

DIGITAL TECHNOLOGY AND SURVEILLANCE IN ASIA-PACIFIC

NEW AVENUES
OF STATE AND PRIVATE SURVEILLANCE
AND POSSIBLE RESPONSES



JAI VIPRA

June 2022

TABLE OF CONTENTS

INTRODUCTION	3
POLITICAL AND ECONOMIC CONTEXT	4
Philippines	4
Thailand	5
India	5
Cambodia	6
SECTION I: STATE SURVEILLANCE	7
State agencies and surveillance	7
<i>Philippines</i>	7
<i>Thailand</i>	8
<i>India</i>	9
<i>Cambodia</i>	9
National digital identification systems	12
Public private partnerships and surveillance	13
Covid-19 contact tracing, monitoring and surveillance	15
SECTION II: PRIVATE SURVEILLANCE	18
SECTION III: AGENDA FOR ACTION	20
A comprehensive personal data protection law	20
New workers' rights against surveillance	21
Taking stock of the private benefits of mass surveillance	21
Sovereignty through participation	22
Data minimisation	23
CONCLUSION	24
ENDNOTES	25

INTRODUCTION

Digital technology has increased the available avenues for mass surveillance. From Edward Snowden's revelations in 2013 about US government surveillance, to the decidedly commonplace data collection of today, surveillance and privacy have become political issues.

The rise of large technology companies like Facebook and Amazon has also increased surveillance challenges. Increasingly, private technology firms drive the surveillance agenda of governments. In this context, the UN Special Rapporteur on Freedom of Opinion and Expression has called for a moratorium on the sale, transfer and use of surveillance technology, pointing out that there is no effective global or national public control over such technologies.¹

This report provides an overview of the surveillance landscape in the Asia-Pacific region, focusing on the Philippines, Thailand, India and Cambodia, and outlines the greatest privacy risks from both state and non-state actors. The political context for the four countries includes the rise of undemocratic forces, neoliberalism, inequality and the diminishing role of the welfare state. The Covid-19 pandemic has affected all four countries differently, but the economic impacts have been adverse in all. The paper elaborates on the surveillance implications of Covid-19 in these countries.



POLITICAL AND ECONOMIC CONTEXT

This section presents the economic and political context to digitalisation and digital surveillance in the selected countries.

Philippines

Only about 50 percent of individuals in the Philippines use the internet. Much like other countries in the Global South, the Philippines' internet use is driven primarily by mobile connections.² Internet access is less prevalent and reliable for rural areas as compared to urban areas, and can be patchy even in urban areas.³

Over 57,000 people had lost their lives to Covid-19 in the Philippines as of March 2022.⁴ These numbers are relatively high

compared to the country's neighbours and were accompanied by widespread hunger. The economy experienced a recession⁵ and is also seeing record high levels of unemployment.⁶

In June 2016, Rodrigo Duterte came to power in the Philippines. His rule has become known for its brutal crackdown on alleged drug dealers and on political opponents, as well as its extensive use of social media for narrative building. The government passed a draconian Anti-Terrorism Law that makes it easy to brand any individual as a terrorist and uses an over-broad definition of terrorism.⁷



Using phone application/registration in Thailand for use when entering shops by ILO Asia Pacific

Thailand

In Thailand, internet coverage is high, particularly in the form of mobile broadband. 78 percent of all people reported using the internet in 2020.⁸ Thailand sees a high prevalence of digital technology in the services sector and a limited prevalence in the manufacturing and agriculture sectors.⁹ Although the government has prepared vision documents and policies for a digital Thailand, the country is saddled with high levels of inequality, high cost of access and a low incidence of advanced digital skills among the population.¹⁰

Added to these issues is political turmoil. In 2014, Thailand was subjected to a military coup. The government established after the coup retained power in 2019 through elections that were widely considered to be manipulated. Since July 2020, the country has seen huge demonstrations for a new Constitution and reform of the monarchy. These demonstrations follow from youth and student protests that were a reaction to the banning of an opposition party. This political discontent is also related to the government's mismanagement of the economy, amplified during the pandemic. The nearly unprecedented anti-monarchy nature of the protests ensured the support of workers and the general public.¹¹

As of early 2022, the protests have been thwarted through repression, although discontent with the government persists and discontent with the monarchy is now mainstream.¹² With the suppression of large-scale street protests, Thai activists are taking to individual demonstrations and social media activism.¹³ This makes digital surveillance a greater danger to dissent today.

AS OF EARLY 2022,
THE PROTESTS
HAVE BEEN
THWARTED THROUGH
REPRESSION,
ALTHOUGH
DISCONTENT WITH
THE GOVERNMENT
PERSISTS AND
DISCONTENT WITH
THE MONARCHY IS
NOW MAINSTREAM.

India

In India, the ICT Access Index as calculated by the International Telecommunication Union, is 38.2—a figure much lower than other BRICS countries, demonstrating the low levels of internet access in the country.¹⁴ In addition, internet access varies across gender and regions.

Demonetisation of Indian currency notes in 2016 precipitated an economic crisis, particularly for small and medium industries, that is yet to abate. The government is keen

to push through neoliberal reforms in the agricultural sector, seeks to privatise public enterprises, and is diluting hard-won labour protections. Its crackdown on protests against discriminatory citizenship laws (the Citizenship Amendment Act and the proposed National Register of Citizens) has been followed by an unprecedented and successful movement by the country's farmers against agricultural reforms. A harsh lockdown during the first wave of the pandemic meant that tens of thousands of workers lost their jobs, migrant workers had to walk to their villages with their families, and millions of Indians fell into poverty. An even harsher second wave between February-June 2021, exacerbated by government inaction, led to 1.5 million deaths by unofficial estimates.¹⁵

Digital technology has been crucial in aiding the government and the ruling party in its goals. Anti-Muslim violence, the lynching of minorities and a pogrom in Delhi were all accompanied by virulent disinformation campaigns through both digital and traditional media, in addition to state-supported online hate speech.¹⁶ Several Indian police agencies also carry out targeted and mass surveillance through emerging technology (such as voice analytics) in a legal vacuum.¹⁷

Cambodia

Cambodia has high internet penetration—about 78.8 percent of the population used the internet as of 2020.¹⁸ This figure was a sharp rise since 2017, when only 32.9 percent of the population used the internet. The increase is in line with the government's goal, stated in 2016, to increase internet penetration to 80 percent by 2020.¹⁹

The government implemented an initially effective if severe response to the Covid-19 crisis. It limited the number of Covid-19 cases to about a thousand as of March 2021 and prevented a single Covid-19 death from occurring in that time.²⁰ By April 2022, the number of deaths had ballooned to over 3,000.²¹ Towards the end of 2021, the country declared that it would pursue a policy of "living with Covid", after which deaths have stabilised albeit under low levels of testing.²²

In April 2020, the government promulgated the State of Emergency Law, restricting freedom of movement and assembly.²³ However, it did not actually declare a state of emergency.²⁴ There are concerns that the government used the pandemic to give itself extraordinary powers for the future.²⁵ The government has already used Covid-related powers to arbitrarily test and detain striking workers at the NagaWorld casino.²⁶

In 2020, two major drivers of the Cambodian economy—garment exports and tourism—took a hit from European sanctions and Covid-19.²⁷ There were large-scale layoffs in the garment industry, and initially no debt relief forthcoming from the government for debt-ridden workers.²⁸ Eventually, the government announced support measures for workers, small and medium enterprises, and the agriculture sector.²⁹

Seen over a longer time period, Cambodia has not been free from the clutches of neoliberalism. The state has been falling short in providing public welfare, and has ended up facilitating private and foreign aid initiatives.³⁰ There have also been reports of the persecution of political opponents and politically motivated arrests.³¹

SECTION I: STATE SURVEILLANCE

State agencies and surveillance

State agencies carry out surveillance in both legal and illegal ways. Undue mass and targeted surveillance can be quite legal, and thus we examine below both methods of surveillance in the selected countries.

Philippines

New Anti-Terrorism Act: The Human Security Act in the Philippines gave the government the right to conduct surveillance on anyone suspected by the government of being a terrorist.³² This law was in place despite the fact that the right to privacy is constitutionally guaranteed in the Philippines.

