UNITED NATIONS ESCAP / APCICT
Economic and Social Commission for Asia and the Pacific

Resource Materials on

DATA PRIVACY LAWS in the ASIA AND THE PACIFIC

Webinar on Data Privacy Laws in ASEAN

APCICT ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

ACKNOWLEDGEMENT

This resource document on DATA PRIVACY LAWS in the ASIA PACIFIC was prepared by Emmanuel C. Lallana, under the overall direction of Kiyoung Ko, Director of the Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP), and used as training material for the Webinar on Data Privacy Laws in ASEAN, jointly organized by the National Privacy Commission (NPC) of the Republic of the Philippines and APCICT/ESCAP, from 30 November to 3 December 2020.

TABLE OF CONTENTS

I. PRIVACY IN A DATA-DRIVEN WORLD[1]

In 2000, Sun Microsystems CEO Scott McNealy remarked that “Privacy is dead — get over it”.[2] A decade later, Mark Zuckerberg repeated that claim. According to him: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people."[3]

It is not surprising that technology industry leaders would say this because they helped create the situation. Ron Ross gives a succinct view of technology and privacy:

> We have built an incredibly complex information technology infrastructure consisting of millions of billions of lines of code, hardware platforms with integrated circuits on computer chips, and millions of applications on every type of computing platform from smart watches to mainframes. And right in the middle of all that complexity, your information is being routinely processed, stored and transmitted through global networks of connected systems.[4]

In sum, the digital technology revolution “has created a situation of severe tension and incompatibility between the right to privacy and the extensive data pooling on which the digital economy is based.”[5]

But what exactly is under threat as a result of the widespread diffusing of digital technologies?

Defining Privacy

There is no agreed upon definition of privacy.[6] In fact, it is argued that privacy is a contested concept - “where disputes about its ‘essence or central meaning’ are both paramount and central to the concept itself”[7]

---

1 by Emmanuel C. Lallana, PhD

2 Peter Timmin “Privacy is dead — get over it’” *Democratic Renewal* 19 APRIL 2006 Shttps://cpd.org.au/2006/04/privacy-is-dead-%E2%80%94-get-over-it/#:~:text=In%202000%2C%20Scott%20McNealy%2C%20CEO,dead%20%E2%80%94%20get%20over%20it'.

3 Bobbie Johnson “Privacy's dead: Facebook chief” *Sydney Morning Herald* January 19, 2010 https://www.smh.com.au/business/privacys-dead-facebook-chief-20100118-mgs8.html

4 Ron Ross “Why Security and Privacy Matter in a Digital World” *NIST* September 28, 2017 https://www.nist.gov/blogs/taking-measure/why-security-and-privacy-matter-digital-world

5 Tehilla Shwartz Altshuler “Privacy in a digital world” *TechCrunch* September 27, 2019 https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world/

6 Policy Brief: Privacy *Internet Society* 30 October 2015 https://www.internetsociety.org/policybriefs/privacy/

7 Deirdre K. Mulligan, Colin Koopman and Nick Doty (2016) “Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy” *Phil. Trans. R. Soc*. A.37420160118 https://royalsocietypublishing.org/doi/full/10.1098/rsta.2016.0118#:~:text=The%20meaning%20of%20privacy%20has,technological%20capabilities%20and%20social%20configurations.&text=Privacy%20is%20essentially%20contested.,changing%20technological%20and%20social%20conditions.

In Conceptualizing Privacy, Daniel Solove identified six approaches to privacy:

(1) *the right to be let alone* - views privacy as a type of immunity or seclusion - that Solove argues is a rather "broad and vague conception of privacy"
(2) *limited access to the self* - "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention." the "three independent and irreducible elements are: secrecy, anonymity, and solitude
(3) *secrecy* – concealment of information or the right to conceal discreditable facts about oneself.
(4) *control over personal information* - following Alan Westin, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others";
(5) *personhood* - constructed around a normative end of privacy, namely the protection of the integrity of the personality.
(6) *intimacy* - views privacy as consisting of some form of limited access or control, and it locates the value of privacy in the development of personal relationships. Following Julie Inness, it is "the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions."[8]

Solove argues that "Privacy is not one thing, but a cluster of many distinct yet related things". It ranges from "the control, use, and disclosure of personal information" to "surveillance, online gossip, identity theft, data security, online behavioral advertising, Big Data, access to records, use of cloud computing services, and much more".

Instead of a comprehensive definition, Solove proposes a taxonomy of privacy with four categories and, within them, sub-categories:

1. Information collection
    - Surveillance,
    - Interrogation
2. Information processing
    - Aggregation;
    - Identification;
    - Insecurity;
    - Secondary use and,
    - Exclusion
3. Dissemination of information
    - Breach of confidentiality;
    - Disclosure;
    - Exposure;

8 Daniel J. Solove "Conceptualizing Privacy" *California Law Review* Vol. 90:1087 (2005) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103

- Blackmail; Appropriation;
- Distortion

4. Invasion:
   - Intrusion;
   - Decisional interference

For Herman Tavani, there are four distinct kinds of privacy.[9] These are:

A. *Physical/Accessibility* - the freedom a person enjoys from sensory intrusion; focuses on the kind of harm that can be caused through physical access to a person or through access to a person's physical possessions; some have used the expression "accessibility privacy" to describe this view.
B. *Decisional* - freedom from interference in one's personal choices, plans, and decisions; Floridi defines decisional privacy as "freedom from procedural interference (that is) achieved thanks to the exclusion of others from decisions (concerning, e.g., education, health care, career, work, marriage, faith)
C. *Psychological/Mental* - protecting one's intimate thoughts. It is also described as "freedom from psychological interference" or when there is a "restriction on others' ability to access and manipulate others' mind."
D. *Informational* - "freedom from epistemic interference"; includes data about "one's daily activities, personal lifestyle, finances, medical history, and academic achievement."

ICT has affected informational privacy in four ways: (1) the amount of personal information that can be collected, (2) the speed at which personal information can be exchanged, (3) the duration of time that the information can be retained, and (4) the kind of information that can be acquired.

Helen Nissenbaum argues that the following three principles dominate public deliberation surrounding privacy: 1) limiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal.[10]

She believes that privacy should not be limited to concerns about control over personal information. Her concern is the flow or sharing of information. For Nissenbaum, information ought to be distributed and protected according to norms governing distinct social contexts—whether it be workplace, health care, schools, or among family and friends.[11] For instance, patients do not hesitate to share personal data with their doctors when seeking treatment and care. But these patients would be troubled if the information gathered by/shared with physicians will be given to pharmaceutical companies or other medical services related companies.

---

9 Herman T. Tavani "Informational Privacy: Concepts, Theories, and Controversies" (2008) in Kenneth Einar Himma and Herman T. Tavani (eds) *The Handbook Of Information And Computer Ethics* (Hoboken, New Jersey: John Wiley & Sons, 2008) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.4600&rep=rep1&type=pdf#page=166

10 Helen Nissenbaum "Privacy as Contextual Integrity" *Washington Law Review* p. 107 https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

11 Helen Nissenbaum "Contextual Integrity Up and Down the Data Food Chain *Theoretical Inquiries in Law* Vol. 20.1:22, p. 224

Nissenbaum proposes to understand privacy as contextual integrity. Contextual integrity means "compatibility with presiding norms of information appropriateness and distribution".[12] In her view, privacy has been violated if "norms of appropriateness" and "norms of flow or distribution" have been transgressed. Norms of appropriateness mean "what information about persons is appropriate, or fitting, to reveal in a particular context". Information that is collected in one situation but used in another situation can constitute privacy violation, while flow or distribution of information means movement, or transfer of information from one party to another. In the case of flow of information, what matters is whether the distribution of information respects contextual norms of information flow.

How does technology affect privacy as contextual integrity? Nissembaum believes that informational norms have not been completely upended by ICT: "As social contexts, activities, roles, and rules migrate online, respective context-specific values, ends, and purposes serve as standards against which information-sharing practices can be evaluated as legitimate or problematic".[13] However, ICT is "threatening to privacy because (it had) radically disrupted flows of personal information, from the corporate and governmental databases of the 1960s to the surveillance cameras and social networks of the present day." The Internet "has mediated disruptions of an unprecedented scale and variety".

The advantages of Nissenbaum's approach are:

- It takes culture into consideration. Privacy violations are determined by contextual informational norms ("privacy norms") which are shaped not only by place but by politics, convention, and cultural expectations. Privacy norms varies in different societies.
- There is no presumption in favor of privacy as secrecy, withholding information, or stopping flow. Data leakage or data collection are not necessarily privacy harms. Privacy as contextual integrity cares only whether the leakage or collection is appropriate.
- Privacy Norms are not fixed but evolve. They can be evaluated in terms of: A) Interests of Affected Parties, B) Ethical and Political Values, and C) Contextual Functions, Purposes, and Values.[14]

Privacy and the Pandemic

The threat of technology to privacy is apparent in the COVID-19 pandemic.

It has been suggested that as a result of the pandemic, the new global consensus is "less data privacy, not more, may be what's best for public health"[15]

12 Nissenbaum "Privacy As Contextual Integrity"

13 Helen Nissenbaum "A Contextual Approach to Privacy Online" *Daedalaus* Fall 2011 https://www.amacad.org/publication/contextual-approach-privacy-online

14 Contextual Integrity Up and Down the Data Food Chain https://nissenbaum.tech.cornell.edu/papers/Contextual%20Integrity%20Up%20and%20Down.pdf p. 225

15 Davide Meyer "More surveillance and less privacy will be the new normal after the coronavirus pandemic" *Fortune* April 20, 2020 https://fortune.com/2020/04/20/privacy-surveillance-coronavirus-pandemic-covid-19-tracking/

An alternative view is exemplified by the' National Privacy Commission (NPC) of the Republic of the Philippines:

> Data protection and privacy should not hinder the government from collecting, using, and sharing personal information during this time of public health emergency. Neither does the law limit public health authorities from using available technology and databases to stop the spread of the virus. The principles contained in the law allow the use of data to treat patients, prevent imminent threats, and protect the country's public health and still provide the level of protection the citizens expect. The Data Privacy Act of 2012 is an enabler in critical times like this.[16]

Finding the right balance is key. Asia provides important cases of balancing privacy and public health.

