ASEAN Regional Coalition to #StopDigitalDictatorship

Joint Submission to the High Commissioner for Human Rights on the Right to Privacy in the Digital Age

June 2022

FOR MORE INFORMATION ON THIS JOINT SUBMISSION, PLEASE CONTACT:

ALTSEAN-Burma Lead: Debbie Stothard
debbie.stot@gmail.com

Asia Indigenous Peoples Pact (AIPP) Lead: Gam Shimray
gam@aippnet.org

Cambodian Center for Human Rights (CCHR) Lead: Chak Sopheap
chaksopheap@cchrcambodia.org

Foundation for Media Alternatives (FMA) Lead: Lisa Garcia
lgarcia@fma.ph

ILGA Asia Lead: Henry Koh
henry@ilgaasia.org

Institute for Policy Research and Advocacy (ELSAM) Lead: Wahyudi Djafar
wahyudi@elsam.or.id

Manushya Foundation Lead: Emilie Pradichit
emilie@manushyafoundation.org

Southeast Asia Freedom of Expression Network (SAFEnet) Lead: Damar Juniarto
damarjuniarto@protonmail.com

Women's Peace Network Lead: Wai Wai Nu
waiwai.peace@gmail.com

Input for OHCHR Report on the right to privacy in the digital age

The right to privacy is an inalienable part of living in the digital age. With technology constantly shifting, and public and private actors becoming increasingly reliant on it, the opportunity for privacy abuses also widens. Privacy concerns are especially pertinent to struggling democracies, where ruling administrations frequently take advantage of technological advances to surveil, monitor, and collect data belonging to their citizens in the view of furthering their political agenda. Over the past years, such practice has proven commonplace in Southeast Asia. For the larger part of its history, the region has had a turbulent history with democracy and human rights. The problem reared its head following the boom of digital rights discourse around the world. It was not until 2010 that Southeast Asia saw its first legislative attempt at regulating digital privacy, thanks to Malaysia's Personal Data Protection Act. By that point, data protection had been on the move in some European countries for almost three full decades,[i] while legal development in North America was almost at the ten-year mark.[ii]

From mass surveillance, to data handover by tech companies, to invasive contact-tracing technologies, this Joint Submission looks at all the recent trends of digital privacy concerns in Southeast Asia, and their legal and policy implications. We develop this Joint Submission as the ASEAN Regional Coalition to #StopDigitalDictatorship (comprising Manushya Foundation, ALTSEAN-Burma, Cambodian Center for Human Rights – CCHR, ELSAM, SAFEnet, Foundation for Media Alternatives - FMA, Asia Indigenous Peoples Pact - AIPP, Women's Peace Network, and ILGA Asia). We will highlight privacy threats and challenges in nine countries, namely Cambodia, Indonesia, Laos PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand.

A. State-sponsored targeted and mass surveillance

The legal framework in Southeast Asian countries are rife with provisions which allow for State surveillance of online activities, interception of communications, and wholesale collection and retention of personal data. As a result, individuals find themselves being under the looming threat of being spied on without the possibility of protecting themselves or remedying any privacy violation which occurs due to surveillance measures.

In **Thailand**, several laws allow for surveillance and arbitrary searches and seizures on the basis of public order or national security, the most prominent being the 2007 Computer Crimes Act ("CCA"). It affords the government unfettered powers to surveil and access personal data without a court warrant or the need for independent oversight. It also contains no provision requiring notification to individuals that his or her data is subject to an ongoing investigation. Similar to the CCA, both the 2019 Cybersecurity Act and 2019 National Intelligence Act empower authorities to carry out mass surveillance on various grounds, including loosely-defined "national security", "economic security", "military security", and "public order". Amid protracted insurgency movements in the region, the government resorted to surveil Malay Muslims residing in the southernmost provinces ("Deep South").[iii] Local populations are monitored through various means, including CCTV cameras and forced collection of biometric data. As of 2021, a reported 8,200 surveillance cameras were being operated in the Deep South under the guise of preserving the safety of individuals.[iv]

In November 2021, a slew of Thai politicians, activists and academics received an email from Apple notifying them of possible 'state-sponsored attackers' who were remotely targeting their iPhones.[v] The news came after a 2018 report by The Citizen Lab of the University of Toronto which revealed Thailand's use of the notorious cyber-surveillance tool Pegasus spyware.[vi] The spyware is believed to still be in use to extract information and identifying data from devices belonging to dissidents all over the country as recently as February 2022.[vii]

In **Myanmar**, the Law Protecting the Privacy and Security of Citizens was enacted in 2017 as the authoritative instrument on privacy rights.[viii] Despite protection guarantees provided therein, the Law leaves open the possibility of State surveillance where it is authorized by the president or the authorities. The Law is also silent on the judicial review procedures to prevent data from being collected and stored illegally. On 13 February 2021, privacy safeguards granted under Chapter IV of the Law were suspended by the State Administration Council, the country's highest governing body post-military coup.[ix] Myanmar has other laws in place which similarly pose privacy risks, i.e. the 2013 Telecommunications Law and the 2021 amendment to the Electronic Transactions Law, both of which permit the authorities and the military to access private data in the interest of "national security" and allow for the prolonged retention of such data on servers designated by the State. On 13 January 2022, an amended draft of the Cybersecurity Law was circulated. It expands the scope of the previous draft, published in 2021, as to afford the junta sweeping powers to monitor citizens' online activities.[x] The 2022 draft prohibits the use of Virtual Private Networks (VPNs), which protects online anonymity, and therefore gives the junta leeway to spy on any critical voice in the digital space. Fines have been imposed against those who fail to comply with this prohibition.[xi]