Its updated version—the Anti-Terrorism Act of 2020—makes it easier for the government to designate anyone a terrorist, increasing the risk of targeted surveillance. It allows for lengthy invasive surveillance and warrantless arrests.³³

The law is aimed at the communist and Muslim insurgencies in parts of the country.³⁴ It enables the persecution of the leftist political opposition and people accused of being communists.³⁵ The Supreme Court upheld all but one section of the law, striking down a part that said “advocacy, protest, dissent, stoppage of work, industrial or mass action, and other similar exercises of civil and political rights” could be designated as terrorism based on their intentions.³⁶ The law is reportedly unpopular.³⁷



Philippines protests: Global Day of Action against red tagging by IndustriALL Global Union

United States involvement: The involvement of the US is palpable in the Philippines' surveillance activities. This involvement has its roots in colonial surveillance imposed by the US on the Philippines before and after the country won its freedom in 1946.³⁸ The US government has trained officials in the Philippines on conducting social media monitoring, enabling their overreach.³⁹ The country has also been subject to the US National Security Agency's overseas surveillance programmes MYSTIC and PRISM, and even signed an Enhanced Defense Cooperation Agreement with the US under former President Aquino.⁴⁰

THE COUNTRY
HAS ALSO BEEN
SUBJECT TO THE US
NATIONAL SECURITY
AGENCY'S OVERSEAS
SURVEILLANCE
PROGRAMMES MYSTIC
AND PRISM, AND EVEN
SIGNED AN ENHANCED
DEFENSE COOPERATION
AGREEMENT WITH THE
US UNDER FORMER
PRESIDENT AQUINO.

Social media and surveillance: Recently, President Duterte vetoed a bill that would require all persons purchasing a SIM card to present an ID card, and for social media users to register their names and phone numbers. His stated motivation for the veto was that it was against free speech and privacy.⁴¹ However, critics have pointed out that the probable real motivation for the veto is that Duterte's party and government rely heavily on fake profiles on social media to spread their messages.⁴² In this way, online anonymity perversely helps the government preserve its power in the Philippines. Critics still maintain that the Bill would be ineffective in stopping terrorism or misinformation, as SIM card identity registries or social media registration have not been shown to work in any country.⁴³

Thailand

The use of legislation against dissent:

In Thailand, the Computer Crime Act, passed in 2007 after a military coup, started the systematic control of the internet by the military.⁴⁴ It requires that service providers store metadata for 90 days, and allows state agencies to access this metadata without needing a court sanction.⁴⁵ This Act also expands the ban on criticising the monarchy to the domain of the internet, uses vague definitions to criminalise the dissemination of "obscene" material, and allows for taking down content that violates public order or good morals of the people.⁴⁶ In February 2019, Thailand enacted a National Cybersecurity Law that was criticised for enabling the government to seize data and devices without court authorisation under vague national security justifications.⁴⁷ The right to privacy was removed in the interim Constitution after the military coup in 2014.⁴⁸ Other laws that are

used to target protestors include the Personal Data Protection Act of 2019. Under this Act, there are broad exemptions to the requirement of consent prior to data collection if the data is collected by the state for some stated purposes.⁴⁹ Activists involved in the recent protests have been charged under the Computer Crime Act among others, as protestors have extensively used social media to communicate and mobilise.⁵⁰

Turning citizens against citizens: In 2017, Privacy International released a report detailing the use of government resources to monitor social media posts for anti-monarchy content. The report revealed that the Thai government staffed people full time to monitor social media, and also incentivised citizens to share the personal information of people that they think are violating the law.⁵¹

Social media surveillance in Thailand predates this wave of protests. Laungaramsri (2016) showed how cyberspace became the military's priority battlefield in the preceding years, and how the Cyber Scout program has been used to create a large group of volunteers, including students, to keep an eye out for anti-monarchy comments online.⁵² In the same vein, the Digital Economy and Society Ministry of Thailand set up a "fake news" prevention and suppression centre, that will coordinate with anti-fake news centres across the country. The centre will operate under a new regulation that gives the government powers to suppress content online under a broad definition of fake news, including information that damages the image of the country and that causes social misunderstandings.⁵³

Counter-insurgency and the Muslim minority: In the southern border regions of



THE REPORT
REVEALED THAT THE
THAI GOVERNMENT
STAFFED PEOPLE FULL
TIME TO MONITOR
SOCIAL MEDIA, AND
ALSO INCENTIVISED
CITIZENS TO SHARE
THE PERSONAL
INFORMATION OF
PEOPLE THAT THEY
THINK ARE VIOLATING
THE LAW.

Thailand, the government has launched an extensive facial recognition data collection drive. All persons registering for a SIM card have to submit their facial data to be used for the facial recognition system to counter insurgency.⁵⁴ Since this policy applies primarily to the Malay Muslim areas of the country and not elsewhere, it has been construed as discriminatory and targeted surveillance, particularly in the context of extrajudicial killings of suspected insurgents.⁵⁵

India

Data protection in the law: India does not yet have a comprehensive privacy or data protection law, although the right to privacy has been declared a constitutional right by the Supreme Court in 2017.⁵⁶ Sectoral guidelines and regulations issued by the Press Council of India, the Medical Council of India, as well as certain financial laws contain provisions for privacy.⁵⁷ The Information Technology Act provides grounds for government surveillance of internet data under Section 69. These include defending the sovereignty of India and public order. The Act also provides a remedy for illegal hacking. The Indian Telegraph Act of 1885 contains provisions that allow Central and State governments to intercept phone and computer-based communication. The government requires an authorisation from the Home Secretary (an administrative position) to intercept communication.⁵⁸ In 2018 the government authorised 10 agencies, including the Narcotics Control Bureau and the Commissioner of Police of Delhi, to intercept communication provided they follow the law and standard operating procedures. The review process for interception, meant to prevent misuse, is not adhered to as a rule.⁵⁹

Emerging technology and state surveillance: India's biggest surveillance challenges seem to be driven by secretive government programmes and new technologies. For example, the National Intelligence Grid or NATGRID is a system that integrates data on people from various sources. The system is currently being challenged in court for allowing the government to monitor telecommunications in bulk.⁶⁰ New technologies, such as facial recognition and drones, are being used to build up

mass databases and target dissenters. For instance, police have been regularly recording protestors' faces at protest sites in order to feed the data into facial recognition systems.⁶¹ Several state and city police forces use facial recognition technology for a litany of uses, including finding missing children, profiling accused persons, and monitoring public spaces.⁶² In fact, some states use facial recognition technology and audio analytics to monitor prison systems through an expansive

IN FACT, SOME STATES USE FACIAL RECOGNITION TECHNOLOGY AND AUDIO ANALYTICS TO MONITOR PRISON SYSTEMS THROUGH AN EXPANSIVE NETWORK OF CAMERAS AND MICROPHONES, AIMING TO TRANSFORM THIS MONITORING INTO DATA FOR PROFILING AND PREDICTION.

network of cameras and microphones, aiming to transform this monitoring into data for profiling and prediction.⁶³ Large parts of such surveillance are carried out in partnership with the private sector with little to no transparency on the terms of the agreements.⁶⁴

New threats to privacy: New laws, such as the Criminal Procedure (Identification) Bill, provide the police with broad powers to collect (without a warrant) biological data and other “measurements” such as signatures and handwriting from arrested persons.⁶⁵ The law has provoked widespread concern over the use of such data collection for profiling, particularly as it allows police authorities to retain the data for up to 75 years.⁶⁶ Meanwhile, a much diluted version of the Data Protection Bill is still pending in Parliament.

Cambodia

Right to privacy: In Cambodia, Article 40 of the Constitution guarantees the right to “privacy of residence, and to the secrecy of correspondence by mail, telegram, fax, telex and telephone”.⁶⁷ However, the State of Emergency Law passed during the pandemic allows the government unbridled digital surveillance powers once a state of emergency is declared by Royal Decree in consultation with the Prime Minister, the President of the National Assembly, and the President of the Senate. The Law grants the government the authority to carry out “surveillance measures by any means for digital information in response to the State of Emergency” and to institute “bans or limits on distributing or broadcasting information that can cause public panic or turmoil, damage to national security or confusion about the situation under the State of Emergency” (unofficial translation).⁶⁸

The Cambodian Ministry of Posts and Telecommunications has the right to control and demand “telecommunications, information and communication technology service data” under the Telecommunications Law. The same law gives telecom subscribers “rights to privacy, security and safety of using the telecommunications service, except otherwise determined by other specific law”.⁶⁹

Search and interception of communication:

The new e-commerce law also contains provisions on data protection and fines for violating these provisions.⁷⁰ A 2018 decree mandates that all Internet Service Providers should incorporate software that allows blocking websites that can be considered as incitement.⁷¹ The new e-commerce law, which applies to nearly all electronic commercial or civil acts, documents and transactions, prohibits encryption of data that may be used as evidence. However, the Code of Criminal Procedure states that investigating officers need to seek authorisation before conducting a search.⁷² This can be considered a violation of citizens’ right to privacy.

Internet Gateway: In 2021, Cambodia announced its intention to implement a “National Internet Gateway”, or a mechanism whereby all internet traffic in and out of the country would be routed through a government-controlled checkpoint.⁷³ In February 2022, the government announced that it had indefinitely delayed the implementation of this Gateway.⁷⁴ Plans for the Gateway have been criticised for splintering the internet, likely decreasing the quality of network provision, increasing costs and stalling innovation.⁷⁵ Critics also point out that the Gateway will almost certainly lead to inspection of content, affecting Cambodian

citizens' right to privacy. The Gateway would also allow the government to arbitrarily terminate any person's internet connection.⁷⁶

National digital identification systems

National identification systems are often used when the state wants to include and exclude people from services, welfare and certification. ID systems can be digital or non-digital, and often, but not always, include biometric data, i.e. data on people's physical characteristics like fingerprints or eye scans.