Contact Tracing - the process of locating individuals who have interacted with an infected person - has been a staple in the fight against infectious diseases. It has been successfully used to contain the outbreaks of measles, HIV, and Ebola. But traditional contact tracing is labor-intensive and time-consuming. Digital contact training (also known as proximity tracing), has made the process more efficient and effective but also privacy threatening.

This is seen in digital contact tracing in the Republic of Korea.

The Republic of Korea's amended Contagious Disease Prevention and Control Act (CDPCA) gave authority to the government to override the Personal Information Protection Act (PIPA) of 2011 during public health emergencies.[17] Under the amended CDPCA, government agencies can collect, profile, and share specified data of suspected and infected individuals. The data collected data can include location data (including location data collected from mobile devices); personal identification information; medical and prescription records; immigration records; transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and, closed-circuit television (CCTV) footage.

The law also directs that at the outbreak of a serious infectious disease, the Ministry of Health makes publicly available the following information about infected persons: the path and means of transportation; the medical institutions that treated them; and, the health status of those in contact with them. The disclosures on the ministry's website on COVID-19 patients include the aforementioned items as well as the gender, nationality, and age of infected persons. The names of infected persons, however, are not revealed.

Unfortunately, some local governments provided highly detailed routes traveled by an infected person as well as the names of restaurants, shops, and other business premises they visited. Also, the general public engaged in profiling and unveiled or inferred embarrassing personal details about them. As a result, some of these individuals suffered from unwanted privacy invasion and were subjected to ostracism. Restaurants, shops, and other business premises

16 https://www.privacy.gov.ph/2020/03/npc-phe-bulletin-no-3-collect-what-is-necessary-disclose-only-to-the-proper-authority/

17 Park S, Choi GJ, Ko H. "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies." JAMA. 2020;323(21):2129–2130. https://jamanetwork.com/journals/jama/fullarticle/2765252. The subsequent discussion is based on this article.

that infected individuals visited experienced abrupt loss of business.

How much information was disclosed? A study of publicly available contact tracing data of 970 COVID patients from seven metropolitan cities in the Republic of Korea (20 January to 20 April 2020) showed that:

1) gender and age of the patients were disclosed;
2) significant places (home/work) ranging across different levels of privacy risks in over 70 per cent of the cases were also disclosed;
3) Inference on sensitive information (hobby, religion) was made possible; and,
4) 48.7 per cent of the cases exposed the patient's social relationships.[18]

These developments led the Republic of Korea's National Human Rights Commission to issue a recommendation on the disclosure of personal data to enhance privacy protection on 9 March 2020 .[19] Within a week, the Korean Center for Disease Control issued guidelines to municipal and local governments that limited the scope and detail of the information to be disclosed.

A study of the Republic of Korea's digital contact-tracing through the lens of the four human rights principles (European Court of Human Rights' necessary, proportional, scientifically valid and time-bounded principles) revealed that "the use of the Republic of Korea's digital contact-tracing was scientifically valid and proportionate (albeit, in need for improvements), it meets the necessity requirement, but is too vague to meet the time-boundedness requirement".[20]

Most ASEAN member states use contact tracing apps. Lao PDR has *LaoKYC* which "monitors the activities and locations of infected individuals who are registered with the application, as well as informs individuals if they had been in close proximity with an infected individual".[21] Myanmar's *Saw Saw Shar* facilitates government's COVID-19 containment efforts, provides notifications on nearby potential high-risk areas with positive cases, and closest fever clinics and quarantine center.[22] Only Brunei Darussalam relies on manual contact tracing.[23] A study, which reviewed contact tracing smart apps used in five ASEAN countries, revealed the following:

- Singapore's *TraceTogether* comes up tops in terms of privacy communications and

18 Jung Gyuwon, Lee Hyunsoo, Kim Auk, Lee Uichin "Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea" Frontiers in Public Health vol 8:2020 https://www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full

19 Park, Choi, & Ko. "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea"

20 Mark Ryan "In defence of digital contact-tracing: human rights, South Korea and COVID-19" *International Journal of Pervasive Computing and Communications* 6 August 2020 https://www.emerald.com/insight/content/doi/10.1108/IJPCC-07-2020-0081/full/html

21 Lao PDR: MPT announces Coronavirus tracking mobile app and website *Data Guidance* 29 April 2020 https://www.dataguidance.com/news/lao-pdr-mpt-announces-coronavirus-tracking-mobile-app-and-website

22 "Myanmar Government Developed A COVID-19 Tracking App" *Eurocham Myanmar* 09 September, 2020 https://eurocham-myanmar.org/post/615/Myanmar-government-developed-a-COVID-19-tracking-App

23 Justin Wong, Wee Chian Koh, Mohammad Fathi Alikhan, Anita B Z Abdul Aziz, and Lin Naing "Responding to COVID-19 in Brunei Darussalam: Lessons for small countries" *Journal of Global Health.* June 2020 https://europepmc.org/article/med/32566154. It is important to note that Brunei's health surveillance system leverages on digital patient records in the national health information management system database that links all health care facilities with near 100% penetration of the population.

overall marks. It clearly takes into account data protection by design and data minimization principles. The privacy statement and accompanying documents explain clearly and in simple English (that is, not in legalese) what the TraceTogether app does, what type of personal data is collected and how it may be used or disclosed. Our review shows that the permissions the app seeks do not exceed its functionality and declared purposes. The few areas where it falls short tend to reflect the nature of an app such as the TraceTogether app rather than an inadvertent or careless departure from an obligation or principle.

1. Malaysia's *MyTrace* is similar to Singapore's TraceTogether in terms of functionality. However, the biggest issue is in its privacy notice which does not state how personal data is processed. It offers little explanation on how permissions are being used in the app.

2. Indonesia's *PeduliLindungi* offers the usual exchange of ID-related information via the mobile phone's Bluetooth signals with other mobile phones. However, unlike the previous apps, it requires the user's complete name during registration. The app also notifies users if they are in crowded areas or "zones" which creates concerns of constant surveillance by the government. It is unclear how users will share their contact history data with the government if there is an infected case. There is no upload button unlike the previous two apps. In addition, the app requires the camera permissions so as to enable a QR code scan web site URL. However, it is only applicable to overseas visitors at the immigration gate and for those participating in rapid COVID-19 tests. This is not clearly stated in either the privacy statement or terms and conditions. Hence, this permission would be considered excessive to the purpose of contact tracing.

3. Viet Nam's *Blue Zone* does not have a specific privacy notice or statement. This is not surprising given that the country does not have a data protection law. Besides the usual functionality found in contact tracing apps, what makes the app unique is that users can scan for other users although no personal information is revealed. While this may be intended to encourage participation by the government, it might cause concerns for users worried about their own privacy. Similarly, to Indonesia, it is also unclear how users will share their contact history data with the government in the case of an infection.

4. Thailand's *Mor Chana* app uses the most permissions. While there are no issues regarding its privacy notice in the pre-installation stage, there are concerns with its excessive use of permissions proportionate to its purpose of contact tracing and the additional purpose of self-assessment for any risk of infection. For example, it requires the camera permission (so that a selfie can be taken during registration). The reasons for these permissions are not explained in the privacy notice.

5. The Philippines' *StaySafe* app requires the most information during registration (name, age, location, gender, photo, company name), although it is not mandatory. It also allows the input of the user's family members as an option. This contradicts the privacy statement that assures that no personal information will be collected. Another potential excessive feature can be seen in the use of camera permission to allow the user to upload a photo, which is not related to the purpose of the app. Neither does the privacy

statement or documentation explain what this is used for.[24]

The concern over technology's threat to privacy during the pandemic led to the development of Privacy Protecting Digital Contact Tracing (PP DCT). PP DCT has three main characteristics:

1. Individuals cannot know who is infected, who is suspected, and who might have exposed them to the virus;
2. The only information individuals may receive is that they were exposed to the virus.
3. Governments cannot know who infected whom and where individuals have been. The only information available to governments or anyone else administering the system is a list of infected and suspected cases.[25]

Singapore's TraceTogether app is an example of PP DCT. This app works by exchanging Bluetooth signals among mobile phones that are in close proximity - defined as within two to five meters - for 30 minutes.[26] Records of these encounters are stored in the users' phones and are not sent to the government authorities. Users will only be asked to share these records when contacted by the Ministry of Health as part of contact tracing investigations. The TraceTogether app has the following privacy safeguards: 1) its use is voluntary; 2) users have to give "explicit consent" to participate in TraceTogether and this consent can be withdrawn anytime; 3) the app also uses temporary user IDs.[27]

The effectiveness of TraceTogether app was not as high as it could be due to low uptake. As a result, Singapore's government developed the TraceTogether Token - a wearable device with the same functionality as the similarly named contact-tracing app. It was developed to drive up digital proximity tracing participation rate to more than 75 per cent (from the current 25 per cent using the app in smart phones).[28] The Government of Singapore intends to give out 2.7 million tokens, particularly to children and the elderly who do not have a smartphone or the latest device for using the app.[29] The TraceTogether app or token will become mandatory to enter public places like cinemas, restaurants, workplaces, schools and shopping malls by the end of December 2020.[30]

The token works like the app - short-range wireless Bluetooth signals emitting from the token will be exchanged with nearby devices (either another token or a Bluetooth-enabled smartphone with the app). The exchange will be encrypted and logged in both devices. This data will be erased automatically after 25 days. The data will not be uploaded to a central server by default. Both the token and app do not collect location data.

