Singapore Journal of Legal Studies
[2021] 76–99

THREE SHADES OF DATA: AUSTRALIA, PHILIPPINES, THAILAND

ROBERT BRIAN **SMITH***, MARK **PERRY**** & NUCHAREE NUCHKOOM **SMITH***

Unauthorised access to data has raised concern amongst business, citizens and legislators globally. However, different jurisdictions have taken various approaches ranging from controlling access via data protection legislation to deeming liability based on the nature of the data, such as through privacy legislation. This paper is a comparative analysis of the privacy legislation of the Philippines, Thailand and Australia through their *Data Privacy Act of 2012*, the *Personal Data Protection Act 2019*, and the *Privacy Act 1988*, respectively. These Acts have many provisions, and Australian states also have their own acts. The Australian federal legislation is the most developed of the three and its effectiveness can be evaluated by outcomes of investigations and enforceable undertakings issued for data breaches. In all three countries, the primary data privacy legislation is also supported by privacy-related provisions under other statues. The analysis focuses on types of data protected by privacy provisions, methods for investigating breaches and imposing penalties, and whether breaches result in administrative action, civil liability or criminal offences.

I. INTRODUCTION

The first 20 years of the 21st century have brought vast changes in the manner in which data is collected, stored, analysed and used.[1] This has raised serious privacy concerns within governments as well as the general population. Government initial responses focussed on privacy laws mandating what data can be collected, how it must be managed, and action that must be taken if there is an inadvertent release of data. At the same time as these governmental responses, criminal networks became aware of the value of data and sophisticated transnational cybercrime attacks became both more prevalent and harder to prosecute. This has led to a need for a much more integrated cross border response from law enforcement authorities.

* Academic Advisor, Walailak University Thailand and MPhil (Law) graduate, University of New England, Australia. This research is supported by an Australian Government Research Training Program (RTP) Scholarship.
** Professor of Law, University of New England.
*** Assistant Professor in Law, School of Social Science and Law, Walailak University, Thailand. Corresponding Author.

1 See for instance Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford: Oxford University Press, 2014).

Essentially, there are three key directions that governments have pursued: legislation that protects the privacy of a person or organisation; legislation that provides for jurisdiction dependant civil or criminal sanctions for inadvertent privacy breaches or limited malicious data breaches; and, for the most extreme cases, rigorous cybercrime legislation with cross-border cooperation.

This paper provides a comparative analysis of the legislative approaches of Australia, the Philippines and Thailand. Australia's privacy and data protection legislation has been in force since 2001 and is mature in form and execution. Due to its federal structure, the legislative response has added complexity as the six states and two territories also have jurisdiction over some matters. This will be discussed later in the paper. Australia is a state party to the *Convention on Cybercrime*.[2] The Philippines, during its year as Chair of Association of Southeast Asian Nations ("ASEAN"), took the lead country role for cybercrime legislation and subsequently took the lead country role for privacy/data protection. The Philippines is a state party to the *Convention on Cybercrime*: the only ASEAN member. Thailand on the other hand introduced its *Personal Data Protection Act*,[3] but is not a party to the *Convention on Cybercrime.*

The term data is commonly understood to mean "items of (chiefly numerical) information, especially one obtained by scientific work, a number of which are typically collected together for reference, analysis, or calculation".[4] Other definitions are used in specific environments, especially regulatory ones, such as "computer data" taken to mean "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function",[5] and a further distinction is added with the term "personal data" as it has been defined by the significant development of Europe's *General Data Protection Regulation* to mean "any information relating to an identified or identifiable natural person".[6]

II. Methodology

This research is based on an analysis of the privacy and data protection provided under the constitution, legislation and jurisprudence of the three nominated countries to determine whether it is sufficiently robust and not open to abuse by state parties. As data breaches often have extra-territorial consequences, the analysis includes a discussion of the extra-territorial reach of the legislation.

---

2 *Budapest*, 23 November 2001, 2296 UNTS 40916 (entered into force 1 July 2004) [*Convention on Cybercrime*]. A Council of Europe convention opened for member and non-member states (Australia entered into force on 1 March 2013).

3 *B.E. 2562 (2019)* (Thailand), online: Ministry of Digital Economy and Society (translation) <https://thainetizen.org/docs/data-protection-cybersecurity-acts/> [*Data Protection Act*].

4 *The Oxford English Dictionary*, 3d ed, *sub verbo* "data".

5 *Convention on Cybercrime*, *supra* note 2, art 1.

6 EC, *Regulation (EU) of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ, L 119, art 4 [*GDPR*].

III. Data Privacy and Data Protection Legislation

A. *Protections under International Conventions*

As data privacy breaches today often have a transnational dimension, it is essential that there be close cross border cooperation to address these issues. All three countries are, therefore, parties to various international conventions.