The World Bank has been aggressive in its push for digital IDs in Asia-Pacific countries. It holds that digital IDs are necessary for a digital economy.⁷⁷ The Philippines is working on a national digital ID under the Philippine Identification System or PhilSys.⁷⁸ In 2018,

Thailand initiated a national digital ID project. It is now planning to replace physical IDs entirely with digital IDs.⁷⁹

While digital IDs have been the bedrock of many a new digital industry, such as fintech in India, they have some disadvantages.

Digitalisation does, of course, help reduce duplication of work, bring together multiple databases, and minimise fraud. It is not the technology of digitalisation that is inherently problematic, it is the fact that digital IDs potentially allow government and private surveillance of people and unfair exclusion.

Digital IDs can facilitate the linking of various databases. This linked data can provide a complete picture of a person and their behaviour. Without adequate encryption and security, such over-linking of data through digital IDs can be a powerful weapon in the hands of the state. India's biometric ID, Aadhaar, has been embroiled in controversy since it was proposed. Recently, there have been reports of Aadhaar data being used by the ruling party to micro-target voters in an election.⁸⁰

The other problem with digital IDs is that when welfare is tied to a compulsory digital ID, it can exclude people from services that they are entitled to. Malfunctioning of digital systems, faulty design, poor infrastructure and poor training of personnel can all lead to exclusion.⁸¹ While we will not go into detail on this issue here as it is outside the scope of surveillance, it is worth mentioning that very often the solution to leakages or corruption in public services delivery cannot be solved through digital IDs. Where technological solutions might serve better purposes is at the rationalisation and modernisation

**CRITICS ALSO
POINT OUT THAT
THE GATEWAY
WILL ALMOST
CERTAINLY LEAD
TO INSPECTION OF
CONTENT, AFFECTING
CAMBODIAN CITIZENS'
RIGHT TO PRIVACY.**

of the backend of these services, such that public officials can run them smoothly and transparently. “Means testing”—where the government focuses excessively on excluding those it considers undeserving from welfare schemes—is hardly the panacea to the general inefficiency of these schemes.

Public private partnerships and surveillance

Private partnerships help governments carry out surveillance more efficiently. They also help governments access the latest technology and use it for mass surveillance.

The Intelligent Operations Center in the Philippines is an example of this type of partnership. The Davao city government partnered with IBM to build this Center as part of a smart city project.⁸² The Intelligent Operations Center facilitates video analytics and modern communication devices for the police. It aims to predict crime and target drug syndicates. The programme reportedly played a primary role in undertaking extrajudicial and targeted killings by the police.⁸³ Reportedly, this surveillance project also fed data into a facial recognition software. The system is also deployed to target minor crimes like jaywalking, and was allegedly used to target political opponents.⁸⁴ The system has now been replicated as an in-house system in the Philippines.

Perhaps the best-known private entity providing surveillance technology to governments is Palantir, a company that has worked with nearly the entire intelligence apparatus of the United States, and which also received funding from the CIA’s venture capital arm. Palantir integrates and analyses

THE INTELLIGENT
OPERATIONS
CENTER FACILITATES
VIDEO ANALYTICS
AND MODERN
COMMUNICATION
DEVICES FOR THE
POLICE. IT AIMS
TO PREDICT CRIME
AND TARGET DRUG
SYNDICATES. THE
PROGRAMME
REPORTEDLY PLAYED
A PRIMARY ROLE
IN UNDERTAKING
EXTRAJUDICIAL AND
TARGETED KILLINGS
BY THE POLICE.

data from various intelligence agencies and presents insights to them. It uses social media data in its analysis as well, and has also been involved in brutal and excessive

police action in the US.⁸⁵ Over the past few years, it has become clear that Palantir helped the National Security Agency improve XKEYSCORE, a tool that is used worldwide to spy on online activities. The range and capabilities of this tool were first exposed by Edward Snowden in 2013.⁸⁶

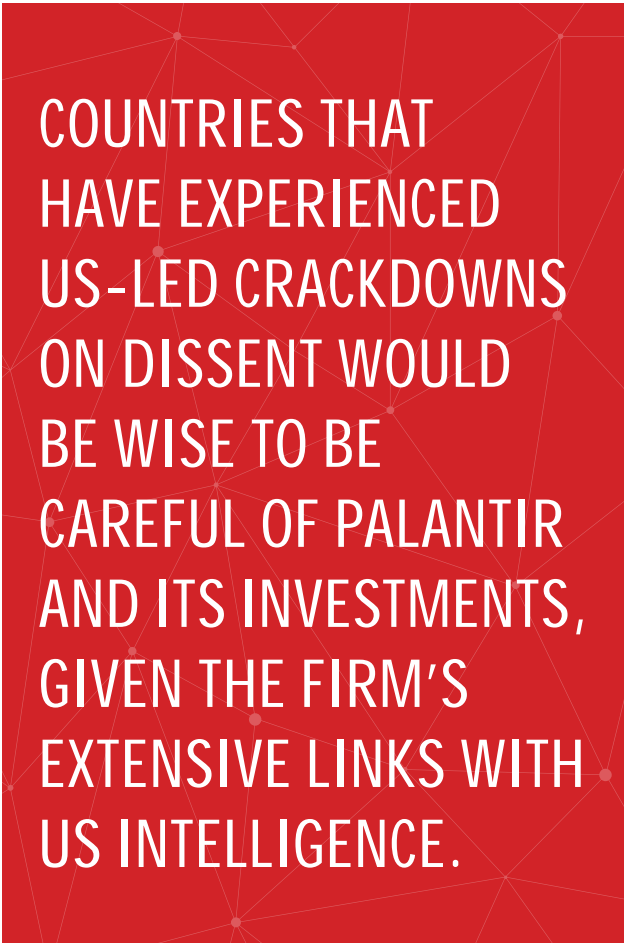
In February 2019, India's largest retailer Future Group tied up with Palantir to analyse shopper behaviour.⁸⁷ Its other partnerships in Asia include AirAsia, Fujitsu and Yamato Holdings. In November 2020, Palantir announced a joint venture with Sampo Holdings, a Japanese insurance company. In Japan, it aims to sell its software to "big companies and government agencies".⁸⁸ The motivation for its investment with Sampo Holdings seems to be a wish to expand into the field of healthcare. Recently, public health agencies in the US and the UK have been criticised for handing over confidential patient data to Palantir to track Covid-19 related indicators.⁸⁹ Countries that have experienced US-led crackdowns on dissent would be wise to be careful of Palantir and its investments, given the firm's extensive links with US intelligence.

The other large supplier of surveillance solutions to governments has been the Israeli company NSO Group. Its malware Pegasus can read extensive amounts of private data from targeted smartphones and is able to turn on a targeted phone's camera and microphone. It has been used by governments of various countries. The company claims that it only sells its solutions to "authorised governments".⁹⁰

In 2019, it was revealed that Pegasus was used to target Indian activists and journalists,

including anti-caste activists. In 2021, a consortium of news agencies revealed a list of persons suspected to have been spied on using Pegasus. Many of these cases were verified via forensic analysis of phones.⁹¹ The software used a vulnerability in WhatsApp to collect data from phones. The list of names includes prominent opposition leaders, journalists, trade unionists and complainants against a former Chief Justice of India. Many of the targeted activists have been pursued by the government for alleged "anti-national" activities.⁹² In addition to India, Pegasus has been used to target activists in Morocco, Mexico, and Saudi Arabia. Citizen Lab detected Pegasus use in 45 countries.⁹³

In Thailand, Pegasus was reportedly used by the state to target at least 17 dissidents.⁹⁴



COUNTRIES THAT
HAVE EXPERIENCED
US-LED CRACKDOWNS
ON DISSENT WOULD
BE WISE TO BE
CAREFUL OF PALANTIR
AND ITS INVESTMENTS,
GIVEN THE FIRM'S
EXTENSIVE LINKS WITH
US INTELLIGENCE.



Students using their smartphones while seated along the riverside in Phnom Penh by AFP Photo

The NSO Group is now pitching Covid-19 contact tracing solutions to governments, creating an obvious cause for concern.⁹⁵ The Thai government also reportedly purchased surveillance software from an Italian organisation in 2013 to perform functions similar to those performed with the Pegasus software.⁹⁶ These operations are coordinated under a cyber warfare unit that is part of the Thai military.⁹⁷

In another example of public-private surveillance collaboration, Thailand has enlisted its Internet Service Providers into monitoring encrypted traffic and sharing metadata with the government.⁹⁸ It has primarily used provisions under the Computer Crime Act to do so.⁹⁹

Covid-19 contact tracing, monitoring and surveillance¹⁰⁰

To control the spread of Covid-19, health administrations in many countries traced the contacts of infected people in order to test them and isolate them if necessary. Both public and private actors developed Covid-19 contact tracing apps. These include India's Aarogya Setu app, the Philippines' StaySafe app, Cambodia's "Stop Covid-19" QR Code system, and Thailand's Mor Chana app.

