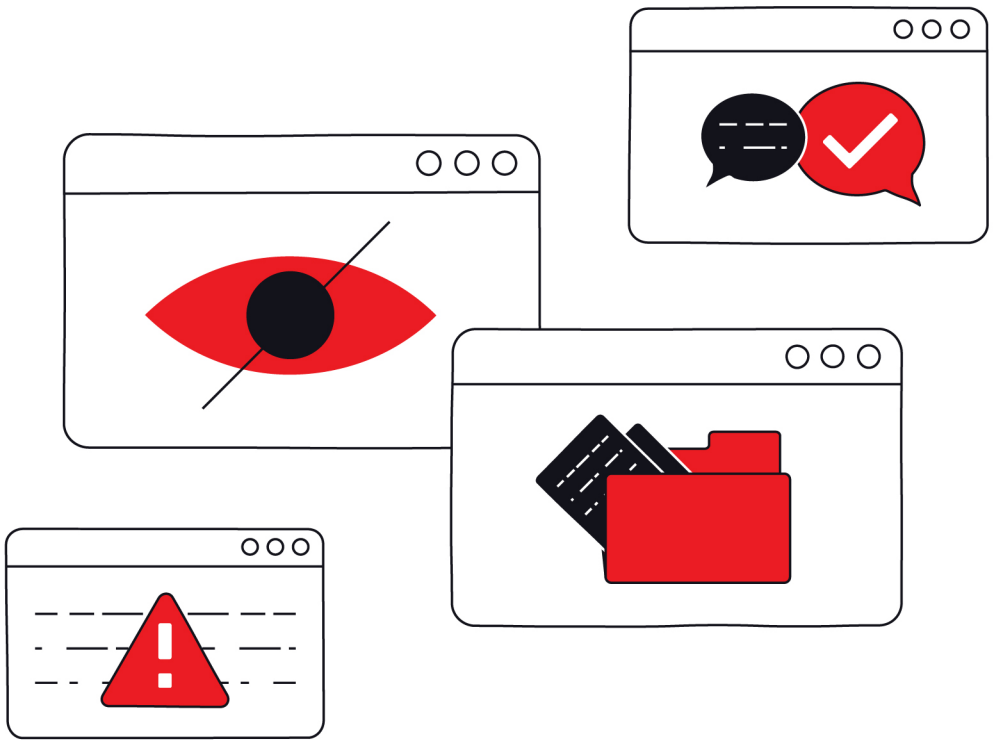
EngageMedia ASIACENTRE SCHOOL OF PUBLIC POLICY CHIANG MAI UNIVERSITY

4-Point Digital Rights Agenda for Political Parties



EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org

Asia Centre is a research institute in Special Consultative Status with the United Nations' Economic and Social Council. The Centre undertakes evidence-based research, convenes events and amplifies its work through media and social media engagement in the area of freedom of expression and digital rights.

Learn more at asiacentre.org

Chiang Mai University School of Public Policy (CMU-SPP) is a public policy school, concurrently operating as a cutting-edge research and consulting organisation, committed to solving complex public problems with inclusive, innovative, progressive, and sustainable policy solutions.

Learn more at spp.cmu.ac.th

Lead Writer

Prapasiri Suttisome, Digital Rights Project Officer (Thailand), EngageMedia

Advisory

Yawee Butrkrawee, Digital Rights Manager (Mekong), EngageMedia

Report Editor

Katerina Francisco, Editorial Coordinator, EngageMedia

Published February 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In light of the upcoming general election in Thailand, EngageMedia, Asia Centre, and the Chiang Mai University-School of Public Policy present four key digital rights issues that political parties must include in their agenda to ensure a well-functioning democracy where citizens can hold their government accountable. These issues could be addressed through legal amendment and the cessation of practices detrimental to the enjoyment of fundamental rights.

First, **promote and protect freedom of expression**. Despite the constitutional guarantees, freedom of expression is severely restricted in Thailand. Laws such as the Computer Crime Act and Articles 112 and 116 of the Penal Code are used to prosecute critics, journalists, human rights activists and academics for critical content, especially online. This crackdown has hampered freedom of expression in Thailand and fostered a culture of self-censorship.