With respect to technology for targeted surveillance, reports have surfaced that the government procured and is utilizing tools such as the phone-breaching product Cellebrite and FinSpy malware to collect data from smartphones belonging to journalists.[xii] The use of sophisticated technology is reported to have increased since the coup, with the 2020-2021 Ministry of Home Affairs budget allocating funds for the procurement of forensic data tools from Sweden which can download the content of mobile devices and recover deleted items, as well as a software to extract and collect data from Apple computers imported from the U.S.[xiii] Security forces have also located online critics by triangulating their social media posts and the individual addresses of their internet hookups.[xiv]

In **Malaysia**, the government resorted to surveillance tactics and technology to control the #Lawan protests, which took place in July 2021, over the government's handling of the COVID-19 pandemic. Firsthand accounts reveal police including those in plainclothes, taking close-up pictures and videos of protesters, and the deployment of drones and a helicopter during the protests.[xv]

In **Cambodia**, the National Internet Gateway ("NIG") Sub-Decree, signed into law in February 2021, permits surveillance of all internet activities, interception and censorship of communications, and retention of bulk personal data; the Sub-Decree is silent on the types of data which could be subject to retention or must be shared with authorities. While the NIG was planned to launch in February 2022, it has since been delayed to an unspecified date.[xvi] In September 2021, Cambodia also entered into a security deal with China, with whom it has had close ties in surveillance matters since years prior, as part of which the Chinese

government would supply new biometric surveillance and DNA screening equipment. While details of the deal remain unknown, it has been suggested that the technologies would emulate those used domestically in parts of China which had given rise to privacy and discrimination concerns.[xvii]

In **Laos PDR**, the government imposed a mandate for all citizens to register their SIM cards, an attempt at removing online anonymity. The deadline to do so, originally set to mid-2021, was extended to January 2022.[xviii] Those who fail to properly register would face disconnection.[xix] The registration process is to be done through an app developed by the Ministry of Post and Telecommunications called 3 Grab SIM Registration, which incidentally requires users to provide excessive permission such as access to contacts, GPS location, and device storage.[xx] Given the absence of data security regulation under the domestic legal framework, the deployment of such a tool could result in a disproportionate, and therefore illegitimate, interference with one's privacy.

In the **Philippines**, the SIM Card Registration Act was passed by the House of Representatives and Senate in March 2022. The Act would require citizens to register their SIM card prior to activation and register on social media platforms using their real names and phone numbers. In April, the Act was vetoed by President Rodrigo Duterte as he believes that the inclusion of social media in the measure "may give rise to a situation of dangerous state intrusion and surveillance".[xxi] While championed as a huge win for privacy rights, some critics believe that the decision was grounded in the President's attempt to protect administration-backed online trolls and bots, which have been furthering various State agendas since the country's general election in 2016.[xxii]

B. COVID-19 and digital contact-tracing and monitoring tools

The COVID-19 outbreak has prompted governments to put in place new laws, regulations, and measures which give rise to privacy risks. Increased reliance on technology to contain the spread of the virus, with little to no oversight, also fundamentally transforms the privacy rights landscape in Southeast Asia.

In **Vietnam**, privacy concerns arose as a result of Bluezone, the government's contact-tracing app. The app can silently transmit complete contact history and determine the real-world identity of users.[xxiii] Although information uploaded to the Bluezone app remains stored on the user's device as opposed to a government server, the app is still capable of harvesting information which could be used by the State to monitor interaction between individuals.[xxiv]

In **Indonesia**, the app PeduliLindungi was launched on 30 March 2020 as a surveillance tool to track the movement of persons exposed to COVID-19. Its Bluetooth feature allows the app to detect surrounding users and notify a user if they are or have been in a location designated as a coronavirus "red zone".[xxv] The app caused privacy issues given the lack of clarity regarding how data privacy and security is administered. It can access users' location and record their geolocation; camera to read users' photos and record videos; and storage to read other files on the device. Such storage access permission has been deemed as unnecessary to the overall functioning of the app.[xxvi] As per April 2022, PeduliLindungi's privacy policy maintains a no-liability clause for "violations or unauthorized access", despite the fact that the app is interconnected with third-party applications which can track users' movements.[xxvii]

PeduliLindungi has also been used to send personal data of users to PT Telkom, a State-owned telecommunication company with servers in Singapore.[xxviii]

In **Malaysia**, several tracing tools have been utilized since the wake of the coronavirus outbreak: Gerak Malaysia which tracks users' location, MyTrace which uses Bluetooth proximity data to trace contact, and MySejahtera which generates QR codes to be presented by individuals wishing to enter public spaces. MyTrace requests users to provide "device and app history" permissions which, if abused, could be used to read sensitive phone log data, and retrieve web bookmarks and history. The app's privacy notice does not specify how personal data is processed or the manners in which such permissions are used.[xxix]