India's Aarogya Setu app was released by the Government of India in April 2020. The Ministry of Home Affairs soon released guidelines making the app mandatory for all public and private employees in containment

zones. This was followed by the app being made mandatory for many different groups of people, including travellers. In some cases the communication from the government was mixed on whether installing the app was compulsory or merely advised. Many employers, prominently those employing gig workers, made the app mandatory for their workers, and many private residential complexes made the app mandatory for outsiders wishing to enter the complex.¹⁰¹ The app was criticised by privacy activists and political leaders for having inadequate privacy safeguards. The app does not have an end date for data retention, and as it collects sensitive data such as location and health status, this leaves it open for abuse even after the pandemic recedes.¹⁰² In April 2021, it was revealed that sensitive data from the app was shared with police in Jammu and Kashmir.¹⁰³

In response to criticism about the app's opacity, the government released some snippets of code, which turned out to not include any code related to data handling by the app.¹⁰⁴ A further

danger of surveillance was presented when India's National Health Authority announced that vaccination centres would verify people's identities using facial recognition technology.¹⁰⁵ It is unclear whether these plans materialised in any vaccination centre.

The Philippines mandated the use of the StaySafe app in national and local government organisations in November 2020. This app had multiple issues related to privacy and accountability. The government encouraged private establishments to integrate their contact tracing data with the app.¹⁰⁶ It recruited a private app developer, Multisys, but ambiguities in its contract with the government mean that citizens cannot pinpoint a specific government agency that is accountable for the app. There is also no clear process for grievance redressal and opting out of the app.¹⁰⁷

Due to vulnerabilities, Citizen Lab was able to access the geolocation data of thousands of users of the StaySafe app. After this revelation,

MANY EMPLOYERS, PROMINENTLY THOSE EMPLOYING GIG WORKERS, MADE THE APP MANDATORY FOR THEIR WORKERS, AND MANY PRIVATE RESIDENTIAL COMPLEXES MADE THE APP MANDATORY FOR OUTSIDERS WISHING TO ENTER THE COMPLEX. THE APP WAS CRITICISED BY PRIVACY ACTIVISTS AND POLITICAL LEADERS FOR HAVING INADEQUATE PRIVACY SAFEGUARDS.

the data was better secured.¹⁰⁸ Concerns about unmitigated data sharing from the app were raised to the Department of Health.¹⁰⁹ Concerns about the indefinite storage of data gathered using the app remain unaddressed.

In February 2021, the Cambodian government rolled out a QR code system for businesses to use so that the movements of customers could be tracked.¹¹⁰ The system notifies people if a place they recently visited was also visited by a Covid positive person. Such tracking presents privacy risks without appropriate safeguards such as periodic data deletion, limiting the visibility of the data, etc.

The government of Thailand took over the technology of the Mor Chana contact tracing app in January 2021. The app reportedly has encryption safeguards built in, and does not display names of users to most authorities. However, it has been criticised for having no clear privacy policy and thus endangering user trust.¹¹¹ In the southern Patani region, the government was criticised for continuing its mass DNA collection drive to identify insurgents despite the risks of infection that this entails during the pandemic.¹¹²

Other countries in the region have also extensively used contact tracing apps. Malaysia's MySejahtera app is used to monitor health conditions and facilitate contact tracing. It appears that this app deletes data after 30 days.¹¹³ In addition to apps, Malaysia used digital IDs to carry out contact tracing and enforce travel restrictions. It even used drones to monitor movement during its version of the lockdown. These drones would click pictures and record videos over marketplaces and residential areas.^{114 115} Indonesia's contact tracing app PeduliLindungi collects location data and also

**IN THE SOUTHERN
PATANI REGION,
THE GOVERNMENT
WAS CRITICISED FOR
CONTINUING ITS MASS
DNA COLLECTION
DRIVE TO IDENTIFY
INSURGENTS DESPITE
THE RISKS OF
INFECTION THAT THIS
ENTAILS DURING THE
PANDEMIC.**

incorporates a facial recognition system that can determine whether a user is wearing a mask.¹¹⁶

Health data is particularly susceptible to misuse by both public and private actors. Increasingly, health insurance companies have begun to provide incentives to customers who "stay active" by tracking their physical activity through fitness tracking apps. Covid-19 health data, too, can be misused in various ways, particularly as it can reveal the movements of people. Data collection for contact tracing must be limited, have restricted availability, and be subject to public accountability.

SECTION II: PRIVATE SURVEILLANCE¹¹⁷

Automation of supervision has made surveillance of workers easier. Take the case of digital giant Amazon. Its orders are packed and sorted at ‘fulfilment centres’. Workers at these centres are tracked minutely using technology. They are also rated, warned and terminated using automated systems. The tracking of their work is so granular and unforgiving that workers often do not have time to use the bathroom. The Verge estimated that using these tracking mechanisms, it is likely that Amazon fired ten percent of its workforce every year simply because they fell below an exacting standard of productivity.¹¹⁸

Companies use surveillance—both social media tracking and CCTV—even to monitor workers’ moods and opinions.¹¹⁹ Amazon already has patents for wrist devices that track workers’ hand movements.¹²⁰ It has also launched a workplace surveillance tool that uses CCTV footage and computer vision technology to track

whether workers maintain social distancing.¹²¹ There are serious implications of such surveillance. It puts the onus of ideal behaviour and avoiding virus contraction on the workers, and can be used for purposes other than the ones intended, such as to pressure workers into working faster or to monitor unionisation.



Amazon Warehouse by Scott Lewis

Contact tracing and other measures taken to manage Covid-19 infections have meant that gig workers too have faced increased surveillance. For example, food delivery workers are subject to constant checking of body temperature, which is even revealed to customers, whereas customers are not required to undergo the same treatment. Workers' location is tracked even when they are not at work.¹²² Uber compels its drivers to click pictures to verify that they are wearing masks, but does not have the same verification mechanism for customers.¹²³ Many of these measures are required only from workers because it is clear that customers would object to invasive tracking of this nature.

As several countries announced lockdowns to control the pandemic, many office workers started working from home. Employers chose to implement surveillance software to track these workers' productivity and ensure that they were not "slacking". Workplace monitoring software has been in extensive use even before the pandemic, but the pandemic increased the pace of adoption. This software can track keystrokes, the time between keystrokes, the time spent away from the computer, track location, review files, record audio, and can also take regular screenshots or record screens.

In March 2020, Gartner conducted a webinar poll for Asia Pacific that indicated that 91 percent of attending HR leaders had implemented work from home arrangements.¹²⁴ In India, workers reported that they are required to keep their video cameras on during work hours.

There is barely any practice of allowing workers to consent to a tracking software. Many tracking software programmes can



**MANY TRACKING
SOFTWARE
PROGRAMMES CAN
ALSO BE INSTALLED
AND IMPLEMENTED
WITHOUT THE
WORKERS'
KNOWLEDGE.**

also be installed and implemented without the workers' knowledge.¹²⁵ In any case, we can hardly expect free and uncoerced consent from a worker to an activity proposed by her employer, given that the consequence of denying consent can easily be unemployment. In a work from home context, this coercive surveillance can extend to the employee's family as it is difficult to separate living and working arrangements at home.

Excessive work monitoring has adverse effects on workers' physical and mental health. They might overwork themselves and burn out. They can also experience high levels of stress, which can turn into chronic stress, particularly if the work involves low discretion but high monitoring.¹²⁶

It is no wonder that employers are seeing an increase in business productivity after a shift to work from home models.¹²⁷ This increase in productivity hides an increase in exploitation and decrease in worker welfare.

SECTION III: AGENDA FOR ACTION

Given the extensive surveillance challenges facing these countries today, progressive actors from all fields would benefit from rallying behind certain positions. As states become more and more hostile to progressive activism and as workers' rights erode, the act of "being watched" assumes new dangers. The following is a non-exhaustive list of important demands that can be considered.