Second, to promote transparency and hold the government accountable, officials must ensure **access to information**. Despite the Official Information Act, the Thai government has consistently invoked national security and public order to either refuse information disclosure requests or petition internet service providers and social media platforms to censor content deemed sensitive.

Third, **protect citizens' right to privacy**. Political parties should prioritise policies and practices that safeguard citizens' personal data from being collected, stored, or shared without proper consent or deviating from its original purposes. In addition, national security should never be an excuse to keep tabs on citizens' communication or activities, let alone the exercise of fundamental rights.

Fourth, **combating online disinformation** is crucial to keep citizens informed and ensure that democracy works in the current digital age. While the government has established a fact-checking mechanism, this does not align with international standards and is often used to defend government positions. Reforms are needed to regain people's trust in public institutions.

Political parties in Thailand should give these issues primary focus on their agendas. Laws and practices that compromise the exercise of freedom of expression, right to information, and privacy must be revised or corrected.

I.
PROMOTE AND PROTECT FREEDOM OF EXPRESSION

The exercise of freedom of expression is severely repressed in Thailand. Barely a year after the general election in 2019, local authorities revisited the use of vaguely-worded laws—namely the Computer Crime Act (CCA), Article 112 (lèse-majesté) and Article 116 (sedition) of the country's Penal Code—to penalise critics, journalists, human rights activists, academics, and students over critical content directed at public officials.

To curb renewed public dissent and calls for institutional reforms, from June 2020 to November 2022 the government charged at least 1,886 individuals for exercising their freedom of expression, including 283 youngsters whose ages are below 18.[1] Some were charged more than once. Political activist Parit Chiwarak, for example, has collected a total of 23 lèse-majesté charges by the end of 2021.[2] This crackdown has directly led to a chilling effect on freedom of expression in Thailand and the acute culture of self-censorship practised by the media and citizenry, especially online.

---

1 "November 2022: The total number of politically charged persons is 1,886 in 1,159 cases." 2022. Thai Lawyers for Human Rights (TLHR). December 4, 2022. https://tlhr2014.com/archives/51251.

2 "Parit Was Accused of Article 112 in a Total of 23 Cases While in Prison for Defending a Youth Who Was Forced to Pay Respect to the Image of Rama 10." 2021. Voice TV. December 17, 2021. https://voicetv.co.th/read/Or2noZvnb.

The COVID-19 pandemic has set the stage for the normalisation of government crackdown on freedom of expression. Through the use of the State of Emergency Decree and related Administrative Orders—especially Regulation No. 1 and Regulation No. 29—any person who disseminates information considered to be false, instigates fear among the public, or distorts information to mislead understanding of the emergency situation could face legal actions from the state. During the pandemic, government critics targeted under the CCA and Penal Code included opposition member Thanathorn Juangroongruangkit and world-renowned Thai rapper and singer Danupha Khanatheerakul, better known by her stage name 'Milli.' They were charged over their comments calling out the government's mismanagement of the public health emergency.

While the state of emergency was lifted on 30 September 2022 after being extended for the 19th time, the authoritarian residues remain. In October 2022, pro-government supporters/groups attempted to notify the police to charge Udom Taepanich, a standup comedian, over his satire mocking the Prime Minister and his supposed failures. Similarly, in November 2022 Amarat Chokepamitkul, a member of the Move Forward Party (MFP), was threatened with lèse-majesté charges over her comments questioning the administration of justice involving Article 112.[3]

EngageMedia's Recommendations:

- Amend Article 25 of the Constitution to stipulate that the promotion and protection of fundamental rights, as stated under Chapter 3 (Rights and Liberties of the Thai People), also extends to the exercise of such rights in online spaces.
- Amend Articles 34, 35, and 36 of the Constitution and remove vaguely-worded clauses to allow for better promotion and protection of fundamental freedoms.
- In the amendment to the Constitution, include the three-part test for the validity of restrictions on freedom of expression: the principle of legitimate interest, necessity, and proportionality.
- Repeal Articles 112 (lèse-majesté) and 116 (sedition) of the country's Penal Code.