On 24 March 2022, the Malaysian government disclosed, at a parliamentary hearing, its plan to sell MySejahtera to MySJ Sdn Bhd, a private firm allegedly owned by known political cronies, raising alam over the potential impact of the acquisition on the privacy of users.[xxx] Some suggest that MySJ has been the legal owner of MySejahtera, its intellectual property rights, and the platform through which the app operates since 2021, casting doubt as to which parties have been managing and accessing data of millions of users.[xxxi] Certain members of parliament have denied this suggestion.[xxxii]

In the **Philippines**, the Stay Safe PH app was adopted as the country's official "contact-tracing, health condition reporting, and social distancing system".[xxxiii] Experts immediately criticized the app for requiring excessive permissions (e.g. camera, device storage, and geolocation) and showcasing unclear standards in its privacy notice for how user information would be collected, used, and retained during COVID-19.[xxxiv] The app was later revealed to have been approved for use without technical vetting, and some law enforcement agencies - such as the National Bureau of Investigation - had access to user data.[xxxv] In January 2021, Multisys - the app's developer - announced its decision to remove the GPS and Bluetooth features of Stay Safe PH to ensure "zero surveillance" and increase public trust.[xxxvi] That same month, a report surfaced that a data transfer deal between Multisys and the Department of Health had not been carried out, despite having been planned since June the year prior. This means that user data stored within the app likely remained under the control of the technology firm and thus excluded from government protection.[xxxvii]

Without clarity on who has been in charge of its control, some suspect that the Stay Safe PH database could be used to manipulate voters ahead of the May 2022 general election. In June 2021, individuals came forward claiming that they had been receiving text messages alerting them about COVID-19 vaccinations and name-dropping the President and his daughter, both of whom were rumored to be running for office.[xxxviii] There are also fears of the database being used to track and monitor critical voices online, given the administration's history of cracking down on dissidents.[xxxix]

In **Singapore**, in response to the school closures caused by the COVID-19 pandemic, the government rolled out an initiative that aims to ensure all secondary school students in the country have a computer for home learning by the end of 2021. According to Singapore's Education Ministry, students must install tracking and remote access software on all laptops supplied under the national digital literacy program, as well as on their own devices used to attend online lessons. The rule poses significant risks to children's right to privacy, as the

software allows school officials and teachers to go through a student's web search history and remotely "view student screens [and] close distracting tabs" in order to "restrict access to objectionable material," both during and outside of school hours.[xl]

C. Monitoring of social media activities

Perhaps the most common method of surveillance in the region, the monitoring of accounts on social media platforms is mainly used to track critical voices and political oppositions and force them to align their online activities with State agenda. Social media, indeed, contains a wealth of information about a person's movements, habits, religious and political views, connections, and many more. Governments may conveniently collect and retain this information for targeting purposes.

In **Laos PDR**, the Ministry of Public Security issued a notice on 21 May 2021 indicating that a special task force had been set up to surveil, trace, and respond to "illegal online media" and "fake news" posted by both domestic and international actors.[xli] This new development is consistent with the Lao President's speech the month before in which he warned of people who "use social media to commit crimes, to destroy the country and to cause any disorder by undermining the unity, creating misunderstanding and creating any antagonistic parties in the country" and called on all security forces to make efforts against such actions.[xlii]

In **Myanmar**, the junta has turned to online messenger accounts operated by nationalist supporters to target and track down political opponents since it came to power. The method was used after junta supporters and the military itself were removed from Facebook after the coup in February 2021. Observers state that since the beginning of 2022, there has been a specific pattern of crackdown on anti-junta activists, with individuals being arrested following the publication of posts on accounts belonging so-called "pro-military social media personalities", giving rise to suspicions that the accounts are run by junta intelligence.[xliii] The police regularly confiscate mobile phones of persons detained on allegations of online crimes. Even prior to the coup, individuals would be demanded to hand over their social media passwords and provide access to other applications on their devices.[xliv]

In **Indonesia**, the government frequently monitors activities on social media platforms, including a Virtual Police program introduced in March 2021, which serves as a form of round-the-clock State surveillance.[xlv] Users-deemed "illegal content" can receive warnings asking for deletion of messages. Such massive online surveillance already existed in 2018 when a "war room" was created by the MCIT under the pretext of fighting "fake news", tasked to monitor social media platforms in real-time.[xlvi]

In **Cambodia**, social media monitoring is similarly rampant. In February 2021, the Ministry of Information announced that it was expanding its monitoring capabilities to include TikTok as well as closed-sourced platforms such as WhatsApp, Messenger, and Telegram to tackle so-called "fake news" surrounding COVID-19.[xlvii] This came after the Prime Minister alleged in November 2020 that the government had spied on social media chat groups across the country, which is in essence fear tactics to impose its rule over truth telling.[xlviii] Such a move effectively exposes all persons engaging in online activities to repercussions for criticizing the Royal Government.