---

24 "A Comparative Review of Contact Tracing Apps in ASEAN Countries", *DPEX* 2 Jun, 2020 https://www.dpexnetwork.org/articles/comparative-review-contact-tracing-apps-asean-countries/

25 Cansu Canca "Why 'Mandatory Privacy-Preserving Digital Contact Tracing' is the Ethical Measure against COVID-19" *Medium* April 10, 2020 https://medium.com/@cansucanca/why-mandatory-privacy-preserving-digital-contact-tracing-is-the-ethical-measure-against-covid-19-a0d143b7c3b6

26 Tang See Kit and Aqil Haziq Mahmud "Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts" *Channel News Asia* 20 March 2020

27 https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616

28 https://www.straitstimes.com/singapore/askst-how-new-token-and-app-will-address-privacy-concerns

29 Irene Than "TraceTogether token collection raises questions" Straits Times OCT 30, 2020 https://www.straitstimes.com/tech/tech-news/tracetogether-token-collection-raises-questions

30 Ibid

When a person tests positive for COVID-19, the Ministry of Health (MOH) will require token users to hand over the device in order to extract data logs for contact tracing. Smartphone app users will be guided to remotely upload data log to the MOH server. The government estimates that the use of these digital tools will cut the time needed to map a patient's contacts and issue quarantine orders from two to three days to less than a day.[31]

Data protection and privacy rules will apply to the data held by the MOH. These rules include purging data from the central database or retaining data in an anonymized form when it is no longer required for contact tracing. People who suspect data breaches by government agencies can complain by completing a form on the Smart Nation website.

The introduction of the TraceTogether tokens have reignited a privacy debate. Critics believe that it could be used as a surveillance tool.[32]

Proponents point out that the tokens cannot be used for surveillance of a person's movements because they don't log GPS location data or connect to mobile networks. Privacy expert Roland Turner observed that

> "(Using the token) you are able to make policy decisions which very carefully tie restraints or obligations only to high-risk activities. Otherwise you're left with much blunter tools... There is perhaps a paradoxical consequence that greater freedoms are possible."[33]

Another privacy issue that emerges during the pandemic is the public disclosure of the names of persons who have tested positive for COVID-19 infection.

In the Philippines, the heads of the Integrated Bar of the Philippines (national lawyers' group), the Philippine Medical Association (national physicians' group) and Philippine College of Surgeons called for the waiver of privacy rights of infected individuals in a public statement entitled *Public Health and Safety Prevails Over Confidentiality of Medical Data.*[34] Specifically, these associations called for the following: "1) That COVID19 patients or PUIs (Persons Under Investigation) **VOLUNTARILY WAIVE** the confidentiality of their medical condition and forthrightly inform those they have been in close contact with; and 2) That the government... **prudently uses and promptly shares medical information** to enable all concerned authorities, institutions and persons to effectively take precautionary and remedial measures (underscoring in the original)". The groups urged government to "promptly provide (**with adequate safeguards**) to all health institutions, concerned law enforcers, and responsible local authorities, the medical data of patients to avoid further infection, facilitate contact training, and promptly alert those affected (underscoring in the original).

The National Privacy Commission (NPC) – the Philippines' privacy regulator - rejected the call for suspending data privacy of COVID infected individuals. The NPC insisted that sharing

---

31 https://www.zdnet.com/article/singapore-looks-to-ease-privacy-fears-with-no-internet-wearable-device/

32 See for instance, https://www.onlinecitizenasia.com/2020/09/15/netizens-unhappy-at-the-idea-of-tracetogether-token-as-it-resembles-dog-tag/ and https://theindependent.sg/making-tracetogether-mandatory-seems-to-contradict-vivian-balakrishnans-pre-election-assurances/

33 Saira Asher "TraceTogether: Singapore turns to wearable contact-tracing COVID tech" BBC News, Singapore 4 July 2020 https://www.bbc.com/news/technology-53146360

34 https://www.philippinemedicalassociation.org/joint-statement-on-lifting-medical-data-confidentiality-for-public-health-and-safety/

personal data to the general public will "not be helpful as this will only induce fear among these individuals given the multiple reports now on physical assaults, harassments, and discrimination endured by patients, Persons Under Investigation (PUIs), Persons Under Monitoring (PUMs), and even health workers."[35]The NPC believes that: "These threats to their safety and security may discourage them to report their symptoms to public authorities, take confirmatory tests, and submit to treatments." The NPC stressed that even in times of calamity or a state of a public health emergency, privacy rights "remain in effect and upholding them equate to protecting lives." It argued that the Data Privacy Act of 2012's provisions are enough for contact tracing, treating patients, and addressing threats while guaranteeing the privacy of COVID-19 positive patients, persons under investigation (PUIs), and persons under monitoring (PUMs).[36]

Despite this, business groups also called for the suspension of the Data Privacy Act a few months later.[37]

The use of visitors logs in shops, cafes and restaurants for contact tracing purposes has also raised privacy concerns. Many countries use QR codes on smartphones to check-in to public places.[38]

In Malaysia, government mandated the use of the *MySejahtera* app in all business premises.[39] Thailand's *Thai Chana* online platform is used "to facilitate disease-control tracking of customers in shopping malls and retailers and help prevent a second wave of COVID-19".[40] Citizens of two countries have expressed concern over the privacy implications of the *MySejahtera* and the *Thai Chana* apps.[41]

The Philippines has no 'digital check-in' app and relies on a paper-based visitors logs. Joint Memorandum Circular No. 20-04-A Series of 2020 issued by the Department of Trade and Industry and Department of Labor and Employment, mandated the collection of personal data when entering public spaces through a health-declaration form or a visitor contact-tracing form. In a nod to privacy, the circular mandates that data gathered must be disposed of properly after 30 days from date of accomplishment. Furthermore, the NPC issued a warning against the repurposing of collected personal data for direct marketing, profiling, or any other use or

35 https://newsbytes.ph/2020/04/07/npc-rejects-call-for-patients-to-waive-privacy-rights-on-health-status/

36 Neil Arwin Mercado "Privacy commission: Agencies to collect only necessary data amid COVID-19 crisis" Philippine Daily Inquirer April 07, 2020 https://newsinfo.inquirer.net/1255108/privacy-commission-agencies-to-collect-only-necessary-data-amid-covid-19-crisis#ixzz6d4g7zS5S

37 Anna Leah E. Gonzales "'Suspend data privacy law, let jeeps run again'" *Manila Times* September 25, 2020 https://www.manilatimes.net/2020/09/25/business/business-top/suspend-data-privacy-law-let-jeeps-run-again/771795/

38 Josh Taylor "QR codes: how an old technology could help contact tracers keep the pandemic in check" *The Guardian* 30 Oct 2020 https://www.theguardian.com/world/2020/oct/31/qr-codes-how-an-old-technology-could-help-contact-tracers-keep-the-pandemic-in-check

39 "Use of MySejahtera app to be mandatory in all business premises, says Ismail Sabri" The Star 03 Aug 2020 https://www.thestar.com.my/news/nation/2020/08/03/use-of-mysejahtera-app-to-be-mandatory-in-all-premises-says-ismail-sabri

40 https://www.pacificprime.co.th/blog/new-anti-covid-19-online-platform/

41 "MySejahtera privacy, safety concerns remain unaddressed" *FocusM* June 18, 2020 https://focusmalaysia.my/mainstream/mysejahtera-privacy-safety-concerns-remain-unaddressed/ and UCA News reporter "Thai Covid-19 app raises privacy concernsBangkok" *UCA News* May 19, 2020 https://www.ucanews.com/news/thai-covid-19-app-raises-privacy-concerns/88069#

purpose beyond what is required for COVID-19 prevention and control.[42]

The concern of using the pandemic to expand surveillance is not unique to Asia.

A joint statement of 120 NGOs issued in April 2020 maintained that "Countries' efforts to contain the coronavirus pandemic must not be used as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance". The statement listed eight conditions that must be satisfied before digital surveillance tools are deployed. The eight conditions include:

> States must ensure that increased collection, retention, and aggregation of personal data, including health data, are only used for the purposes of responding to the COVID-19 pandemic. Data collected, retained, and aggregated to respond to the pandemic must be limited in scope, time-bound in relation to the pandemic and must not be used for commercial or any other purposes.[43]

This position is supported in an editorial published in the prestigious *Nature* magazine:

> With present-day technology for collecting and crunching data, there is great promise in using innovative, data-driven tools to fight the virus. But institutionalizing large-scale citizen data collection systems is a dangerous path that could lead to intrusive practices from which it will be difficult to retrace our steps.[44]

Privacy and Surveillance

Even without the pandemic, surveillance - "the systematic investigation or monitoring of the actions or communications of one or more persons" - has become the norm[45]. Governments and giant corporations have become data miners, collecting information about every aspect of individuals' activities, behavior and lifestyle like never before.

The mid-1980s saw the rise of a new form of surveillance – "dataveillance". This new form of monitoring of the actions of individuals or groups relies less on "(expensive) physical and electronic surveillance of individuals" but on "(cheap) surveillance of people's behavior through the increasingly intensive data trails that their behaviour was generating".[46]

Surveillance used to be the domain of government. It has now become vital to private corporations. Tracking individual behavior is at the core of the business models of companies. Worse still, the collection and processing of personal data are done without the full knowledge of the data subjects.