A comprehensive personal data protection law

People must have legal recourse to surveillance by the government and private sector. A data protection law sets out the conditions under which personal data can be collected, processed and shared. It can

contain principles that limit data collection to a specified purpose, require consent for data collection, processing and sharing, mandate security standards for data storage, and so on. Thailand (pending implementation) and the Philippines have already enacted general data protection laws, while Cambodia and India are yet to enact theirs. Data protection legislation



A "Bridge to Health" divides India by Heinrich Böll US

**BUT WE NEED TO ASK
IF FINANCIALISATION
OF NEW AREAS OF
THE ECONOMY, AND
NEW METHODS OF
INDEBTEDNESS,
ARE ENDEAVOURS
WORTHWHILE ENOUGH
TO JUSTIFY CREATING A
MASS SURVEILLANCE
PROGRAMME.**

also draws the boundaries of surveillance by private actors. For example, the National Privacy Commission of the Philippines held that employee monitoring could only be done in conformity with the provisions of the Data Protection Act, which means that the monitoring would have to be proportional to requirements rather than excessive. It also held that companies should consider monitoring methods that intrude less on privacy.¹²⁸

New workers' rights against surveillance

Trade unions will find that this is an opportune time to arrive at positions on workers' rights

against surveillance. This applies to both blue-collar and white-collar workers. Whether in factories, warehouses, while delivering items or while working from home, workers are being increasingly subjected to minute surveillance. A pushback against this must take the form of demanding that such surveillance be minimised, and where it is carried out, demanding that the data collected be made transparent. Often such data can be beneficial to the workers' own case for benefits as it demonstrates productivity.

Taking stock of the private benefits of mass surveillance

Mass surveillance programmes may very often be instituted because they provide valuable resources for the private sector. Many digital ID and health ID projects seem to be instituted for this reason. Authentication using such IDs can make identification processes smoother for the private sector. In some cases, authentication difficulties can be reduced by loosening regulations around authentication rather than creating a national digital ID system. In other cases, the social value of these businesses is itself called into question. For instance, Aadhaar has been the basis of "Know Your Customer" verification for new financial technology businesses in India. But we need to ask if financialisation of new areas of the economy, and new methods of indebtedness, are endeavours worthwhile enough to justify creating a mass surveillance programme.¹²⁹ The causes of poverty and deprivation often lie elsewhere.

Data collected from such programmes can aid in business decision-making. Health IDs and

THE FLIP SIDE OF DIGITAL SOVEREIGNTY IS EXCESSIVE CONTROL BY THE NATIONAL GOVERNMENT. SUCH EXCESSES CAN BE ALLAYED THROUGH A PARTICIPATORY SYSTEM OF INTERNET GOVERNANCE, WHERE RESIDENTS AT THE LOCAL AND NATIONAL LEVELS PROVIDE BINDING INPUT TO REGULATORS ON VARIOUS ASPECTS OF INTERNET GOVERNANCE THROUGH COUNCIL MEETINGS, TOWN HALLS, RANDOM SAMPLE VOTING, AND OTHER METHODS.

digitalisation of health data in particular can serve as a goldmine for business. There needs to be greater public deliberation and participation in determining the acceptable trade-off between privacy and the benefits of digital intelligence, as well as ensuring that these benefits are distributed in equitable ways. If it is determined that the intelligence derived from data is valuable enough to be collected despite the privacy implications, the people's collective rights over their own data must be instituted through law. This would mean that people and their organisations can demand access to the data to develop their own solutions using it. India's proposed non-personal data policy is an example of such an attempt.¹³⁰

Where digital IDs are instituted, there should be a demand for decentralising and securing

data storage to minimise the chances of it being compromised, and also for transparency in any algorithms used to include or exclude people based on digital ID authentication.¹³¹

Sovereignty through participation

The Ukraine war saw many Western countries targeting Russia's digital infrastructure with the cooperation of private enterprises. Without commenting on the necessity of the sanctions, they made clear that some countries have an interest in maintaining digital sovereignty in the case of geopolitical conflicts. China's Great Firewall, Cambodia's proposed National Internet Gateway, Russia's attempt to separate its networks from the world, and the US government's insistence

that TikTok data of US citizens be stored inside the US—can all be seen as attempts to bolster digital sovereignty. The flip side of digital sovereignty is excessive control by the national government. Such excesses can be allayed through a participatory system of internet governance, where residents at the local and national levels provide binding input to regulators on various aspects of internet governance through council meetings, town halls, random sample voting, and other methods. The internet is an essential infrastructure for communication and the additional investment in ensuring its democratic regulation can be easily justified.

Data minimisation

The collection of large reams of behavioural data by private enterprises, most notably social media companies, is a risk for many reasons. The first risk is the fact that these companies themselves glean insights about people's behaviour, and this has adverse impacts on people's autonomy and market competition. The second risk is that the more data that is collected, the more it is vulnerable to being leaked or accessed by malicious actors. The third risk is the most relevant to this discussion – the more personal data that is collected, the more chance for governments to access it for purposes of suppression or manipulation. Private companies may or may not hand over this data to governments, but both scenarios present their own problems: those of public and private censorship respectively.¹³²

The only fool proof protection against surveillance is minimising the collection of data. Institutions are subject to capture and the most comprehensive laws are subject

to being ignored. But these institutions and laws are still important demands, because they limit the worst excesses of surveillance and improve public consciousness related to privacy. Nevertheless, progressive actors need to seriously consider different possible compromises between the incremental benefits of data collection and the incremental risk of surveillance. Some data collection has undoubtedly made our lives easier. Some has provided less clear benefits: for example, app-based contact tracing for Covid-19 has not worked spectacularly well in many countries, and even data-based ad targeting is not as effective as previously thought.¹³³

In this light, a reasonable position is that we should minimise the use of data and related technologies when the privacy harms are significant. When new policy challenges present themselves, it is worthwhile to conduct privacy risk assessments from a social point of view rather than for compliance reasons. Independent or civil society organisations can explore developing such assessments.

IN THIS LIGHT, A
REASONABLE POSITION
IS THAT WE SHOULD
MINIMISE THE USE OF
DATA AND RELATED
TECHNOLOGIES WHEN
THE PRIVACY HARMS
ARE SIGNIFICANT.

CONCLUSION

Surveillance challenges in all the four countries studied follow from the ubiquity of data generation and electronic communication today. Unmitigated state surveillance is sometimes legally sanctioned despite a constitutional right to privacy, and where restrictions on state action exist, they are more often than not ignored. National digital ID systems perform the dual functions of surveillance and resource-creation for the private sector. The involvement of the private sector has helped immensely in the development and expansion of oppressive state surveillance through partnerships that transfer technology to the state and protect it from legal implications. The Covid-19 pandemic has meant that state surveillance was ramped up in the guise of contact tracing, and is likely to remain after the pandemic has receded.

Surveillance by private entities over workers and employees has also risen rapidly. Workers of all types are now subject to being observed at all times of work, and their benefits can be tied to the conclusions drawn from such observations. Many times, these conclusions are drawn by automated systems and workers

are fired using these systems. This surveillance intensifies labour exploitation and leaves workers more vulnerable than before.

Progressive actors and civil society in the Asia Pacific region can rally around a few demands to ensure that the relentless march of surveillance is held back. Legal rights to data protection and privacy are crucial but not sufficient. Oftentimes, data collection and processing itself has to be stopped in its tracks. Assessments of privacy impact and the social value of data collection should be ramped up to allow people to determine whether they are willing to trade their privacy for certain benefits, and whether these benefits can be achieved through other means. At the same time, the people's rights to the following must be protected: (a) the right to privacy at work; (b) the right to use data generated by their own individual or collective actions; and (c) transparency of automated decision-making in data-based programmes such as digital IDs. In general, a participatory approach to digital sovereignty can help find a middle ground between national digital independence and national digital control.