In the **Philippines**, authorities have certain capacity to monitor social media platforms and users' activities. In 2018, the Armed Forces of Philippines created a social media monitoring cell to "counter misinformation by violent extremism organizations".[xlix] One year later, the Department of Information and Communications Technology (DICT) extended its efforts to thwart cyber-attacks by rolling out the Cybersecurity Management System to monitor cyberthreats, including to conduct social media monitoring that is performed in "near real time".[l] Additionally, police officers are instructed to monitor crimes, abuses, and false information on social media.[li]

In **Thailand**, the Ministry of Digital Economy and Society ("DES") is seeking to further monitor the usage of online activity and social media and considers linking users' registration on platforms with their ID cards. The DES Minister claimed that the move is aimed at promoting the digital economy and combating fake news and illicit content in the digital space.[lii] If implemented, the system would allow the authorities to collect and use publicly available social media data without explicit procedural safeguards.

D. Control over and requests for data handover to tech companies

Companies may act as proxy in committing privacy rights violations by handing over personal data of its users or subscribers to governments when requested. In some countries, domestic legislation exists to oblige companies to retain data and disclose it for law enforcement purposes. Such mandatory storage and surrender of user data to authorities by service providers violate users' rights, as authorities need not show proof of an immediate goal, or ensure that requests are made in specific and narrowly tailored circumstances in strict compliance with international standards.

In **Singapore**, a total of 1,831 Google accounts became subject to data handover requests by the government throughout the first half of 2020. From June to December that year, data of an additional 1,415 accounts were also demanded; Google complied with 84 percent of such requests. Facebook, on the other hand, received a whopping 2,296 requests concerning over 5,000 users throughout 2021. Its average compliance rate stands at 74 percent.[liii] These numbers constitute a sharp increase from previous years, likely due to increased online activity during the COVID-19 pandemic and the implementation of the 2019 Protection from Online Falsehoods and Manipulation Act, which aims to prevent the circulation of false information through electronic means. According to Facebook, the requests cover basic subscriber information including name, date of registration, and length of service. In some cases, the government may also seek to receive IP address logs and/or account content.[liv]

In **Thailand**, the Ministry of DES published regulations regarding the computer traffic data retention criteria for service providers on 13 August 2021. It requires telecommunication and broadcast carriers – including online application stores and social media service providers – to preserve internet traffic logs for 90 days in general cases; or up to six months but not longer than two years if required by relevant law enforcement agencies.[lv] This means that any exchange or publication of information made on Clubhouse, Telegram, Line, WhatsApp, Facebook, YouTube, Instagram or Google Drive are subject to state surveillance. These are among the main platforms used by pro-democracy activists and protesters to communicate and discuss the issues deemed hostile to the government. The service providers are obliged to keep numerous kinds of computer traffic data, including ID of users, users' activities in the

system, log-on and log-off, records of attempts to access the system as well as successful and unsuccessful data records, accessed files, amongst others.[lvi]

Facebook reported 164 requests for data regarding 273 users or accounts and provided 74 percent of the data requested from January to June 2020, while it received 103 requests for 136 users' information and complied with 69 percent of requests during the second half of the year. Throughout the first half of 2021, 309 requests regarding 390 users or accounts were recorded, with a median compliance rate of 63 percent.[lvii] Google showed lower levels of compliance, having responded to none out of the two requests it received in 2021.[lviii]

In **Myanmar**, telecommunications companies were prohibited from keeping the public informed about some directives issued by the military after the coup. As a result, the precise extent of official requests for users' data from service providers remain unknown. However, according to a February 2022 report, Norwegian telecoms company Telenor, who has become the leading operator in Myanmar with over 18 million subscribers, has been sharing copious amounts of sensitive user data with the junta since the coup. The report reveals that at least 200 requests were made to Telenor by the junta-controlled Ministry of Transport and Communications since the beginning of 2021. Requested information include records of calls, call locations, and last known location of a number. All of these requests were complied with.[lix] Telenor also announced, in mid-2021, a plan to sell its subsidiary, Telenor Myanmar, to military-linked operators.[lx] The proposed sale, which later gained a junta seal of approval, is feared to potentially risk data belonging to millions of customers being exposed.

Recommendations

In response to these trends, the **ASEAN Regional Coalition to #StopDigitalDictatorship** recommends the following on the basis of prevailing privacy rights principles and best practices:

To Governments

1. Develop effective safeguards against abuse of surveillance technologies, data collection and violation of online privacy, including by ensuring effective and independent oversight mechanisms are in place to limit unfettered executive discretion and establish redress mechanisms consistent with the obligation to provide victims of surveillance-related violations with adequate and effective remedy;
2. Repeal or otherwise amend laws which provide for overbroad executive powers to infringe on the right to privacy to bring them in line with the international human rights standards applicable to privacy rights derogation, i.e. necessity, proportionality, and legality;
3. Refrain from requiring or pressuring tech companies, internet service providers or other telecommunications companies to hand over user data in contravention of the right to privacy and ensure their compliance with their responsibilities to respect human rights in line with the UN Guiding Principles on Business and Human Rights (UNGPs) and the GNI Principles;
4. Provide transparent, detailed, and regular updates relating to data disclosure requests from government authorities to tech companies and internet providers, in a public and accessible manner, and information on legal proceedings or action taken against tech

companies and internet providers for failure to comply with such requests;
5. Refrain from imposing against tech companies, internet service providers or other telecommunications companies' disproportionate data retention mandates, including in responding to public health crises.