---

3 MP "Amarat" had her microphone cut off during the discussion related to the institution by "Chuan", who cited the need to uphold rules and regulations. (2022, November 2). The Momentum. https://themomentum.co/report-chuan-mic/

- Amend Section 14 (2) of the Computer Crime Act, removing overly broad language and providing clear definitions or specifications to avoid arbitrary interpretations.
- Repeal Section 14 (3) of the Computer Crime Act, which overlaps with Articles 112 and 116 under the Penal Code.

II.
ENSURE ACCESS TO INFORMATION

Access to information ensures transparency and the proper function of democratic governance, and enables citizens to hold the government accountable. Thailand's Constitution (2017) guarantees the right to access information under Article 41. Meanwhile, the Official Information Act (OIA) stipulates the implementing rules and processes to ensure public access to information.

Despite these legal guarantees, the Thai government has consistently invoked national security and public order to restrict these rights to information, either by refusing information disclosure requests or petitioning internet service providers and social media platforms to take down content it deems inappropriate. This has been reflected in the government's attempt to revise the OIA and a number of content removal requests made to service providers.

The draft amendment to the OIA, approved in March 2021, would tighten restrictions on any data disclosure that could be used to harm the monarchy, national defence, and security. The exemption from public disclosure also extends to information regarding military intelligence, locations, and weapons. Many critics perceived this as an attempt to shield the

military from public scrutiny over their weapon procurement with foreign powers.[4] Most notably, the new draft bill grants authorities the discretionary power to assess and reject the disclosure requests, if deemed to be disruptive to government operations.[5]

Over the first six months of 2022, the Ministry of Digital Economy and Society (MDES) has sought court authorisation and cooperation from social media platforms to block over 2,630 websites, 47 per cent of which were removed for allegedly insulting the monarchy.[6] According to Facebook's Transparency Center, the platform restricted access to 2,240 items in Thailand between January and June 2022.[7] Data from Google Transparency Report from the same reporting period reveals that there have been 419 requests for content removal from YouTube, citing government criticism.[8]

It must be noted that most service providers complied to avoid culpability under Articles 15 and 20 of the CCA.[9] These practices are likely to continue unabated, especially with the recent implementation of MDES ministerial notification in October 2022. The notification accelerates the takedown process to within 24 hours once a complaint is made, bypassing the court order.

Meanwhile, a new development that may affect the affordability of access to the internet was the merger of mobile service providers DTAC and TRUE in October 2022, which would result in a duopoly of the telecommunication sector in Thailand. Per the econometric model conducted by a local think tank, the cost of services is likely to increase 10-20 per

---

4 *Matichon*. 2021. "'Rome' Criticized the Draft Official Information Act as a Threat to the People, Opening the Way for the State to Not Disclose Military Budget.," March 25, 2021. https://www.matichon.co.th/politics/news_2641726.

5 The Internet Law Reform Dialogue (iLaw). n.d. "New Information Act Draft: Public Information Confidentiality License." *Https://Ilaw.or.Th/*. https://ilaw.or.th/node/5874.

6 "Chaiyawut Admires YouTube and Tiktok for Cooperating to Combat Fake News, Revealing Concern for Social Media, Which Causes Social Division." 2022. Royal Thai Government. June 2022. https://www.thaigov.go.th/news/contents/details/55666.

7 "Content Restrictions Based on Local Law: Thailand" Transparency Center, Meta https://transparency.fb.com/data/content-restrictions/country/TH/

8 "Government requests to remove content," Transparency Report, Thailand, Google, https://transparencyreport.google.com/government-removals/overview

9 Asia Centre and Destination Justice. 2022. "Internet Freedom in Thailand: August 2022." p.18. https://asiacentre.org/wp-content/uploads/Internet-Freedoms-in-Thailand-2022.pdf.

cent on average, but 66-120 per cent in the worst-case scenario.[10] As a regulatory body, the National Broadcasting and Telecommunications Commission (NBTC) was heavily criticised for its failure to properly oversee the merger and protect public interest.

EngageMedia's Recommendations:

- Retract the attempt to amend the Official Information Act.
- Revise Sections 15 and 20 of the Computer Crime Act to avoid imposing disproportionate liability offences on service providers.
- Quash the MDES ministerial notification "Suppression of Dissemination and Removal of Computer Data from the Computer System B.E. 2565" (October 2022).
- Ensure that the NBTC performs its regulatory responsibilities by supervising telecommunications providers and ensuring that they compete and operate in a free, fair, and independent manner.