ENDNOTES

- 1 UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Office of the High Commissioner for Human Rights. June 2019. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736&LangID=E>
- 2 Digital Development Dashboard. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx>
- 3 Jasmin Romero. PH gov't still 'very far' from achieving wider internet access: dev't study agency. ABS-CBN News. November 2021. <https://news.abs-cbn.com/spotlight/11/11/21/wider-internet-access-in-ph-still-a-problem-devt-study-agency-says>
- 4 Sofia Tomacruz, Bonz Magsambol. Two years later, what's changed with COVID-19 in the Philippines?. Rappler. March 2022. <https://www.rappler.com/newsbreak/iq/what-has-changed-covid-19-philippines-march-2022/>
- 5 Andreo Calanzo. Philippines sees limited economic impact from virus surge. Bloomberg News. March 2021. <https://www.bloomberg.com/news/articles/2021-03-15/philippines-sees-limited-economic-impact-from-virus-surge>
- 6 Sofia Tomacruz, Bonz Magsambol. *ibid.*
- 7 Kanak Mishra. Deconstructing the Philippines' New Anti-Terrorism Law. Jurist. August 2020. <https://www.jurist.org/commentary/2020/08/kanak-mishra-philippines-anti-terrorism-law/>
- 8 Digital Development Dashboard. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx>
- 9 Juthathip Jongwanich. Is Thailand ready for the digital economy? East Asia Forum. March 2022. <https://www.eastasiaforum.org/2022/03/17/is-thailand-ready-for-the-digital-economy/>
- 10 Thailand Digital Economy and Society Development Plan. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Apr-Digital2016/S2_Present_Pansak_Siriruchatapong.pdf; https://file.onde.go.th/assets/portals/1/ebookcategory/23_Digital_Thailand_pocket_book_EN/; https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Apr-Digital2016/S2_Present_Pansak_Siriruchatapong.pdf
- 11 Claudio Sopranzetti. The protests in Thailand are making history. Al Jazeera. October 2020. <https://www.aljazeera.com/opinions/2020/10/21/the-protests-in-thailand-are-making-history/>
- 12 Hannah Beech. (Bangkok): A Push for Parentheses Miffs Thais (Who Have Bigger Problems). The New York Times. April 2022. <https://www.nytimes.com/2022/04/02/world/asia/bangkok-thailand-krung-thep.html>
- 13 Subel Rai Bhandari. Young Thai activists adapt, get creative in protesting for monarchy reform. Benar News. March 2022. <https://www.benarnews.org/english/news/thai/adaptive-protests-03082022143956.html>
- 14 World Intellectual Property Organization. Global Innovation Index 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf
- 15 Harsh Mander. Harsh Mander: How many Indians actually died during the second Covid-19 wave?. Scroll. in. February 2022. <https://scroll.in/article/1018163/harsh-mander-how-many-indians-actually-died-during-the-second-covid-19-wave>
- 16 Neelanjan Sircar. In India, disinformation has emerged as a new form of state-sponsored violence. Scroll. in. October 2021. <https://scroll.in/article/1007070/in-india-disinformation-has-emerged-as-a-new-form-of-state-sponsored-violence>
- 17 Ameen Jauhar and Jai Vipra. Why India can't let private sector develop facial recognition tech for law enforcement. The Print. January 2022. <https://theprint.in/opinion/why-india-cant-let-private-sector-develop-facial-recognition-tech-for-law-enforcement/796468/>
- 18 The World Bank. Individuals using the Internet (% of population)—Cambodia. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=KH>
- 19 Reth Soeng and Ludo Cuyvers. The Telecommunications Sector and Its Impact on Cambodia's Services Export Performance. The International Trade Journal. July 2021, 1:1-21. <https://www.tandfonline.com/doi/abs/10.1080/08853908.2021.1943072>
- 20 Katrin Travouillon. COVID-19 worsens Cambodia's political oppression. East Asia Forum. January 2021. <https://www.eastasiaforum.org/2021/01/05/covid-19-worsens-cambodias-political-oppression/> and Mom Kunthear. Covid QR code logs 100K. The Phnom Penh Post. March 2021. <https://www.phnompenhpost.com/national/covid-qr-code-logs-100k>
- 21 Hanna Ritchie et. al. Cambodia: Coronavirus Pandemic Country Profile. Our World in Data. Accessed on April 25, 2022. <https://ourworldindata.org/coronavirus/country/cambodia>
- 22 Grace Li. 'Living with COVID' Cambodia jumps to 2nd in Nikkei Recovery Index. Nikkei Asian Review. February 2022. <https://asia.nikkei.com/Spotlight/Coronavirus/COVID-19-Recovery-Index/Living-with-COVID-Cambodia-jumps-to-2nd-in-Nikkei-Recovery-Index>

- 23 Darren Touch. Cambodia's State of Emergency Law and the Fight Against COVID-19. Asia Pacific Foundation of Canada. May 2020. <https://www.asiapacific.ca/publication/cambodias-state-emergency-law-and-fight-against-covid-19>
- 24 Prum Pheak. The Post's recap of 2020: A tumultuous road of a year. The Phnom Penh Post. December 2020. <https://www.phnompenhpost.com/national/posts-recap-2020-tumultuous-road-year>
- 25 Randle DeFalco. Opportunism, COVID-19, and Cambodia's State of Emergency Law. Just Security. August 2020. <https://www.justsecurity.org/71194/opportunism-covid-19-and-cambodias-state-of-emergency-law/>
- 26 Josep Prat. Cambodia Weaponizes COVID-19 in its Struggle Against Striking Workers. The Diplomat. March 2022. <https://thediplomat.com/2022/03/cambodia-weaponizes-covid-19-in-its-struggle-against-striking-workers/>
- 27 Joshua Kurlantzick. Who Will Benefit From Cambodia's New Oil Wealth?. World Politics Review. January 2021. <https://www.worldpoliticsreview.com/articles/29332/in-cambodia-oil-drilling-comes-online-but-who-will-benefit>
- 28 Galileo de Guzman Castillo. Cambodia COVID-19 Situationer. Focus on the Global South. June 2020. <https://focusweb.org/cambodia-covid-19-situationer/>
- 29 Cambodia to support SMEs and the agriculture sector. Khmer Times. February 2022. <https://www.khmertimeskh.com/501029437/cambodia-to-support-smes-and-the-agriculture-sector/>
- 30 Anne-Meike Fechter. Transnationalizing the 'Moral neoliberal'? Private aid initiatives in Cambodia. South East Asia Research. January 2020, 28(1):87-102. <http://sro.sussex.ac.uk/id/eprint/89964/2/Fechter%20Transnationalalising%20the%20Moral%20Neoliberal.pdf>
- 31 Cambodia: backsliding on human rights jeopardizes free and fair elections. Human Rights Watch. April 2022. <https://www.hrw.org/news/2022/04/04/cambodia-backsliding-human-rights-jeopardizes-free-and-fair-elections>
- 32 Republic Act No. 11479. Republic of the Philippines. <https://www.officialgazette.gov.ph/2020/07/03/republic-act-no-11479/>
- 33 Ibid.
- 34 Criselda Yabes. Philippines' anti-terror law poses a direct threat to democracy. Nikkei Asian Review. March 2022. <https://asia.nikkei.com/Opinion/Philippines-anti-terror-law-poses-a-direct-threat-to-democracy>
- 35 Ibid.
- 36 J.C. Gotinga and Aie Balagtas See. Philippines Supreme Court Strikes Down Anti-Terror Law Provision that Prevents Dissent. Benar News. December 2021. <https://www.benarnews.org/english/news/philippine/philippines-terrorism-law-12092021122921.html>
- 37 Kristine Joy Patag. Fact check: Lacson's defense of anti-terrorism law safeguard is 'misleading'. Philstar Global. April 2022. <https://www.philstar.com/headlines/2022/04/04/2172159/fact-check-lacson-defense-anti-terrorism-law-safeguard-misleading>
- 38 Alfred W. McCoy. Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State. University of Wisconsin Press. 2009. <https://history.wisc.edu/publications/policing-americas-empire-the-united-states-the-philippines-and-the-rise-of-the-surveillance-state/>
- 39 Samuel Woodhams. Social Media in Asia: A New Frontier for Mass Surveillance and Political Manipulation. The Diplomat. November 2019. <https://thediplomat.com/2019/11/social-media-in-asia-a-new-frontier-for-mass-surveillance-and-political-manipulation/>
- 40 Rick Bahague. Philippines. 2014 - Communications surveillance in the digital age. GIS Watch. <https://giswatch.org/en/country-report/communications-surveillance/philippines>
- 41 AFP. Philippines' Duterte blocks Bill to register social media users. The Straits Times. April 2022. <https://www.straitstimes.com/asia/se-asia/philippines-duterte-blocks-bill-to-register-social-media-users>
- 42 Caitlin Thompson. Duterte vetoes surveillance law in the Philippines, protects his troll farms. Coda. April 2022. <https://www.codastory.com/newsletters/philippines-sim-card-bill/>
- 43 Ibid.
- 44 Pinkaew Laungaramsri. Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand. Mass surveillance and the militarization of cyberspace in post-coup Thailand. Austrian Journal of South-East Asian Studies, 2016, 9(2), 195-214. <https://aseas.univie.ac.at/index.php/aseas/article/view/2648/2260>
- 45 Metadata is data about data. For instance, if the data includes messages, metadata can include the number of messages.
- 46 Danny O'Brien and Genny Gebhart. The Amended Computer Crime Act and the State of Internet Freedoms in Thailand. Electronic Frontier Foundation. December 2016. <https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand>
- 47 Thailand passes controversial cybersecurity law that could enable government surveillance. TechCrunch. February 2019. <https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/>
- 48 Thai Netizen Network and Privacy International. The Right to Privacy in Thailand. Stakeholder Report, Universal Periodic, 25th Session – Kingdom of Thailand. September 2015. https://privacyinternational.org/sites/default/files/2017-12/privacy_thailand.pdf