To Businesses

1. Ensure the companies' terms of service and policies are uniform and in compliance with international standards on freedom of expression and protection of data privacy, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological and societal developments, in line with the obligation to respect human rights under UNGPs;
2. Conduct assessments and due diligence processes to determine the impact of business activities on users, with respect to online freedom, privacy and data security;
3. Publish regular information on official websites regarding the legal basis of requests made by governments and other third parties and regarding the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own policies and community guidelines;
4. Provide users with clear data protection safeguards and adhere to the principles of data minimization, purpose and use limitation, limited access and data retention.

Endnotes

[i] In 1970, the German state of Hesse enacted the world's first Data Protection Act. Sweden followed suit with passing its own Data Act on 11 May 1973.

[ii] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) entered into force on 1 January 2001. In the U.S., the 1996 Health Insurance Portability and Accountability Act (HIPAA) and 1998 Children's Online Privacy Protection Act (COPPA) were some instruments which contain provisions on how personal data is stored and used.

[iii] Freedom House, *Freedom on the Net 2020: Thailand*, (2020), available at: https://freedomhouse.org/country/thailand/freedom-net/2020; Manushya Foundation, the Justice for Peace Foundation, the Thai CSOs Coalition for the Universal Periodic Review (UPR), and the Thai Business and Human Rights (BHR) Network, *Joint Civil Society Report: List of Themes to be considered by the Committee on the Elimination of Racial Discrimination (CERD)*, (2020), available at: https://www.manushyafoundation.org/joint-civil-society-report-cerd

[iv] Southeast Asia Globe, *Phones require face scans in Thailand's Muslim Deep South*, 31 January 2022, available at: https://southeastasiaglobe.com/phones-scan-faces-in-thailands-muslim-deep-south/ ; Chiang Rai Times, *Government Surveillance Crackdown in Thailand's Deep South*, 15 December 2021, available at: https://www.chiangraitimes.com/news/government-surveillance-crackdown-in-thailands-deep-south/

[v] Prachatai, *Apple ส่งอีเมลเตือนนักกิจกรรมไทย 5 ราย ระวังถูกแฮ็กเกอร์ที่สนับสนุนโดยรัฐโจมตี,* (24 November 2021), available at: https://prachatai.com/journal/2021/11/96088

[vi] The Citizen Lab, *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, (18 September 2021),* available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[vii] FULCRUM Analysis On Southeast Asia, *Digital Surveillance in Thailand: When Pegasus Takes Flight*, (24 February 2022), available at: https://fulcrum.sg/digital-surveillance-in-thailand-when-pegasus-takes-flight/

[viii] Security of Citizens, 2017, available at: https://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf

[ix] Clyde & Co, *Myanmar Amends Legislation on the Privacy and Security of Citizens amid State of Emergency*, (24 February 2021), available at: https://www.clydeco.com/en/insights/2021/02/myanmar-amends-legislation-on-

the-privacy-and-secu ("[b]ecause of the suspension of this section, any of the above actions by governmental authorities now appear to be lawful in Myanmar").

[x] Free Expression Myanmar, *Unofficial Translation of the Cyber Security Law (DRAFT),* (2022), available at: https://freeexpressionmyanmar.org/wp-content/uploads/2022/01/Cyber-Security-Bill-2022-EN.pdf

[xi] Cyber Security Law, 2021, available at: https://freeexpressionmyanmar.org/wp-content/uploads/2021/02/21-02-Draft-Cyber-Law-Unofficial-Translation.pdf

[xii] MIT Technology Review, *The spyware used by Arab dictators has now shown up in Myanmar*, (10 July 2019), available at: https://www.technologyreview.com/2019/07/10/65585/spyware-dealers-spotted-in-myanmar/

[xiii] Business and Human Rights Resource Centre, *Use of MSAB digital forensic tools in Myanmar exposes gap between EU tech investment & regulation*, (14 June 2021), available at: https://www.business-humanrights.org/en/latest-news/use-of-msab-digital-forensic-tools-in-myanmar-exposes-gap-between-eu-tech-investment-regulation/

[xiv] The New York Times, *Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown*, (1 March 2021), available at: https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html

[xv] FMT (Free Malaysia Today), *Authorities obstructed freedom of assembly at Lawan protest, say groups*, (1 September 2021), available at: https://www.freemalaysiatoday.com/category/nation/2021/09/01/authorities-obstructed-freedom-of-assembly-at-lawan-protest-say-groups/

[xvi] Security Week, *Cambodia Delays Controversial Internet Gateway*, (16 February 2022), available at: https://www.securityweek.com/cambodia-delays-controversial-internet-gateway

[xvii] VOA, *Surveillance Tools, DNA Screening Equipment Part of Cambodia's New Security Deal With China*, (6 October 2021), available at: https://www.voacambodia.com/a/surveillance-tools-dna-screening-equipment-part-of-cambodia-new-security-deal-with-china/6258369.html