10 Kamsaeng, Chatra. 2022. "5 Rumors vs 5 True Stories: True + DTAC Merger Deal and the Role of the NBTC." *The 101 World*, May 6, 2022. https://www.the101.world/5-narratives-vs-5-facts-about-dtac-true-merger/.

III.
RESPECT AND PROTECT THE RIGHTS TO PRIVACY

In June 2022, the government passed the Personal Data Protection Act (PDPA). While this signified a progressive first step toward better safeguards on data privacy, Section 4(2) of the law is vaguely worded and provides immunity for public officials acting for national security reasons. This exemption raises the fear of officials abusing the subjectivity of legal provisions in the name of national security or public interests, ranging from education to public health.

Such concerns over data privacy are not entirely unfounded. During the COVID-19 pandemic, the government had rolled out multiple contract tracing applications, namely Mor-Chana and Thai-Chana, to contain the spread of the virus. The applications, however, were ranked as the most privacy-invading contact tracing app in Southeast Asia.[11] In June 2020, the Ministry of Defense admitted that it had requested the Department of Disease Control and service providers to hand over location data from the contact tracing app of those who were in close proximity to COVID-19 patients.

---

11 Pichayada Promchertchoo, Channel News Asia, February 2021. https://www.channelnewsasia.com/asia/transparency-thailand-covid19-contact-tracing-app-mor-chana-297901

Personal data, collected by public officials, could also be weaponised for political gains through the practice of doxxing, or the act of revealing sensitive, personal information online, usually with malicious intent. In January 2022, the vaccination record of Progressive Movement founder Thanathorn Juangroongruangkit was leaked to discredit his criticism of the government's mismanagement of vaccine provision.[12] The leaked data came from the government-run vaccine registration application Mor-Prom.

Another key infringement upon the right to privacy in Thailand is state surveillance. In 2019, the National Intelligence Act—which allows public officials to intercept data and communications that may threaten public security and internal affairs—was passed allegedly to provide legal cover for the digital surveillance of activists and government critics.[13] Evidence also suggests that Thai authorities have reinvigorated their efforts to gain unauthorised access to the mobile devices of political dissidents through the purchase of surveillance software.

From 2020 to 2021, the Royal Thai Army allegedly deployed surveillance technology from cyberespionage firm Circles to intercept emails and phone calls.[14] In November 2021, at least 17 Thai human rights defenders and activists received notifications from Apple, cautioning that they may fall victim to state-sponsored cyber attacks.[15] In July 2022, the government admitted that it has used surveillance software to "listen into or access a mobile phone to view the screen, monitor conversations and messages" in cases related to national security.[16]

---

12 "Thanathorn Confirms Legitimate Vaccination, Accuses Government of Discrediting Him with Personal Information Release". (2022, January 10). Daily News Online. https://www.dailynews.co.th/news/654362/

13 Sombatpoonsiri, Janjira. "Digital Surveillance in Thailand: When Pegasus Takes Flight."Fulcrum. February 2022. https://fulcrum.sg/digital-surveillance-in-thailand-when-pegasus-takes-flight

14 Marczak, Bill. 2021. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." The Citizen Lab. June 29, 2021. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

15 A joint collaboration between local CSO iLaw and Canadian-based think tank Citizen Lab later revealed that the software involved was Pegasus Spyware, which was developed by Israeli NSO group and sold only to foreign governments, see https://plus.thairath.co.th/topic/speak/101820

16 Reuters. 2022. "Govt Admits Using Phone Spyware, Cites 'National Security.'" Bangkok Post. July 20, 2022. https://www.bangkokpost.com/thailand/general/2350068/govt-admits-using-phone-spyware-cites-national-security.