- 49 Thanakorn Wongpanya. 2019, a year to keep an eye on many laws, inheritance from the NCPD, entering the final phase of the NLA. The Standard. December 2018. https://thestandard.co.translate.googleusercontent.com/ncpd-legal-2019/?x_tr_sl=auto&x_tr_tl=en&x_tr_hl=en&x_tr_pto=wapp
- 50 Thailand's protests and their digital dimension. DW. October 2020. <https://www.dw.com/en/thailands-protests-and-their-digital-dimension/a-55315079>
- 51 Privacy International. The Right to Privacy in Thailand. Submission on the right to privacy in Thailand. February 2017. https://privacyinternational.org/sites/default/files/2017-12/HRC_thailand.pdf
- 52 Pinkaew Laungaramsri., ibid. <https://aseas.univie.ac.at/index.php/aseas/article/view/2648/2260>
- 53 Cabinet green-lights national network of 'anti-fake news' centres. The Nation Thailand. February 2022. <https://www.nationthailand.com/in-focus/40011798>
- 54 Chantip Tatiyakaroonwong. The Patani Panopticon: biometrics in Thailand's deep south. New Mandala. May 2020. <https://www.newmandala.org/the-patani-panopticon-biometrics-in-thailands-deep-south/>
- 55 Jack Brook. Phones require face scans in Thailand's Muslim Deep South. Globe. January 2022. <https://southeastasiaglobe.com/phones-scan-faces-in-thailands-muslim-deep-south/>
- 56 Justice K.S. Puttaswamy (Retd) vs Union Of India And Ors. on 24 August, 2017. Supreme Court of India. <https://indiankanoon.org/doc/91938676/>
- 57 State of Cyber Security and Surveillance in India: A Review of the Legal Landscape. Centre for Internet and Society. <https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf>
- 58 Rahul Tripathi. Interception of phone, computer data: the law, procedures and safeguards. The Indian Express. December 2018. <https://indianexpress.com/article/explained/interception-of-phone-computer-data-the-law-procedures-and-safeguards-5511051/>
- 59 What Enables the State to Disregard the Right to Privacy?. EPW Engage. January 2019. <https://www.epw.in/engage/article/what-enables-state-disregard-right>
- 60 No blanket permission given for surveillance under NETRA, NATGRID: Centre to HC. The Economic Times. February 2021. <https://economictimes.indiatimes.com/news/defence/no-blanket-permission-given-for-surveillance-under-netra-natgrid-centre-to-hc/articleshow/80706304.cms?from=mdr>
- 61 Gautam Bhatia. India's Growing Surveillance State. Foreign Affairs. February 2020. <https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state>
- 62 Ameen Jauhar. Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges. Vidhi Centre for Legal Policy. August 2021. <https://vidhilegalpolicy.in/research/indian-law-enforcements-ongoing-usage-of-automated-facial-recognition-technology-ethical-risks-and-legal-challenges/>
- 63 Abhijit Ahaskar. Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges. Livemint. February 2022. <https://www.livemint.com/technology/tech-news/smart-ai-based-systems-can-now-listen-to-gunshots-cries-for-help-11645558422045.html>
- 64 Ameen Jauhar and Jai Vipra. Procurement of Facial Recognition Technology for Law Enforcement in India: Legal and Social Implications of the Private Sector's Involvement. Vidhi Centre for Legal Policy. December 2021. <https://vidhilegalpolicy.in/research/procurement-of-facial-recognition-technology-for-law-enforcement-in-india-legal-and-social-implications-of-the-private-sectors-involvement/>
- 65 An Analysis Of The Criminal Procedure (Identification) Bill, 2022. Project 39A, National Law University, Delhi. <https://www.project39a.com/identification-bill>
- 66 Zoya Mateen and Meryl Sebastian. CPC: Criminal Procedure Identification Bill raises fears of surveillance in India. BBC News. April 2022. [https://www.bbc.com/news/world-asia-india-61015970#:~:text=The%20Criminal%20Procedure%20\(Identification\)%20bill,the%20president%20for%20his%20assent](https://www.bbc.com/news/world-asia-india-61015970#:~:text=The%20Criminal%20Procedure%20(Identification)%20bill,the%20president%20for%20his%20assent)
- 67 Constitution of the Kingdom of Cambodia. <https://www.refworld.org/docid/3ae6b5a40.html>
- 68 Full Text of Approved State of Emergency Draft Law. Agence Kampuchea Presse. April 2020. <https://akp.gov.kh/post/detail/29564>
- 69 Law on Telecommunications. <https://trc.gov.kh/en/laws/>
- 70 UNCTAD. Digital Identity for Trade and Development. 2020. https://unctad.org/system/files/official-document/dtlkdb2020d1_en.pdf
- 71 Cambodia blocks some independent news media sites: rights group. Reuters. July 2018. <https://www.reuters.com/article/us-cambodia-election-censorship/cambodia-blocks-some-independent-news-mediasites-rights-group-iduskbn1kh29q>
- 72 Jay Cohen, Pichrotanak Bunthan and Marina Sar. Cambodia—Data Protection Overview. Data Guidance. September 2021. <https://www.dataguidance.com/notes/cambodia-data-protection-overview>
- 73 Adrian Wan and Charles Mok. Internet Impact Brief: Cambodia National Internet Gateway. Internet Society. February 2022. <https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-cambodia-national-internet-gateway/>

- 74 Shaun Turton. Cambodia postpones 'national internet gateway' plan due to COVID. Nikkei Asian Review. February 2022. <https://asia.nikkei.com/Spotlight/Society/Cambodia-postpones-national-internet-gateway-plan-due-to-COVID>
- 75 Adrian Wan and Charles Mok. How Cambodia's Internet Gateway Will Harm the Internet. Internet Society. February 2022. <https://www.internetsociety.org/blog/2022/02/how-cambodias-internet-gateway-will-harm-the-internet/>
- 76 Human Rights Watch, ibid. <https://www.hrw.org/news/2022/04/04/cambodia-backsliding-human-rights-jeopardizes-free-and-fair-elections>
- 77 World Bank. The Digital Economy in Southeast Asia. 2019. <http://documents1.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf>
- 78 State of Privacy Philippines. Privacy International. January 2019. <https://privacyinternational.org/state-privacy/1009/state-privacy-philippines>
- 79 Tian Jiao Lim. Exclusive: Thailand's vision for trusted digital ID. GovInsider. August 2020. <https://govinsider.asia/transformation/thailands-vision-for-a-self-sovereign-digital-id/>
- 80 N Vinoth Kumar. Did BJP steal Aadhaar data to target Puducherry voters? EC to investigate. The Federal. March 2021. <https://thefederal.com/puducherry-elections-2021/did-bjp-steal-aadhaar-data-in-puducherry-to-target-voters/>
- 81 Reetika Khera. Aadhaar Failures: A Tragedy of Errors. EPW Engage. April 2019. <https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare>
- 82 Phoebe Magdirila. IBM Helps the Biggest City in the Philippines Transform to a Smart City. Tech In Asia. June 2013. <https://www.techinasia.com/ibm-helps-philippines-city-transform-into-smart-city>
- 83 George Joseph. Inside The Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte. The Intercept. March 2019. <https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/>
- 84 Ibid.
- 85 Sharon Weinberger. Techie Software Soldier Spy. New York Magazine. September 2020. <https://nymag.com/intelligencer/2020/09/inside-palantir-technologies-peter-thiel-alex-karp.html>
- 86 Sam Biddle. How Peter Thiel's Palantir Helped The NSA Spy On The Whole World. The Intercept. February 2017. <https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/>
- 87 Scary Data Mining Firm Palantir Meeting 'Future' of Indian Retail Doesn't Bode Well. Newsclick. February 2019. <https://www.newsclick.in/scary-data-mining-firm-palantir-meeting-future-indian-retail-doesnt-bode-well>
- 88 Wataru Suzuki. Palantir launches \$100m Asian venture with Japan's Somo. Nikkei Asian Review. November 2019. <https://asia.nikkei.com/Business/Technology/Palantir-launches-100m-Asian-venture-with-Japan-s-Somo>
- 89 Charles Piller. US scientists say diversion of epidemiological data to Palantir hinders public health goals. Privacy International. July 2020. <https://privacyinternational.org/examples/4184/us-scientists-says-diversion-epidemiological-data-palantir-hinders-public-health>
- 90 Thomas Brewster. Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Forbes. August 2016. <https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=70101c83997c>
- 91 Pegasus Project: 174 Individuals Revealed By The Wire On Snoop List So Far. The Wire. August 2021. <https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance>
- 92 Seema Chisti. WhatsApp confirms: Israeli spyware was used to snoop on Indian journalists, activists. The Indian Express. November 2019. <https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/>
- 93 Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. Hide and Seek. Citizen Lab. September 2018. <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>
- 94 Janjira Sombatpoonsiri. Digital Surveillance in Thailand: When Pegasus Takes Flight. Fulcrum. February 2022. <https://fulcrum.sg/digital-surveillance-in-thailand-when-pegasus-takes-flight/>
- 95 Pegasus Creator NSO Group Has A Covid-19 Software: Why You Should Be Worried. Hindustan Times. April 2020. <https://tech.hindustantimes.com/tech/news/pegasus-creator-nso-group-has-a-covid-19-software-why-you-should-be-worried-story-SMsYXKFoz90PG2VBIKrA8L.html>
- 96 Janjira Sombatpoonsiri, ibid. <https://fulcrum.sg/digital-surveillance-in-thailand-when-pegasus-takes-flight/>
- 97 Gerard McDermott. Thailand's Creeping Digital Authoritarianism. The Diplomat. February 2021. <https://thediplomat.com/2021/02/thailands-creeping-digital-authoritarianism/>
- 98 IU AJN. Internet providers are helping the Thai government track down dissidents. New Mandala. July 2020. <https://www.newmandala.org/internet-providers-are-helping-the-thai-government-track-down-dissidents/>
- 99 Ibid.