---

42 https://www.privacy.gov.ph/2020/10/privacy-commission-issues-advisory-cautioning-establishments-against-repurposing-of-collected-data/

43 *States' use of digital surveillance technologies to fight pandemic must respect human rights* https://freedomhouse.org/article/states-use-digital-surveillance-technologies-fight-pandemic-must-respect-human-rights

44 Pandemic data challenges. *Nat Mach Intell* 2, 193 (2020) https://www.nature.com/articles/s42256-020-0172-7

45 Roger Clarke What 'Überveillance' Is, and What To Do About It Version of 30 September 2007 http://www.rogerclarke.com/DV/RNSA07.html#Surv

46 Roger Clarke's Dataveillance and Information Privacy Home-Page http://www.rogerclarke.com/DV/#SurvD

Take the case of smart phones. An August 2018 study revealed that unknown to smartphone owners, Google is tracking Android device location even when the phone is stationary. In a 24-hour period, an Android device sends about 4.4MB of data to Google. iPhone users are better off. The same study showed that "iPhones send data 10 times less frequently to Apple's servers than the Android device to Google's servers".[47]

The difference between iPhone and Android extend to data protection. Christopher Soghoian argues for the rise of "digital security divide" - "increasingly a gap between the privacy and security of the rich, who can afford devices (iPhones) that secure their data by default, and of the poor, whose devices (Android) do very little to protect them by default".[48] iPhones encrypt calls, text messages, all the data on the device, while Android leaves users completely vulnerable to surveillance.

Social media companies collect and analyze users' online behavior to produce profiles that can be further used for commercial purposes. Facebook tracks what we like, love, laugh at, surprised with, sad and angry about to develop profiles that they sell to advertisers. The profiles that are developed by social media companies are highly specific. A University of North Carolina study showed that

> using only 'Facebook Likes'… researchers were able to fairly reliably 'model' (computationally and statistically guess to a high degree of accuracy) 'latent' traits of 58,000 volunteers. The traits modeled-often with eighty to ninety percent accuracy-included "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender" among others.[49]

Social media companies do not even need to analyze data that individual users provide to create profiles. The posts of one's friends are sufficient. An analysis of Twitter accounts (profiles and interactions) of a subscriber's friends can generate reliable profiles about the subscriber. According to a study, the tweets of eight to nine friends of a subscriber could lead to "startlingly accurate profiles" (with up to 95 percent accuracy) of the subscriber.[50]

Social media companies are not the only ones profiting from collecting, processing, and selling personal data. There are third-party data brokers - companies that "create consumer profiles based on information compiled from a variety of sources, including surveys and questionnaires, public records like government lists and voter documentation, and enterprise insights from loyalty programs, credit reports and more."[51] The profiles that data brokers create "come not

---

47 Liam Tung, "Want Google to track you less? Get an iPhone, ditch the Android", ZDNet, 23 August 2018. Available at https://www.zdnet.com/article/want-google-to-track-you-less-get-an-iphone-ditch-the-android/.

48 Christopher Soghoian "Your smartphone is a civil rights" TEDSummit issuehttps://www.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue/transcript?utm_source=newsletter_weekly_2016-11-05&utm_campaign=newsletter_weekly&utm_medium=email&utm_content=talk_of_the_week_button&fbclid=IwAR06hBAmnKlaIAAARruuwQ-JGam0Lz-z4MeWEYmMcoI3iQwbxXKtcY_8das

49 Zeynep Tufecki Algorithmic Harms Beyond Facebook And Google: Emergent Challenges Of Computational Agency https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf p. 210

50 Nicole Lindsey "New Research Study Shows That Social Media Privacy Might Not Be Possible" CPO Magazine Feb 3, 2019 https://www.cpomagazine.com/data-privacy/new-research-study-shows-that-social-media-privacy-might-not-be-possible/

51 Gigya Uncovering the Hidden Costs of Third-Party Data

just from data you've shared, but from data shared by others, and from data that's been inferred".[52]

The increasing importance of collecting and processing data in business has given rise to the concept of "Surveillance capitalism" - "a new economic order that claims human experience as free raw material for hidden commercial of extraction, prediction and sales."[53]

Surveillance Capitalism describes a market driven process where the commodity for sale is users' personal data captured on mass surveillance of the Internet. This activity is often carried out by companies that provide users with 'free' online services, such as search engines (Google) and social media platforms (Facebook)

The biggest tech companies like Google, Amazon, Facebook and Apple collect and control massive quantities of data about our behaviors and turn these into products and services.[54] For instance, Google processes an average of 40,000 searches per second, 3.5 billion per day and 1.2 trillion per year. Its parent company, Alphabet, was recently valued at USD 822 billion.

David Lyon argues that "Surveillance should now be thought of, not only relating to economic, technological, social or political realities, but as a highly significant cultural formation in the making."[55] It is a cultural formation in the making because our daily lives are increasingly mediated by digital tools that are also efficient data collecting mechanisms.

Surveillance enabled by everyday devices that we use has become so pervasive that many consider it a normal part of life in the Information Age. But what makes surveillance culture unprecedented is that people actively participate in an attempt to regulate their own surveillance and the surveillance of others.[56] We surveille each other when we follow social media posts, we allow others to surveil us when we tweet, post memes and share pictures. We attempt to regulate surveillance of others by adjusting our FB privacy settings.

To be clear, "surveillance culture does not for a moment signify any unified or all-embracing situation. It is merely an umbrella term for many different kinds of phenomena that point to the reality of a 'whole way of life' that relates, positively and negatively, to surveillance."[57]

But the emergence of surveillance culture is worrying because "we cannot opt out of it, any

---

https://www.356.ibm.com/partnerworld/gsd/showimage.do?id=40879

52 Sacha Molitorisz "It's time for third-party data brokers to emerge from the shadows" The Conversation April 4, 2018 https://theconversation.com/its-time-for-third-party-data-brokers-to-emerge-from-the-shadows-94298

53 "The Definition" in Shoshana Zuboff *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019)

54 Explainer: what is surveillance capitalism and how does it shape our economy? http://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158#:~:targetText=Surveillance%20capitalism%20describes%20a%20market,mass%20surveillance%20of%20the%20internet.

55 David Lyon The Culture of Surveillance: Watching as a Way of Life (Cambridge: Polity, 2018) p. 50

56 Ibid, p. 6

57 David Lyon "Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity" *International Journal of Communication* 11 (2017) p. 830 https://ijoc.org/index.php/ijoc/article/download/5527/1933#:~:text=Surveillance%20culture%20is%20a%20product,%2C%20simply%2C%20of%20digital%20modernity.&text=We%20collude%20as%20never%20before,in%20the%20online%20public%20domain.

more than we might opt out of automobile culture by refusing to drive".[58]

Towards an Ethical Framework

The European Data Protection Supervisor (EDPS) believes that an ethical framework that better respects and safeguards human dignity "could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual".[59]

For the EDPS in the current environment where the use of digital technology is pervasive "adherence to the law is not enough" and the privacy stakeholders need "to consider the ethical dimension of data processing".[60] The EDPS sets out the relationship between ethics and law:

> Ethical thinking and deliberation come before, during, and after the law. Ethics are the foundations of our legal systems and ensure that they are updated when necessary. Debating ethics and discussing what is right and wrong is the process of societal self-reflection and self-evaluation on which we, as members of society, establish values and norms and enact binding, enforceable rules.[61]

This view finds favor in some Asian jurisdictions.

In 2018, the Office of Privacy Commissioner for Personal Data in Hong Kong, China marked "the beginning of... strengthened initiative for a cultural change in data privacy protection" by publishing a commissioned study entitled *Ethical Accountability Framework for Hong Kong, China*.[62] The privacy commissioner expressed the "hope that in the not-too-distant future, ethical data stewardship will become a well-received norm among organizations in Hong Kong".

In the Philippines, ethics is incorporated in NPC's training program called the DPO Accountability, Compliance, and Ethics (ACE) Program which is "aimed at establishing a skills benchmark for local privacy professionals".[63] Privacy Commissioner Raymund Liboro believes "that one important component of successful digital governance is making sure that legitimate business interests thrive with accountability, compliance and ethics".[64]

---

58 Kenan Malik "As surveillance culture grows, can we even hope to escape its reach?"https://www.google.com/amp/s/amp.theguardian.com/commentisfree/2019/may/19/as-surveillance-culture-grows-can-we-even-hope-to-escape-its-reach

59 European Data Privacy Supervisor, "Towards a new digital ethics: Data, dignity and technology", Opinion 4, 2015, p. 12 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf

60 Ibid, p. 4.

61 Expert Q&A: European Data Protection Supervisor on Digital Ethic, p. 3 https://edps.europa.eu/sites/edp/files/publication/19-03-25_reuters_interview_en.pdf

62 "Ethical Accountability Framework for Hong Kong, China: A Report prepared for the Office of the Privacy Commissioner for Personal Data", n.d. https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf

63 National Privacy Commission, Philippines, "NPC launches DPO ACE Program, sets benchmark for data privacy training in PH", 12 December 2018. https://www.privacy.gov.ph/2018/12/npc-launches-dpo-ace-program-sets-benchmark-for-data-privacy-training-in-ph/

64 https://www.privacy.gov.ph/2019/09/press-statement-of-privacy-commissioner-raymund-enriquez-liboro-on-the-industry-wide-code-of-ethics-and-code-of-conduct-by-fintech-alliance/

II. COMPARING REGIONAL PRIVACY FRAMEWORKS: OECD, APEC, ASEAN & GDPR

In this section, the following regional privacy frameworks will be compared:

- OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980, 2013);
- APEC Privacy Framework (2015),
- ASEAN Framework on Personal Data Protection (2016); and the
- EU General Data Protection Regulation (2018).