[xviii] The Laotian Times, *Laos to Enforce Nationwide Sim Card Registration*, (24 June 2020), available at: https://laotiantimes.com/2020/06/24/laos-to-enforce-nationwide-sim-card-registration/

[xix] The Laotian Times, *Laos to Enforce Nationwide Sim Card Registration*, (24 June 2020), available at: https://laotiantimes.com/2020/06/24/laos-to-enforce-nationwide-sim-card-registration/

[xx] ASEAN Digest, *Laos Extends Deadline for SIM Card Registration*, (30 September 2021), available at: https://aseandigest.net/2021/09/30/laos-extends-deadline-for-sim-card-registration/

[xxi] CNN Philippines, *Duterte vetoes proposed SIM Card Registration law*, 15 April 2022, available at: https://www.cnnphilippines.com/news/2022/4/15/Duterte-vetoes-SIM-Card-Registration-act.html

[xxii] Rappler, *Investigating troll farms: What to look out for*, 17 July 2021, available at: https://www.rappler.com/newsbreak/iq/investigating-troll-farms-what-to-look-out-for/ ; Friedrich Naumann Foundation, *Fake Accounts, Bots, and Trolls: How Social Media influences Philippine's future*, 8 May 2022, available at: https://www.freiheit.org/southeast-and-east-asia/fake-accounts-bots-and-trolls-how-social-media-influences-philippines

[xxiii] App Assey, *Bluezone - Electronic mask*, (28 August 2020), available at: https://www.appassay.org/apps/bluezone

[xxiv] Southeast Asia Globe, *Vietnam's contact-tracing app: Public health tool or creeping surveillance?,* (29 September 2020), available at: https://southeastasiaglobe.com/bluezone-contact-tracing-app/

[xxv] Article 19, *13 human rights organizations raised concerns about the PeduliLindungi contact tracing app*, (26 June 2020), available at: https://www.article19.org/resources/indonesia-open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/

[xxvi] The Citizen Lab, *An Analysis of Indonesia and the Philippines' Government-launched COVID-19 Apps*, (21 December 2020), available at: https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/

[xxvii] EngageMedia, *PeduliLindungi: To Care for and Protect?*, (5 April 2022), available at: https://engagemedia.org/2022/pandemic-control-pedulilindungi/

[xxviii] EngageMedia, *PeduliLindungi: To Care for and Protect?*, (5 April 2022), available at: https://engagemedia.org/2022/pandemic-control-pedulilindungi/

[xxix] DPEX, *A Comparative Review of Contact Tracing Apps in ASEAN Countries*, (2 June 2020), available at: https://www.dpexnetwork.org/articles/comparative-review-contact-tracing-apps-asean-countries/

[xxx] MalayMail, *How MySejahtera's development became a data privacy concern: A timeline,* (2 April 2022), available at: https://www.malaymail.com/news/malaysia/2022/04/02/how-mysejahteras-development-became-a-data-privacy-concern-a-timeline/2051081

[xxxi] CodeBlue, *More Court Documents Show MySJ Owns MySejahtera Platform, IP Rights,* (4 April 2022), available at: https://codeblue.galencentre.org/2022/04/04/more-court-documents-show-mysj-owns-mysejahtera-platform-ip-rights/

[xxxii] SoyaCincau, *Khairy: Govt will not compromise confidentiality of MySejahtera user data, denies app is sold to private company,* (27 March 2022), available at: https://www.malaymail.com/news/malaysia/2022/04/02/how-mysejahteras-development-became-a-data-privacy-concern-a-timeline/2051081 ; MalayMail, *Khairy says MySejahtera app not sold to private companies, vows privacy remains protected*, (27 March 2022), available at: https://www.malaymail.com/news/malaysia/2022/03/27/khairy-says-mysejahtera-app-not-sold-to-private-companies-vows-privacy-rema/2049891

[xxxiii] Republic of the Philippines, Department of Interior and Local Government, DILG to LGUs, public: Use StaySafe.PH app to boost contact tracing, (30 March 2021), available at: https://dilg.gov.ph/news/DILG-to-LGUs-public-Use-StaySafePH-app-to-boost-contact-tracing/NC-2021-1062#:~:text=In%20April%202020%2C%20the%20National,reporting%2C%20and%20social%20distancing%20system.

[xxxiv] The Citizen Lab, *An Analysis of Indonesia and the Philippines' Government-launched COVID-19 Apps*, (21 December 2020), available at: https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/

[xxxv] EngageMedia, *From contact tracing to voter tracing? Risk of data misuse in the Philippines*, (4 February 2022), available at: https://engagemedia.org/2022/philippines-contact-voter-tracing/

[xxxvi] BusinessWorld, *Multisys's StaySafe.ph removes GPS, Bluetooth for data privacy*, (15 January 2021), available at: https://www.bworldonline.com/corporate/2021/01/15/338983/multisyss-staysafe-ph-removes-gps-bluetooth-for-data-privacy/

[xxxvii] Rappler, *Citizens' data collected by StaySafe app still in hands of private firm*, (21 January 2021), available at: https://www.rappler.com/nation/citizens-data-collected-by-staysafe-app-hands-of-multisys-private-firm/