- 100 For a detailed list of contact tracing technology used by different countries, please see this compilation by Norton Rose Fulbright: <https://www.nortonrosefulbright.com/en-th/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy>
- 101 For a detailed list of when and for whom Aarogya Setu was made mandatory, please see this tracker developed by the Internet Democracy Project: <https://internetdemocracy.in/2020/05/aarogya-setu-tracker/>
- 102 Aarogya Setu Privacy Woes: Over 40 Organisations Push Back Against Mandatory Usage of COVID-19 App. The Wire. May 2020. <https://thewire.in/rights/aarogya-setu-privacy-woes-letter>
- 103 Gaurav Vivek Bhatnagar. Aarogya Setu Data Was Made Available to J&K Police in Kulgam, Reveals RTI. The Wire. April 2021. <https://thewire.in/government/aarogya-setu-data-was-made-available-to-jk-police-in-kulgam-reveals-rti>
- 104 Prasad Banerjee. Aarogya Setu Data Was Made Available to J&K Police in Kulgam, Reveals RTI. Livemint. November 2020. <https://www.livemint.com/technology/tech-news/experts-look-for-aarogya-setu-code-not-bits-of-it-11606178251490.html>
- 105 Himani Chandna. Modi govt now plans a 'touchless' vaccination process, with Aadhaar-based facial recognition. The Print. April 2021. <https://theprint.in/health/modi-govt-now-plans-a-touchless-vaccination-process-with-aadhaar-based-facial-recognition/634719/>
- 106 Gov't mandates use of StaySafe contact tracing app in local, national level. CNN Philippines. November 2020. <https://cnnphilippines.com/news/2020/11/27/StaySafe-contact-tracing-app-COVID-19.html>
- 107 R2KRN Special Report: Pandemic Of Apps. Action for Economic Reforms. June 2020. <https://aer.ph/r2krn-special-report/>
- 108 Pellaeon Lin, Jeffrey Knockel, Irene Poetranto, Stephanie Tran, Justin Lau, and Adam Senft. Unmasked II: An Analysis of Indonesia and the Philippines' Government-launched COVID-19 Apps. Citizen Lab. December 2020. <https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/>
- 109 Pia Ranada. Gov't goes full-throttle on StaySafe app, but user data concerns remain. Rappler. December 2020. <https://www.rappler.com/newsbreak/in-depth/government-full-throttle-staysafe-app-questions-remain-users-data>
- 110 Businesses in Cambodia advised to download "Stop Covid" QR code. Xinhua. February 2021. http://www.xinhuanet.com/english/asiapacific/2021-02/21/c_139757074.htm
- 111 Pichayada Promchertchoo. Data privacy concerns over Thailand's COVID-19 contact tracing app amid new wave of cases. Channel News Asia. February 2021. <https://www.channelnewsasia.com/news/asia/transparency-thailand-covid19-contact-tracing-app-mor-chana-14096014>
- 112 Chanatip Tatiyakaroonwong, ibid. <https://www.newmandala.org/the-patani-panopticon-biometrics-in-thailands-deep-south/>
- 113 MySejahtera privacy, safety concerns remain unaddressed. Focus Malaysia. June 2020. <https://focusmalaysia.my/mainstream/mysejahtera-privacy-safety-concerns-remain-unaddressed/>
- 114 Clara Bullock. Malaysian authorities use drones to curb spread of Covid-19. AirMed&Rescue. April 2020. <https://www.airmedandrescue.com/latest/news/malaysian-authorities-use-drones-curb-spread-covid-19>
- 115 Moonyati Yatid, Farlina Said and Tengku Nur Qistina. Digital surveillance: Privacy, data ecosystem and effectiveness. Khmer Times. May 2020. <https://www.khmertimeskh.com/50727689/digital-surveillance-privacy-data-ecosystem-and-effectiveness/>
- 116 Pellaeon Lin et al., ibid. <https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/>
- 117 For more examples of worker surveillance in the context of Covid-19, please see the compilation by Tandem research here: https://docs.google.com/spreadsheets/d/1NNaz4Q3P8rf7qSG50SA4Ru40IVqCGqng_Y_f0_evrao/edit?ts=5ec3aff0#gid=0 or navigate from the following link: <https://tandemresearch.org/blog/covid19-trackers-an-overview>
- 118 Colin Lecher. How Amazon automatically tracks and fires warehouse workers for 'productivity'. The Verge. April 2019. <https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations>
- 119 Shweta Mohandas and Deepika Nandagudi Srinivasa. The Boss Will See You Now—The Growth of Workplace Surveillance in India, is Data Protection Legislation the Answer? Centre for Internet and Society. December 2020. <https://cis-india.org/internet-governance/blog/the-boss-will-see-you-now-the-growth-of-workplace-surveillance-in-india-is-data-protection-legislation-the-answer>
- 120 Thuy Ong. Amazon patents wristbands that track warehouse employees' hands in real time. The Verge. February 2018. <https://www.theverge.com/2018/2/1/16958918/amazon-patents-trackable-wristband-warehouse-employees>
- 121 Sarah O'Connor. Commentary: Workplace surveillance may hurt us more than it helps. Channel News Asia. January 2021. <https://www.channelnewsasia.com/news/commentary/work-monitor-surveillance-tech-aws-panorama-safety-privacy-13943892>
- 122 Zoe Tabary and Avi Asher-Schapiro. Tech experts voice concerns of gig worker surveillance in pandemic. Reuters. November 2020. <https://www.reuters.com/article/us-tech-conference-gigworkers-trf-nidUSKBN27R2TT>

- 123** Ajeet Mahale. Uber announces new safety features amid COVID-19, masks now mandatory for both driver and riders. The Hindu. May 2020. <https://www.thehindu.com/news/national/uber-announces-new-safety-features-amid-covid-19-masks-now-mandatory-for-both-driver-and-riders/article31612490.ece>
- 124** Coronavirus in Mind: Make Remote Work Successful!. Gartner. March 2020. <https://www.gartner.com/en/documents/3981830/coronavirus-in-mind-make-remote-work-successful->
- 125** Matthew Finnegan. The New Normal: When work-from-home means the boss is watching. Computerworld. October 2020. <https://www.computerworld.com/article/3586616/the-new-normal-when-work-from-home-means-the-boss-is-watching.html>
- 126** Sarah O'Connor, ibid. <https://www.channelnewsasia.com/news/commentary/work-monitor-surveillance-tech-aws-panorama-safety-privacy-13943892>
- 127** Sammi Caramela. Working From Home Increases Productivity. Business News Daily. April 2022. <https://www.businessnewsdaily.com/15259-working-from-home-more-productive.html>
- 128** Cathrine Gonzales. Employers may monitor staff in work-from-home setup — NPC. Inquirer.net. June 2020. <https://newsinfo.inquirer.net/1286931/employers-may-monitor-staff-in-workhome-setup-npc>
- 129** Jai Vipra. Regulating AI in the Finance Sector in India. IT for Change and Friedrich Ebert Stiftung. February 2020. https://itforchange.net/sites/default/files/1625/Regulating%20AI%20in%20finance%20sector%20in%20India_0.pdf
- 130** Report by the Committee of Experts on Non-Personal Data Governance Framework. Ministry of Electronics and Information Technology. December 2020. https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
- 131** Srikanth. One Nation One Ration Card, PDS Interoperability — Technology demands. Medium. October 2020. <https://medium.com/karana/one-nation-one-ration-card-pds-interoperability-technology-demands-f25392edcccb>
- 132** Kristy Hughes. Free Speech in the Digital World under Threat?. Economic and Political Weekly, November 2012, Vol. 47, Issue 46. <https://www.epw.in/journal/2012/46/commentary/free-speech-digital-world-under-threat.html>
- 133** Natasha Lomas. The case against behavioral advertising is stacking up. TechCrunch. January 2019. <https://techcrunch.com/2019/01/20/dont-be-creepy/>



Surveillance has long been one of the primary threats to political and economic activism. Emerging digital technology interacts with the practice of surveillance to strengthen and broaden it, leading to retaliation and creating a chilling effect that protects entrenched interests. This report examines the role of digital technology in changing surveillance practices in the Asia-Pacific region, with a focus on Philippines, Thailand, India and Cambodia. It situates both state and private surveillance in the political context of these countries, and describes the nexus between the two. The report also elaborates upon the impact of the Covid-19 pandemic on surveillance in these countries.