OVERVIEW[65]

The four regional frameworks will be compared using the following metrics: 1) Objective; 2) Application by jurisdiction; 3) Application scope by entity – data controllers vs processors; 4) Accountability provisions; 5) Consent requirements; and, 6) Default position on data flow – serves to promote vs restrict.

	OECD	APEC	ASEAN	GDPR
Objective	Economic	Economic	Economic	Fundamental Rights
Application by jurisdiction	Territorial subject to national law	Territorial subject to national law	Territorial subject to national law	Extra-territorial – not subject to national law
Application scope by entity	Data controllers	Data controllers + processors (voluntary)	Data controllers	Data controllers + processors (mandatory)
Accountability provisions	Principle	Principle + Voluntary mechanism	Principle	Principle + voluntary mechanisms + legal requirements
Consent requirements	Consent, where applicable	Consent, where applicable	Consent, where applicable	Consent (freely given, specific, informed and unambiguous, and in some

65 Based on *GSMA and Access Partnership Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation* September 2018 https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

				cases, explicit consent)
Default position on data flow	Promotes data flow	Promotes data flow	Promotes data flow	Restrictive (outside the group); promotes data flow (within the group)

PRINCIPLES[66]

Matrix below compares the principles in the four regional frameworks.

OECD	APEC	ASEAN	GDPR
I. Collection Limitation There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	III. Collection Limitation The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.		II. Purpose Limitation 1 b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');
II. Data Quality Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be	VI. Integrity of Personal Information Personal information should be accurate, complete and kept up to date to the extent necessary for the purposes of use.	II. Accuracy of Personal Data The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal	

66 Compiled by Emmanuel Lallana, PhD

accurate, complete and kept up to date.		data is to be used or disclosed.	
III. Purpose Specification The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	IV. Uses of Personal Information. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.		III. DATA MINIMIZATION 1 c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
IV Use Limitation Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.		I. Consent, Notification and Purpose An organization should not collect, use or disclose personal data about an individual unless: (i) the individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data; or (ii) the collection, use or disclosure without notification or consent is authorized or required under	

		domestic laws and regulations. An organization may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.	
V. Security Safeguards Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	VII. Security Safeguards Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held and should be subject to periodic review and reassessment.	III. Security Safeguards The personal data should be appropriately protected against loss and unauthorized access, collection, use, disclosure, copying, modification, destruction or similar risks.	VI. Integrity and Confidentiality 1 f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).
VI. Openness	V. Choice		

Principle There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.		
VII. Individual Participation An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and	VIII. Access and Correction Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time;ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the	IV. Access and Correction Upon request by an individual, an organization should: (i) provide the individual access to his/her personal data which is in the possession or under the control of the organization within a reasonable period of time; and, (ii) correct an error or omission in his personal data, unless domestic laws and regulations require or authorize the organization not to provide access or correct the personal data in the particular circumstances.	

to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	accuracy of personal information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.		
VIII. Accountability A data controller should be accountable for complying with measures which give effect to the principles stated above.	IX. Accountability A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.	VII. Accountability An organization should be accountable for complying with measures which give effect to the Principles. (i) An organization should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organization should also make available information on how to contact the organization about its data protection policies and practices.	Accountability 2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).
	I. Preventing Harm personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may		

	result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.		
	II. Notice Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for		

	limiting the use and disclosure of, and for accessing and correcting, their personal information.		
		V. Transfers to Another Country or Territory (f) Before transferring personal data to another country or territory, the organization should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organization will protect the personal data consistently with these Principles.	
		VI. Retention An organization should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.	V. Storage Limitation 1 e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of

			the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘’);
			I. Lawful, Fair and Transparent 1 a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

III. DATA PRIVACY LAWS in SELECT ASIA – PACIFIC ECONOMIES[67]

An overview of the privacy laws and regulatory regimes in Australia, Hong Kong, China, Japan, New Zealand and the Republic of Korea are compared in terms of Definition of Personal Information; Use And Disclosure; Individual Rights; Cross-Border Transfers; Security; Data Protection Officers; Data Breach Notification; and, Regulatory Body.

PRIMARY LEGISLATION

Australia	*Australian Privacy Act of 1988* *Privacy Amendment (Notifiable Data Breaches) Act, 2018*
Hong Kong, China	*Personal Data (Privacy) Ordinance (PDPO)*
Japan	*Act on the Protection of Personal Information* ("APPI"), 2003. Amended in 2017
New Zealand	*Privacy Act 1993* Amended in 2020
Republic of Korea	*Personal Information Protection Act* ('PIPA'); *Act on the Promotion of Information and Communications Network Utilization and Information Protection* ('Network Act'); and, *Act on the Use and Protection of Credit Information* ('Credit Information Act'). Amended PIPA and CIPA in 2020

67 Complied by Emmanuel Lallana from information from Deloitte *Unity in Diversity: The Asia Pacific Privacy Guide* July 2019 https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-unity-diversity-privacy-guide.pdf

DEFINITION OF PERSONAL INFORMATION

Australia	As information about an identified individual, or an individual who is reasonably identifiable whether the information is true or not; and is recorded in a material form or not. Sensitive information is a specific type of personal information, which includes information about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, health information and tax file number information.
Hong Kong, China	Personal data is defined as information that: 1) relates to a living person (known as a data subject); 2) can be used to, directly or indirectly, identify them; and, 3) is in a form in which accessing or processing the data is practicable. In Hong Kong, China, the law does not define 'sensitive' data. However, there are codes of practice issued to regulate data such as Identification Card numbers and unique identifiers, including passport numbers and patient numbers. The regulator has issued specific guidance on biometric data, stating that data can only be collected when necessary, and with free and informed consent to collect it from the data subject.
Japan	Personal information is defined as information, which relates to a living individual, and can fall within any of the following: 1) containing a name, date of birth or other description, in vocal or written format, through drawing or electromagnetic record, to include scenarios where the information can be collated with other information to identify a specific individual; and 2) containing an individual identification code. Personal data includes biometric data. Special care required personal information ('sensitive information') includes personal information comprising of an individual's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions.
New Zealand	Personal information includes any information about an identifiable individual, such as a name, date of birth, address, biometric information and/or gender etc. If there is a reasonable chance someone could be identified from the information, it is personal information. This also applies to individuals whose death is maintained pursuant to the Birth, Deaths, Marriages, and Relationships Registration Act 1995,

	or any former Act.
Republic of Korea	Personal information relates to a living person and can be used to identify an individual. Examples include a person's name, image or resident registration number. Information is also personal if it can be combined with other information to identify a specific individual. Sensitive data includes information such as, and related to, an ideology, belief, membership of a trade union or political party, political mindset, health and sexual life. Sensitive data also includes any other personal information which is likely to cause harm to the privacy of a data subject.

USE AND DISCLOSURE

Australia	Personal information can only be used for the original purpose it was collected for, unless certain conditions are met – for example, if an individual consents to a secondary use of their personal information or if further use is required by law. If the organization uses or discloses personal information for a secondary purpose, the individual should be provided with a written notice of use or disclosure.
Hong Kong, China	Personal data can only be used for the original or a directly related purpose, unless voluntary and explicit consent is provided by the data subject for the new purpose. If personal data is used or disclosed for a new purpose (i.e. a purpose other than the purpose for which the data was to be used at the time of the collection or a directly related purpose), prescribed consent must be obtained from the data subject. Prescribed consent means express consent given voluntarily which has not been withdrawn in writing.
Japan	Personal information must be used for a specific purpose stipulated at the time of collection. However, personal information can be used for a new purpose if consent is obtained from the principal or where any of the above exceptions (provided in collection and notice) apply.
New Zealand	An agency must not use or disclose personal information without taking reasonable steps to validate that it is accurate, complete relevant, up to date, and not misleading. The agency must not use the

	information for a purpose other than the one it was collected for. Personal information must not be disclosed unless: 1) Associated with, or directly related to the original purpose of collection; 2) Information was obtained from a publicly available publication; 3) It is directed to and approved by the individual concerned; and, 4) Approved by the Privacy Commissioner.
Republic of Korea	Processors must process personal information: 1) in a lawful and fair manner; 2) in accordance with the specified and intended purpose. Provided the information is unidentifiable and consent was provided for an intended purpose, exceptions apply where: 1) purpose is likely to infringe upon the data subject's interest; is required for legal proceedings or used as part of statistics and/or academic research. Provided the information is unidentifiable and consent was provided for that purpose. Sensitive data cannot be processed unless: explicitly required or permitted by laws and regulations; or, consent has been obtained.

INDIVIDUAL RIGHTS

Australia	Individuals have the right to: • Be informed of their rights prior to collection and use of their personal information through notification. • Access and correct their personal information, and organizations must respond within 30 days or inform individuals that they are unable to do so within the timeframe.
Hong Kong, China	Data subjects have the right to: • Be informed of their rights at, or prior to, collection and use of their data, the retention period, the security measures in protecting their data and how they can raise an access and correction request. • Access and correct personal data: organizations must respond to requests within 40 days or inform the individuals that they are unable to do so within the timeframe.

Japan	Individuals have the right to: • Be informed of their rights prior to collection and use of their personal information. • Request correction, rectification and/or deletion of their personal information. • Object to processing by lodging a utilization cease request, based on reasonable grounds. • Lodge complaints to the PPC or any other authorized entity about the handling of their personal information.
New Zealand	Individuals have the right to: • Be informed of their rights prior to collection and the intended use of their personal information. • Access and correct personal information held about them.
Republic of Korea	Data subjects have the right to: • Be informed of their rights and how the information will be used. • Request access, correction and erasure to their personal information.