[xxxviii] ABS-CBN News, *Palace disowns text alerts with Duterte-Duterte COVID-19 vaccine message*, (3 June 2021), available at: https://news.abs-cbn.com/video/news/06/03/21/duterte-duterte-covid-vaccine-text-message-2022-elections

[xxxix] EngageMedia, *From contact tracing to voter tracing? Risk of data misuse in the Philippines*, (4 February 2022), available at: https://engagemedia.org/2022/philippines-contact-voter-tracing/

[xl] Human Rights Watch, *Singapore Spying on Students' Laptops,* (5 February 2021), available at: https://www.hrw.org/news/2021/02/05/singapore-spying-students-laptops

[xli] Manushya Foundation, *Joint Statement Laos: The Lao Government Must Stop Online Surveillance and Mandatory Registration of Social Media Platforms*, (28 May 2021), available at: https://www.manushyafoundation.org/joint-statement-laos-govt-must-stop

[xlii] RFA (Radio Free Asia), *Laotians 'Confused' by President Urging Police Whistleblowing, Threatening Social Media Use*, (24 April 2021), https://www.rfa.org/english/news/laos/president-04122021153932.html

[xliii] RFA (Radio Free Asia), Myanmar junta using social media to track its opponents, (03 March 2022), available at: https://www.rfa.org/english/news/myanmar/social-media-03032022175020.html

[xliv] The New York Times, *Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown*, (1 March 2021), available at: https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html ; Freedom House, *Freedom on the Net 2020: Myanmar*, (2020), available at: https://freedomhouse.org/country/myanmar/freedom-net/2020

[xlv] Tempo.co, *State Uses Virtual Police for Mass Surveillance, SAFEnet Says*, (5 March 2021), available at: https://en.tempo.co/read/1439061/state-uses-virtual-police-for-mass-surveillance-safenet-says

[xlvi] Bloomberg, *Inside the Government-Run War Room Fighting Indonesian Fake News*, (24 October 2018), available at: https://www.bloomberg.com/news/articles/2018-10-24/inside-the-government-run-war-room-fighting-indonesian-fake-news.

[xlvii] UCA News, *Cambodia expands monitoring of 'fake news''*, (19 January 2021), available at: https://english.cambodiadaily.com/news/cambodia-expands-monitoring-of-fake-news-171922/

[xlviii] VOD, *Hun Sen says one in every five group chat participants spies for him*, (25 November 2020), available at: https://vodenglish.news/hun-sen-says-one-in-every-five-group-chat-participants-spies-for-him/

[xlix] Philstar, *US trains Philippine soldiers on social media monitoring*, (3 October 2018), available at: https://www.philstar.com/headlines/2018/10/03/1856933/us-trains-philippine-soldiers-social-media-monitoring

[l] Inquirer, *Israeli surveillance firm to build PH cybersecurity platform*, (17 January 2019), available at: https://technology.inquirer.net/82783/israeli-surveillance-firm-to-build-ph-cybersecurity-platform

[li] Republic of the Philippines, Philippine New Agency, *Cops urged to utilize social media as part of anti-crime efforts*, (14 February 2020), available at: https://www.pna.gov.ph/articles/1093722

[lii] Bangkok Post, *State mulls ID linkages for social media*, (31 May 2021), available at: https://www.bangkokpost.com/business/2124235/state-mulls-id-linkages-for-social-media

[liii] Facebook Transparency, *Government Requests for User Data*, (2021), available at: https://transparency.fb.com/data/government-data-requests/country/SG/

[liv] BBC, *Outcry as Google bans political advertising in Singapore as election looms*, (5 December 2019), available at: https://www.bbc.co.uk/news/world-asia-50668633 ; The Straits Times, *Google explains ban on political ads regulated under Pofma code of conduct in e-mail to SDP*, (5 December 2019), available at: https://www.straitstimes.com/politics/sdp-criticises-googles-ban-on-political-ads-regulated-under-pofma-code-of-conduct; Protection from Online Falsehoods and Manipulation Act (POFMA) Office, *Code of Practice for Transparency of Online Political Advertisements*, (2 October 2019), available at: https://www.pofmaoffice.gov.sg/documents/Political%20Advertisements%20Code%20and%20Annex.pdf.

[lv] The Royal Thai Government Gazette, *Notification of the Ministry of Digital Economy and Society on Criteria for the Retention of Computer Traffic Data by Service Providers B.E. 2561,* (13 August 2021), available at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF

[lvi] Bangkok Post, *Data legal upgrade sparks concerns,* (17 August 2021), available at: https://www.bangkokpost.com/business/2166227/data-legal-upgrade-sparks-concerns

[lvii] Facebook Transparency, *Government Requests for User Data*, (2021), available at: https://transparency.facebook.com/government-data-requests/country/TH

[lviii] Google Transparency Report, *Requests for user information*, (2020), available at: https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:TH;time:&lu=user_requests_report_period

[lix] Myanmar Now, *Telenor has shared sensitive customer data with military since the coup: industry sources*, (7 February 2022), available at: https://myanmar-now.org/en/news/telenor-has-shared-sensitive-customer-data-with-military-since-the-coup-industry-sources