In November 2022, ahead of the 2022 APEC Summit in Bangkok where political protests were expected, no less than 44 activists, human rights defenders, and asylum seekers received alerts from Facebook, warning that their accounts may have been subjected to "government-backed or sophisticated attacks".[17]

EngageMedia's Recommendations:

- Amend Section 18 of the Computer Crime Act to ensure that the court authorises any information requests from authorities beforehand.
- Amend Section 4 of the Personal Data Protection Act (PDPA) to remove legal immunity of public officials justified under overly-broad national security purposes.[18]
- Cease the practice of doxxing, interception of communication and online surveillance of critics, opposition members, and human rights defenders through the abuse of state-of-the-art surveillance technologies and data collection systems.

17 "44 activists-NGOs found warned of possible government-sponsored attacks on Facebook accounts." n.d. Freedom of Expression Documentation Center. The Internet Law Reform Dialogue (iLaw). https://freedom.ilaw.or.th/node/1158.

18 Manushya Foundation, Access Now, Article 19, and the ASEAN Regional Coalition to #StopDigitalDictatorship, Joint UPR Submission: Digital Rights in Thailand, for the UN Universal Periodic Review of Thailand (3rd UPR Cycle), 39th Session of the UPR Working Group, March 2021, p.9

IV.
CHECK THE FACT-CHECKER AND COMBAT ONLINE DISINFORMATION

In 2019, the MDES established the Anti-Fake News Center (AFNC) to combat false and misleading information on social media. Apart from identifying content it deems inaccurate or harmful to the country's reputation, the AFNC also issues what it considers "corrections". However, the AFNC does not operate by international standards such as the International Fact-Checking Network (IFCN) Code of Principles.

Although the AFNC claims to be impartial and verifies information, it has disproportionately sided with government policy. More than 80 per cent of all government-related posts were published to defend the government's position.[19] This implicitly equates public criticism to fake news and disinformation. From 2020 to 2021, the direct collaboration between the AFNC and the police resulted in 116 people being charged, out of 293 reported cases.[20]

---

19 Schuldt, L. (2021). Official Truths in a War on Fake News: Governmental Fact-Checking in Malaysia, Singapore, and Thailand. Journal of Current Southeast Asian Affairs, 40(2), 340-371.

20 MCOT. "The Ministry of Digital Economy and Society Reveals the Number of Fake News Prosecution Cases in 2020-21." December 9, 2022. https://www.mcot.net/view/u5iAuRrB.

On top of this, the government is itself a purveyor of disinformation. In 2020 and 2022, leaked confidential documents revealed that the Thai military enlisted as many as 17,000 personnel to spread online disinformation, promoting pro-government narratives while discrediting vocal critics and human rights defenders.[21] Prominent rights activists subjected to these smear campaigns included Angkhana Neelapaijit and Anchana Heemmina, who criticised the mistreatment of Muslim minorities in three southernmost provinces of Thailand.[22]

These systematic state-sponsored disinformation operations prompted social media platforms to suspend accounts linked to the military. In October 2020, Twitter closed down 926 accounts.[23] Facebook soon followed suit with 185 accounts removed in March 2021.[24]

EngageMedia's Recommendations:

- Depoliticise the Anti-Fake News Center by transferring it to a more specialised public organisation such as the Thai Media Fund, which focuses on media and digital literacy.
- Commit the Anti-Fake News Center and its fact-checking operations to international standards such as the IFCN Code of Principles or the European Code of Standards for Independent Fact-Checking Organisations.
- Prioritise the removal of genuine false content and issuing corrections and public apologies rather than criminalisation.
- Cease the state-sponsored disinformation operations against political dissents, social activists, and human rights defenders.

---

21 Prachatai English. n.d. "PM Involvement in 'Information Operations' Raised in No-Confidence." https://prachatai.com/english/node/9435.

22 "[Thailand] Angkhana Neelapaijit and Anchana Heemmina File Civil Case against PM's Office and Royal Thai Army for Their Involvement in a Disinformation and Smear Campaign", Protection International, November 16, 2020, https://www.protectioninternational.org/en/news/thailand-angkhana-neelapaijit-and-anchana-heemmina-file-civil-case-against-pms-office-and-royal

23 Twitter. n.d. "Disclosing Networks to Our State-Linked Information Operations Archive." https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.

24 "185 Accounts Related to Thai Military Information Operation Removed." n.d. Prachatai English. https://prachatai.com/english/node/9101.

EngageMedia.org

/Thailand-Digital-Rights-Agenda-Political-Parties/