CROSS BORDER TRANSFER

Australia	Personal information can only be transferred to another organization outside of Australia where reasonable steps have been taken by the transferring organization to ensure the overseas recipient does not breach the Privacy Act.
Hong Kong, China	Organizations can only transfer personal data if data subjects are informed when personal data is collected that: • Their personal data may be transferred and; • The classes of people to whom it may be transferred to. The regulator prohibits cross border transfer of data except in specified circumstances. However, that provision has not yet been enacted. The regulator currently provides a 'Guidance on Personal Data Protection in Cross-border Data Transfer' 8 to outline best practices for the cross-border transfer of data. For example, the PCPD recommends organizations review data transfer agreements and to keep an inventory of personal data.
Japan	Personal information must not be transferred to a third party unless consent has been obtained from the principal or any one of the above exceptions apply, as provided within 'Collection and notice'.

	Personal information may be transferred outside of Japan where: • Consent is obtained from the principal. • The foreign state has privacy laws which are considered equivalent to Japan. • The foreign party maintains an internal personal information protection system consistent with standards set by the PPC.
New Zealand	Once transferred, personal information should not be held, used or disclosed unless it falls within or is directly related to the scope of the original purpose for collection. Security controls must be in place to ensure personal information is safeguarded from misuse or disclosure to another party. The regulator has the power in exceptional cases to restrict cross-border transfer of personal information from New Zealand by issuing a transfer prohibition notice if: • It believes the receiving party does not provide protections contained within or comparable to the Privacy Act • The transfer would likely contravene the basic principles set out by the OECD with regard to using and security personal information
Republic of Korea	Personal information can only be shared with third parties where any one of the following conditions has been satisfied: • Where consent has been provided by a data subject. • Where required by law. • Where required for the processor to carry out work under laws and regulations. • Where necessary to execute and perform a contract with the data subject. • Where necessary for the protection of the data subject or a third party, such as a legal representative, from danger to life,body or economic profits. When transferring personal information to third parties, processors must inform the data subject of the recipient, purpose for sharing, type of personal information shared, period of use and retention, and individual rights. For the purposes of transferring personal information across borders, processors must obtain explicit consent from the data subject and must not enter into contractscontrary to the PIPA.

SECURITY

Australia	Organisations must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. The Privacy Commissioner provides guidance on what is considered reasonable in the context of securing personal information.
Hong Kong, China	Organisations must take practicable steps to protect personal data from unauthorised or accidental access, processing, erasure, loss or use. The following factors should be considered: • Kind of data and the harm when data is inadequately protected • Security measures incorporated into data storage equipment • Secure transmission of data • Physical location of the data storage • Measures for assurance of integrity, prudence and competence of people who could access data
Japan	Organizations must take necessary and appropriate actions to protect personal information from leakage, loss or damage. For example, they must exercise necessary and appropriate supervision over employees who handle personal information, to prevent unauthorised access or misuse.
New Zealand	An agency is required to ensure personal information is protected against loss, misuse, disclosure, unauthorised use or unauthorised disclosure through reasonable security safeguards while considering physical, electronic, operational, transmission and destruction-related security.
Republic of Korea	Processors must prevent personal information from loss, theft, forgery, disclosure, alteration, damage and destruction by implementing technical, managerial and physical measures, such as: • Controlling access and restricting authority to access • Adopting encryption technology • Installing, maintaining and upgrading security programs, storage and locks • Developing an internal management plan • Preserving log-on records

DATA PROTECTION OFFICER

Australia	Organizations are not required to appoint a data protection officer (DPO). However, the regulator has recommended that organizations appoint a DPO as good practice.

Hong Kong, China	There is no mandatory requirement to appoint a data protection officer. However, the regulator advocates for companies to be accountable for the protection of personal data to build trust with clients, enhance reputation and increase competitiveness.
Japan	The APPI does not specifically require the appointment of data protection officers. However, the guidelines on the APPI (the "APPI Guidelines") state that the appointment of a person responsible for dealing with personal data is one example of the security measures that information handlers must take under the APPI.
New Zealand	Agencies are required to appoint a privacy officer. The privacy officer is responsible for: • Encouraging compliance with the Privacy Act; • Dealing with requests made to the agency, such as access and correction; and • Working with the Commissioner in relation to investigations.
Republic of Korea	Designation of a privacy officer, who is responsible for: • Protecting, controlling and managing personal information; • Establishing and implementing personal information protection plans; • Surveying processing practices and improve shortcomings regularly; • Managing complaints; • Building internal controls systems; • Preparing and implementing education programmes; and Taking and reporting immediate corrective measures, if necessary.

DATA BREACH NOTIFICATION

Australia	A mandatory data breach notification regime commenced in Australia in 2018. The regulator and data subjects must be notified for breaches concerning personal information, credit reporting information, credit eligibility information and tax file numbers.
Hong Kong, China	There is no requirement to notify data subjects or the regulator of a data breach. However, the regulator could conduct an investigation relating to a breach and issue an enforcement notice if appropriate. The Commissioner has recommended voluntary notification in the event of a data breach.

Japan	While there is no mandatory breach reporting scheme, the regulator provides voluntary guidance (Guidelines for the Act on Protection of Personal Information) for organizations to undertake assessment, remediation and reporting of breaches as best practice.
New Zealand	Data breach notification is not mandatory. However, the regulator provides guidance about responding to a data breach as best practice.
Republic of Korea	Data breach notification is a requirement which processors must adhere to the PIPA.

REGULATORY BODY

Australia	Office of the Australian Information Commissioner (OAIC) The Commissioner's roles and responsibilities involve: • Conducting investigations into acts, which may breach the Privacy Act; • Managing complaints about the handling of personal information;and • Providing privacy advice to the public, government agencies and businesses.
Hong Kong, China	Office of the Privacy Commissioner for Personal Data (PCPD) The PCPD's roles and responsibilities include: • Enforcement; • Monitoring and supervising compliance; • Promotion of education, training and best practice; • Corporate governance; and • Meeting changing needs relating to technological developments, trends and expectations.
Japan	Personal Information Protection Commission (PPC). The Commissioner's roles and responsibilities include:

	• Formulating and promoting policy; • Supervising; • Mediating complaints; • International cooperation; • Public relations; • Conducting personal information protection assessments • Issuing accreditations to organizations; and • Reporting.
New Zealand	The PCO is the New Zealand regulator of privacy led by the Privacy Commissioner. The Commissioner's roles and responsibilities include: • Making public statements on privacy matters; • Inquiring and investigating matters, such as complaints, which may affect individual privacy; • Endorsing and promoting privacy understanding; • Monitoring privacy impacts of new technologies and new legislation; • Developing codes of practice within specific industries and sectors; and • Monitoring and assessing government data matching programmes.
Republic of Korea	Personal Information Protection Commission (PIPC) The PIPC is responsible for: • Protecting personal information; • Ensuring personal information is fairly collected and legitimately processed; • Monitoring data protection violations; • Mediating to redress damage caused by violations; and • Ensuring data protection laws are properly interpreted and applied.

IV. DATA PRIVACY LAWS of ASEAN MEMBER STATES[68]

This section compares the four data privacy laws of ASEAN Member States (AMS) in terms of Scope, Principles, Data Subject Rights, Cross Border Transfer, Regulatory Agencies and Penalties.

The four laws are:

- Malaysia's Personal Data Protection Act of 2010[69]
- Singapore's Personal Data Protection Act of 2012[70]
- Philippines' Data Privacy Act of 2012[71]
- Thailand's Personal Data Protection Act (2019)[72]

Scope

Malaysia's data privacy laws regulate commercial transactions only. The Philippine law applies to the government (but with exemptions). It also protects journalists and their information sources. Thailand's law exempts the legislature and the courts.

Malaysia	Singapore	Philippines	Thailand
PART I. PRELIMINARY Application 2. (1) This Act applies to— (a) any person who processes; and (b) any person who has control over or authorizes the processing of, any	Purpose 3. is to govern the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of	SEC. 4. Scope This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal	SEC 5 applies to the collection, use, or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand regardless of whether such collection, use, or disclosure takes place in the

68 Compiled by Emmanuel C. Lallana, PhD
69 http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf
70 https://sso.agc.gov.sg/Act/PDPA2012
71 https://www.privacy.gov.ph/data-privacy-act/#:~:text=%E2%80%93%20This%20Act%20shall%20be%20known,SEC.&text=%E2%80%93%20It%20is%20the%20policy%20of,to%20promote%20innovation%20and%20growth
72 https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf

personal data in respect of commercial transactions. (2) Subject to subsection 1, this Act applies to a person in respect of personal data if— (a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b) the person is not established in Malaysia but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.	organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. Application of Act 4.—(1) Parts III to VI shall not impose any obligation on — (a) any individual acting in a personal or domestic capacity; (b) any employee acting in the course of his employment with an organization; (c) any public agency or an organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data; or (d) any other organizations or personal data, or classes of organizations or personal data, prescribed for the purposes of this provision.	information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph : Provided, That the requirements of Section 5 are complied with.	Kingdom of Thailand or not.
Non-application 3. (1) This Act shall not apply to the Federal Government and State Governments. (2) This Act shall not apply to	(4) This Act shall not apply in respect of (a)personal data about an individual that is contained in a record that has been in existence for at least 100 years; or	This Act does not apply to the following: (a) Information about any individual who is or was an officer or employee of a	Sec 4 This Act shall not apply to: (1) the collection, use, or disclosure of Personal Data by a Person who collects such Personal Data for personal benefit or household activity of

any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.	(b) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) shall apply in respect of personal data about an individual who has been dead for 10 years or fewer. (5) Except where business contact information is expressly referred to, Parts III to VI shall not apply to business contact information. (6) Unless otherwise expressly provided in this Act — (a) nothing in Parts III to VI shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act; and (b) the provisions of other written law shall prevail to the extent that	government institution that relates to the position or functions of the individual, including (1) The fact that the individual is or was an officer or employee of the government institution;(2) The title, business address and office telephone number of the individual; (3) The classification, salary range and responsibilities of the position held by the individual; and (4) The name of the individual on a document prepared by the individual in the course of employment with the government; (b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services; (c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or	such Person only; (2) operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity; (3) a Person or a juristic person who uses or discloses Personal Data that is collected only for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest; (4) The House of Representatives, the Senate, and the Parliament, including the committee appointed by the House of Representatives, the Senate, or the Parliament, which collect, use or disclose Personal Data in their consideration under the duties and power of the House of Representatives, the Senate, the Parliament or their committee, as the case may be; (5) trial and adjudication of courts

	any provision of Parts III to VI is inconsistent with the provisions of that other written law.	permit given by the government to an individual, including the name of the individual and the exact nature of the benefit; (d) Personal information processed for journalistic, artistic, literary or research purposes; (e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed existing laws; (f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with existing laws; and (g) Personal information	and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure; (6) operations of data undertaken by a credit bureau company and its members, according to the law governing the operations of a credit bureau business.

		originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. SEC. 5. Protection Afforded to Journalists and Their Sources. – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter. SEC. 6. Extraterritorial Application. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:	

		(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident; (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: (1) A contract is entered in the Philippines; (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and (c) The entity has other links in the Philippines such as, but not limited to: (1) The entity carries on business in the Philippines; and (2) The personal information was collected or held by an entity in the Philippines.	

Principles

All laws define the purpose and limitations of collection, usage, retention or disposal of data collected.

Malaysia	Singapore	Philippines	Thailand
PART II PERSONAL DATA PROTECTION Division 1 Personal Data Protection Principles 5. (1) The processing of personal data by a data user shall be in compliance with the following Personal Data Protection Principles, namely— (a) the General Principle; (b) the Notice and Choice Principle; (c) the Disclosure Principle; (d) the Security Principle; (e) the Retention Principle; (f) the Data Integrity Principle; and (g) the Access Principle, as set out in sections 6, 7, 8, 9, 10, 11 and 12 6. General Principle	Division 2 — Purpose Limitation of purpose and extent 18. An organization may collect, use or disclose personal data about an individual only for purposes (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable. Personal data collected before appointed day 19. Notwithstanding the other provisions in this Part, an organization may use personal data about an individual collected before the appointed day for the purposes for which the personal data was collected unless (a) consent for such use is withdrawn in accordance with section 16;	CHAPTER III PROCESSING OF PERSONAL INFORMATION SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. SEC. 12. Criteria for Lawful Processing of Personal Information. SEC. 13. Sensitive Personal Information and Privileged Information. SEC. 14. Subcontract of Personal Information. SEC. 15. Extension of	Chapter II Personal Data Protection Part 1 General Provisions Section 19 The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do Section 22. The collection of Personal Data shall be limited to the extent necessary in relation to the lawful purpose of the Data Controller. Section 23 In collecting the Personal Data, the Data Controller shall inform the data subject, prior to or at the time of such collection, of the following details, except the case where the data subject already knows of such details Section 24

- lawful purpose directly related to an activity of the data user - necessary for or directly related to that purpose; and - adequate but not excessive in relation to that purpose 7. Notice & Choice Principle 8. Disclosure Principle 9, Security Principle 10. Retention Principle 11. Data Integrity Principle 12. Access Principle	(b) the individual, whether before, on or after the appointed day, has otherwise indicated to the organization that he does not consent to the use of the personal data. 20. Notification of purpose	Privileged Communication.	The Data Controller shall not collect Personal Data from any other source, apart from the data subject directly

Rights of Data Subjects

Data subjects in the four AMS enjoy the same sets of rights.

Malaysia	Singapore	Philippines	Thailand
Division 4 Rights of data subject 30. Right of access to personal data	PART V ACCESS TO AND CORRECTION OF PERSONAL DATA 21. Access to personal data	CHAPTER IV RIGHTS OF THE DATA SUBJECT SEC. 16. Rights of the Data Subject - The data subject is	Chapter III Rights of the data subject Section 30 . The data subject is entitled to request access to and obtain a copy of the Personal

31. Compliance with data access request 32. Circumstances where data user may refuse to comply with data access request 33. Notification of refusal to comply with data access request 34. Right to correct personal data 35. Compliance with data correction request 36. Circumstances where data user may refuse to comply with data correction request 37. Notification of refusal to comply with data correction request	22. Correction of personal data Part VI: Care of Personal Data 23. Accuracy of personal data 24. Protection of personal data 25. Retention of personal data 26. Transfer of personal data outside Singapore	entitled to: (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed; (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity...: SEC. 17. Transmissibility of Rights of the Data Subject. SEC. 18. Right to Data Portability. SEC. 19. Non-Applicability.	Data related to him or her Sec 31. The data subject shall have the right to receive the Personal Data concerning him or her from the Data Controller Sec 32. The data subject has the right to object the collection, use, or disclosure of the Personal Data concerning him or her at any time... Sec 33. The data subject shall have the right to request the Data Controller to erase or destroy the Personal Data, or anonymize the Personal Data to become the anonymous data which cannot identify the data subject Sec 34. The data subject shall have the right to request the Data Controller to restrict the use of the Personal Data Sec 35 The Data Controller shall ensure that the Personal Data remains accurate, up-to-date, complete, and not misleading. Sec 36. In the case where the data subject requests the Data Controller to act in compliance with section 35, if the Data Controller does not take action

			regarding the request of the data subject, the Data Controller shall record such request of the data subject together with reasons

Cross Border Transfer

All laws have provisions on cross-border data transfer.

Malaysia	Singapore	Philippines	Thailand
129. (1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette. (2) For the purposes of subsection (1), the Minister may specifyany place outside Malaysia if— (a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or (b) that place ensures an adequate level of protection in(3) Notwithstanding	26.—(1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act. (2) The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.	SEC. 6. Extraterritorial Application. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if: (a) The act, practice or processing relates to personal information about a Philippine citizen or a resident; (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: (1) A contract is entered in the Philippines; (2) A juridical entity unincorporated in the	Section 28 In the event that the Data Controller sends or transfers the Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have adequate data protection standard, and shall be carried out in accordance with the rules for the protection of Personal Data as prescribed by the Committee in section 16(5), except in the following circumstances: (1) where it is for compliance with the law; (2) where the consent of the data subject has been obtained, provided that the data subject has been informed of the inadequate Personal Data protection standards of the

subsection (1), a data user may transfer any personal data to a place outside Malaysia if— (a) the data subject has given his consent to the transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which— (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (e) the data user has reasonable grounds for believing that in all circumstances of the case— (i) the transfer is for the avoidance or mitigation of adverse action against the	(3) An exemption under subsection (2) — (a) may be granted subject to such conditions as the Commission may specify in writing; and (b) need not be published in the Gazette and may be revoked at any time by the Commission. (4) The Commission may at any time add to, vary or revoke any condition imposed under this section	Philippines but has central management and control in the country; and (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and (c) The entity has other links in the Philippines such as, but not limited to: (1) The entity carries on business in the Philippines; and (2) The personal information was collected or held by an entity in the Philippines.	destination country or international organization; (3) where it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract; (4) where it is for compliance with a contract between the Data Controller, and other Persons or juristic persons for the interests of the data subject; (5) where it is to prevent or suppress a danger to the life, body, or health of the data subject or other Persons, when the data subject is incapable of giving the consent at such time; (6) where it is necessary for carrying out the activities in relation to substantial public interest. In the event that there is a problem with regard to the adequacy of Personal Data protection standards of the destination country or international organization, such problem shall be submitted to the Committee to decide. The decision made by the Committee may be reviewed when there is a new evidence convincing that the destination country or international organization

data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act; relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act. (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.			that receives such Personal Data has developed adequate Personal Data protection standards. Section 29 In the event that the Data Controller or the Data Processor whis in the Kingdom of Thailand has put in place a Personal Data protection policy regarding the sending or transferring of Personal Data to another Data Controller or Data Processor who is in a foreign country, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings. If such Personal Data protection policy has been reviewed and certified by the Office, the sending or transferring of Personal Data to a foreign country, which is in accordance with such reviewed and certified Personal Data protection policy, can be carried out and shall be exempt from compliance with section 28. The Personal Data protection policy, the nature of the same affiliate undertaking or affiliated business in order to jointly operate the undertaking or business, and the rules and

			methods for the review and certification in paragraph one shall be as prescribed and announced by the Committee. In the absent of a decision by the Committee in accordance with section 28, or the Personal Data protection policy referred in paragraph one, the Data Controller or the Data Processor may send or transfer the Personal Data to a foreign country in exemption to compliance with section 28, if the Data Controller or the Data Processor provides suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods as prescribed and announced by the Committee.

Regulatory Body

The Philippines and Thailand have "independent" regulatory bodies - that is independent from other branches or arms of the government.

Malaysia	Singapore	Philippines	Thailand
PART IV - APPOINTMENT, FUNCTIONS AND POWERS OF COMMISSIONER	ART II PERSONAL DATA PROTECTION COMMISSION	CHAPTER II THE NATIONAL PRIVACY COMMISSION	Section 8 Personal Data Protection Committee

	AND ADMINISTRATION Personal Data Protection Commission 5.— (1) The Info-communications Media Development Authority is designated as the Personal Data Protection Commission. (2) The Personal Data Protection Commission is responsible for the administration of this Act.		