[lx] Myanmar Now, *Telenor sale to military-linked consortium to be complete in mid-February*, (4 February 2022), available at: https://www.myanmar-now.org/en/news/telenor-sale-to-military-linked-consortium-to-be-complete-in-mid-february

About Us

Asia Indigenous Peoples Pact (AIPP)

The Asia Indigenous Peoples Pact (AIPP) is a regional organization founded in 1992 by indigenous peoples' movements. AIPP is committed to the cause of promoting and defending indigenous peoples' rights and human rights and articulating issues of relevance to indigenous peoples. At present, AIPP has 46 members from 14 countries in Asia with 18 indigenous peoples' national alliances/networks (national formations), 30 local and sub-national organizations. AIPP strengthens the solidarity, cooperation and capacities of indigenous peoples in Asia to promote and protect their rights, cultures and identities, and their sustainable resource management systems for their development and self-determination.

ALTSEAN-Burma

ALTSEAN-Burma was formed in October 1996 by a diverse network of organizations and individuals at the Alternative ASEAN Meeting on Burma, held in Bangkok. Their mission is to develop and strengthen strategic relationships among key networks and organizations from Burma, Southeast Asia, and the international community; support cooperation and partnership among activists, particularly women, youth, ethnic groups, LGBTQ+, displaced people, migrants, and other marginalized communities; implement innovative strategies that are responsive to emerging needs and urgent developments; and produce practical resources for these purposes. ALTSEAN has pursued its mission through advocacy, training and collaboration, focusing on women's participation and leadership, business and human rights, atrocity prevention, and broader human rights and democracy issues. ALTSEAN supports grassroots activists by ensuring local voices are heard at international strategy forums, including their robust analysis and policy recommendations.

Cambodian Center for Human Rights (CCHR)

CCHR is a leading non-aligned, independent, non-governmental organization that works to promote and protect democracy and respect for human rights — primarily civil and political rights - in Cambodia. It empowers civil society to claim its rights and drive for progress; and through detailed research and analysis it develops innovative policy, and advocates for its implementation.

Foundation for Media Alternatives (FMA)

Founded in 1987, the Foundation for Media Alternatives (FMA) assists citizens and communities, especially civil society organizations (CSOs) and other disadvantaged sectors, in the strategic and appropriate use of information and communications technologies (ICTs) for democratization and popular empowerment. FMA exists to enable the empowerment of civil society and social movements in the information age by advocating for democratic governance of ICTs; human rights in digital environments; equitable and safe access to and responsible use of ICTs; gender-transformative perspectives, policies and practices – through critical and meaningful engagement with development stakeholders.

ILGA Asia

ILGA Asia is the Asian Region of the International Lesbian, Gay, Bisexual, Trans, and Intersex Association, representing more than 190 member organizations across East Asia, South Asia, Southeast Asia, and West Asia. Our vision is a world where Asia is a safe place for all, where all can live in freedom and equality, be properly informed in the nature of sexual orientation and gender identity & expression and sex characteristic (SOGIESC) rights, have access to justice, and diversity is respected.

Institute for Policy Research and Advocacy (ELSAM)

The Institute for Policy Research and Advocacy (ELSAM) is a civil society organization that works to enhance the democratic political order in Indonesia by empowering civil society. Founded in 1993, it actively participates in efforts to promote human rights through policy and legal research, advocacy, and training.

Manushya Foundation

Manushya Foundation is a women-led and innovative non-profit organization with the goal to reinforce the power of local communities, in particular women human rights defenders, so they can advance their human rights and fight for equality and social justice. Manushya means “Human Being” in Sanskrit; it was founded in 2017 to engage, mobilize and empower local communities across Asia to be at the center of decisions and policies that affect them by: connecting humans through inclusive coalition building and; by developing strategies focused at placing local communities’ voices at the center of human rights advocacy and domestic implementation of international human rights obligations and standards. Manushya Foundation strengthens the solidarity and capacity of communities and grassroots to become

Agents of Change fighting for their rights and providing solutions to improve their lives, their livelihoods and the human rights situation on the ground.

Southeast Asia Freedom of Expression Network (SAFEnet)

SAFEnet is a network of digital rights defenders in Southeast Asia which was established on 27 June 2013 in Bali, Indonesia. The establishment of SAFEnet was motivated by the widespread criminalization of netizens because of its expression on the Internet after the enactment of Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). This prompted a number of bloggers, journalists, Internet governance experts, and activists to form this association. In 2018, SAFEnet began to widen the issue of advocacy towards the fulfillment of digital rights after previously only focusing on advocating freedom of expression on the Internet.

Women's Peace Network

Women's Peace Network is composed of lawyers, community leaders, and peace activists from Myanmar and around the globe who share a common goal: peacefully promote and protect human rights. They strive to ensure that Myanmar is a place where all people can enjoy peace, justice, and prosperity and live together harmoniously. They work to protect the rights, enhance the status, and increase the inclusion of marginalized women, youth, and communities in the Rakhine state and across Myanmar, so that they can live peacefully and prosperously.