Functions of the Regulatory Body

Malaysia	Singapore	Philippines	Thailand
Functions of Commissioner 48. The Commissioner shall have the following functions: (a) to advise the Minister on the national policy for personal data protection and all other related matters; (b) to implement and enforce the personal data protection laws, including the formulation of operational policies and procedures; (c) to promote and encourage associations	Functions of Commission 6. The functions of the Commission shall be — (a) to promote awareness of data protection in Singapore; (b) to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection; (c)to advise the Government on all matters relating to data protection;	SEC. 7. Functions of the National Privacy Commission. – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions: (a) Ensure compliance of	Section 16 The Committee shall have the following duties and power: (1) to make the master plan on the operation for the promotion and protection of Personal Data, which are consistent with policies, national strategies and relevant national plans, in order to propose to the committee of the national digital economy and society, in accordance with the law governing development of the digital economy and society; (2) to promote and support

or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of this Act (d) to cooperate with bodies corporate or government agencies for the purpose of performing his functions; (e) to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act; (f) to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to	(d) to represent the Government internationally on matters relating to data protection; (e) to conduct research and studies and promote educational activities relating to data protection, including organizing and conducting seminars, workshops and symposia relating thereto, and supporting other organizations conducting such activities; (f) to manage technical co-operation and exchange in the area of data protection with other organizations, including foreign data protection authorities and international or inter-governmental organizations, on its own behalf or on behalf of the Government; (g) to administer and enforce this Act; (h) to carry out functions conferred on the Commission under any other written law; and	personal information controllers with the provisions of this Act; (b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: Provided, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act; (c) Issue cease and desist orders, impose a temporary or permanent ban on the	government agencies and the private sector in carrying out of activities in accordance with the master plan under (1), as well as to conduct the evaluation of the operation result of such master plan; (3) to determine measures or guidelines of the operation in relation to Personal Data protection in order to comply with this Act; (4) to issue notifications or rules for the execution of this Act; (5) to announce and establish criteria for providing protection of Personal Data which is sent or transferred to a foreign country; (6) to announce and establish guidance for the protection of Personal Data as guidelines which the Data Controller and the Data Processor shall comply; (7) to recommend the Cabinet on the enactment, or revision, of the existing laws or rules applicable to the protection of Personal Data; (8) to recommend the Cabinet on the enactment of the Royal Decree or reconsideration the suitability of this Act at least every five years; (9) to provide advice or

their personal data; (g) to monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any person; (h) to promote awareness and dissemination of information to the public about the operation of this Act; (i) to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data; (j) to represent Malaysia through participation in events that relate to personal data protection as authorized by the Minister, whether within or outside Malaysia; and (k) to carry out such activities and do such things as are necessary,	(i) to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order published in the Gazette.	processing of personal information, upon finding that the processing will be detrimental to national security and public interest; (d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy; (e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act; (f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country; (g) Publish on a regular basis a guide to all laws relating to data protection;	consultancy on any operation for the protection of Personal Data of the government agency and private agency, in acting in compliance with this Act; (10) to interpret and render rulings with respect to the issues arising from the enforcement of this Act; (11) to promote and support learning skills and understanding on the protection of Personal Data among the public; (12) to promote and support research for the development of technology relating to the protection of Personal Data; (13) to perform any other acts as prescribed by this Act, or other laws, which state the duties and power of the Committee.

advantageous and proper for the administration of this Act, or such other purposes consistent with this Act as may be directed by the Minister.		(h) Publish a compilation of agency system of records and notices, including index and other finding aids; (i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act; (j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: (k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person; (l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws; (m) Propose legislation, amendments or modifications to Philippine laws on privacy	

		or data protection as may be necessary; (n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection; (o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws; (p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and (q) Generally, perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.	

Penalties

All AMS privacy laws have set fines and imprisonment for violations.

Malaysia	Singapore	Philippines	Thailand
130. Unlawful collecting, etc., of personal data 131. Abetment and attempt punishable as offences 132. Compounding of offences 133. Offences by body corporate	PART X - GENERAL 51. Offences and penalties 52. Offences by bodies corporate, etc. 53. Liability of employers for acts of employees 55. Composition of offences 56, General penalties 57. Public servants and public officers	CHAPTER VIII PENALTIES Sec 25. Unauthorized Processing of Personal Information and Sensitive Personal Information SEC 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence SEC 27. Improper Disposal of Personal Information and Sensitive Personal Information SEC 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes Sec 29. Unauthorized Access or Intentional Breach SEC 30 Concealment of Security Breaches Involving Sensitive Personal Information SEC 31. Malicious Disclosure	Chapter VII Penalties Part I - Criminal Liability Section 79. Any Data Controller who violates the relevant provisions of this law in a manner that is likely to cause other person to suffer any damage, impair his or her reputation, or expose such other person to be scorned, hated, or humiliated, shall be punished with imprisonment for a term not exceeding six months, a fine not exceeding Baht five hundred thousand, or both. Section 80. Any person who comes to know the Personal Data of another person as a result of performing duties under this Act and discloses it to any other person shall be punished with imprisonment for a term not exceeding six months, a fine not exceeding Baht five hundred thousand, or both. Section 81 In the case where the offender who commits the offense under this Act is a juristic person

		SEC 32. Unauthorized Disclosure SEC. 33. Combination or Series of Acts SEC. 34 Extent of Liability SEC. 35. Large-Scale SEC. 36. Offense Committed by Public Officer SEC. 37. Restitution.	and the offense is conducted as a result of the instructions given by or the act of any director, manager or person, who shall be responsible for such act of the juristic person, or in the case where such person has a duty to instruct or perform any act, but omits to instruct or perform such act until the juristic person commits such offense, such person shall also be punished with the punishment as prescribed for such offense. Part II Administrative Liability Section 82 Any Data Controller who fails to comply with relevant sections or fails to obtain consent using a form or statement set forth by the Committee..., or fails to notify the impact of the withdrawal of consent, shall be punished with an administrative fine not exceeding Baht one million. Section 83 Any Data Controller who obtains consent by deceiving or misleading the data subject about the purposes, or fails to send or transfer the Personal Data, shall be punished with an administrative fine not exceeding

			Baht three million. Section 84 Any Data Controller who violates relevant sections or fails to send or transfer the Personal Data, shall be punished with an administrative fine not exceeding Baht five million. Section 85 Any Data Processor who fails to comply with relevant sections, shall be punished with an administrative fine not exceeding Baht one million. Section 86 Any Data Processor who fails to comply with relevant sections without appropriate reasons or fails to send or transfer the Personal Data in accordance with relevant sections, shall be punished with an administrative fine not exceeding Baht three million. Section 87 Any Data Processor who send or transfer the Personal Data under section 26 paragraph one or three, by not complying with section 29 paragraph one or three, shall be punished with an administrative fine not exceeding Baht five million. Section 88 Any representative of

			the Data Controller or of the Data Processor who fails to comply with section 39 paragraph one which applies mutatis mutandis according to section 39 paragraph two, and section 41 paragraph one which applies mutatis mutandis according to section 41 paragraph four, shall be punished with an administrative fine not exceeding Baht one million. Section 89 Any person who fails to act in compliance with the order given by the expert committee, or fails to provide statement of facts undersection 75, or fails to comply with section 76(1), or fails to facilitate government officials under section 76 paragraph four, shall be punished with an administrative fine not exceeding Baht five hundred thousand. Section 90 The expert committee shall have the power to render the punishment as an administrative fine prescribed in this Part. In the event that it deems fit, the expert committee may issue an order for rectification or a warning first.

V. PRIVACY REGULATORY LANDSCAPE IN ASIA PACIFIC[73]

"Regulations are indispensable to the proper functioning of economies and societies", according to the OECD, as they "underpin markets, protect the rights and safety of citizens and ensure the delivery of public goods and services."[74]

The matrix below compares the regulatry landscape in select Asia- Pacific (including ASEAN) states.

Jurisdiction	Constitutional right to privacy	Regulator	Independent	Maximum penalty for breach of law
Australia	No	Office of the Australian Information Commissioner	Yes	Financial penalty (up to AU$2.1 million) and enforceable undertakings
Hong Kong, China	Yes	The Office of the Privacy Commissioner for Personal Data	Yes	Personal liability and/or criminal sanctions
Japan	Yes	Personal Information Protection Commission	Yes	Personal liability and/or criminal sanctions
Malaysia	No	Personal Data Protection Department, Malaysian Communications and Multimedia Commission	No	Personal liability and/or criminal sanctions
New Zealand	No	Privacy Commissioner's Office	Yes	Financial penalty (up to NZ $350,000) and codes of practice

73 DeLoitte *Unity in Diversity: The Asia Pacific Privacy Guide July 2019*, p. 75

74 OECD *Regulatory Policy and Governance* https://www.oecd-ilibrary.org/governance/regulatory-policy-and-governance/setting-the-scene-the-importance-of-regulatory-policy_9789264116573-4-en#:~:text=Regulations%20are%20indispensable%20to%20the,time%2C%20regulations%20are%20rarely%20costless.

Philippines	Yes	National Privacy Commission	Yes	Personal liability and/or criminal sanctions
Singapore	No	Personal Data Protection Commission / Info communications Media Development Authority	No	Personal liability and/or criminal sanctions
Republic of Korea	Yes	Personal Information Protection Commission	Yes	Personal liability and/or criminal sanctions
Thailand	No	Personal Data Protection Committee	Yes	Personal liability and/or criminal sanctions

Asian and Pacific Training Centre for Information and Communication Technology for Development
5th Floor, G-Tower, 175 Art Center Daero, Yeonsu-gu, Incheon, Republic of Korea

www.unapcict.org