Australia and the Philippines are state parties to the *Convention on Cybercrime*.[7] The *Convention* requires that state parties make illegal access to the whole or part of a computer system a criminal offence[8], as well as making 'the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data' a criminal offence.[9] More importantly, the *Convention* mandates that state parties cooperate as widely as possible in collecting evidence, investigating and conducting proceedings concerning criminal offences related to computer systems and data.[10]

All three economies are members of Asia Pacific Economic Cooperation ("APEC"), which developed its own privacy framework in 2005 and revised it in 2015.[11] The framework is intended to apply to natural persons and not legal persons[12] and recognises the need to consider social, cultural and other differences in the member economies.[13] It also allows them to implement the framework at a domestic level to suit their circumstances.[14] The framework includes a number of principles: preventing misuse of personal data and consequent harm to individuals;[15] notice should be given so that individuals may know what data is being collected about them and why;[16] data collection should be restricted to information relevant to the purpose of the data collection process[17] and only used for that purpose;[18] where possible an individual should be given a choice in relation to the collection, usage, and disclosure of their information[19] which should be accurate, complete and up-to-date for the intended purpose;[20] personal information should be protected with reasonable security safeguards;[21] individuals should be able to access and correct their personal information;[22] and finally personal information controllers should be accountable for complying with the measures.[23]

---

7 *Convention on Cybercrime*, *supra* note 2.
8 *Ibid*, art 2.
9 *Ibid*, art 3.
10 *Ibid*, art 25(1).
11 *APEC Privacy Framework (2015)* at para 5 [*APEC Privacy Framework*].
12 *Ibid* at para 9.
13 *Ibid* at para 17.
14 *Ibid* at para 18.
15 *Ibid* at para 20.
16 *Ibid* at paras 21-23.
17 *Ibid* at para 24.
18 *Ibid* at para 25.
19 *Ibid* at para 26.
20 *Ibid* at para 27.
21 *Ibid* at para 28.
22 *Ibid* at paras 29-31.
23 *Ibid* at para 32.

The Framework also provides guidance on domestic and international implementation.[24] Internationally, there should be information sharing among member economies;[25] cross-border cooperation in investigation and enforcement;[26] development of cross-border privacy mechanisms;[27] as far as possible, there should be no restriction on cross-border transfers[28] and there should be interoperability between privacy frameworks.[29]

To implement the framework APEC developed the *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement*[30] and the *APEC Cross-Border Privacy Rules System.*[31] Australia became a participant in the APEC Cross-Border Privacy Rules ("CBPR") system in November 2018.[32] The Philippines announced its participation in September 2019 as it saw benefits in terms of trade.[33] In August 2019 the Philippines chaired the first ASEAN Data Protection and Privacy Forum in Bangkok.[34] This initiative was endorsed by the 19th ASEAN Telecommunications and Information Technology Ministers Meeting ("TELMIN") meeting as a key initiative on data governance.[35]

ASEAN, which membership includes the Philippines and Thailand, also developed its own personal data protection framework.[36] This framework has been acceded to by all ten members of ASEAN and in its preamble acknowledges the APEC privacy framework. It seeks 'to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information'.[37] In line with ASEAN's policy of consensus and non-intervention in the affairs of member states,[38] the framework 'does not constitute or create, and is

---

24 *Ibid* at pt IV.

25 *Ibid* at paras 57-61.

26 *Ibid* at paras 62-64.

27 *Ibid* at paras 65-68.

28 *Ibid* at paras 69, 70.

29 *Ibid* at paras 71, 72.

30 Opened for signature 28 February 2010.

31 *APEC Cross-Border Privacy Rules System*.

32 Australia, Attorney-General's Department, "Asia-Pacific Economic Cooperation and Privacy", online: Attorney-General's Department <https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/APECprivacy.aspx>.

33 Philippines, National Privacy Commission, "PH joins APEC Privacy System" (20 September 2019), online: National Privacy Commission <https://www.privacy.gov.ph/2019/09/ph-joins-apec-privacy-system/>.

34 Philippines, National Privacy Commission, "PH leads ASEAN's move to protect privacy" (22 August 2019), online: National Privacy Commission <https://www.privacy.gov.ph/2019/08/ph-leads-asean-move-to-protect-privacy/>.

35 ASEAN, Joint Media Statement, "The 19th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings Joint Media Statement" (25 October 2019), online: ASEAN <https://asean.org/joint-media-statement-19th-asean-telecommunications-information-technology-ministers-meeting-related-meetings/#:~:targetText=The%2019th%20ASEAN%20Telecommunications,24%20and%2025%20October%202019.&targetText=The%20Ministers%20also%20held%20consultations,and% 20the%20Republic%20of%20Korea.>.

36 *ASEAN Framework on Personal Data Protection*, ASEAN, 25 November 2016 (entered into force 25 November 2016).

37 *Ibid*, art 1.

38 *Charter of the Association of Southeast Asian Nations*, 20 November 2007, 2624 UNTS 46745 (entered into force 15 December 2008) art 2(2).

not intended to constitute or create, obligations under domestic or international law and will not give rise to any legal process and will not be deemed to constitute or create any legally binding or enforceable obligations, express or implied'.[39]

The *Framework* describes the principles that should be adopted by the member states in relation to personal data protection, namely: personal data should not be collected, used or disclosed without the person being notified and giving consent;[40] the collection and disclosure of data should have a purpose that a reasonable person would consider appropriate;[41] the data must be accurate and complete for the proposed purpose;[42] security safeguards should be in place to protect the data;[43] an individual or organisation should be able to access its data and correct any errors or omissions;[44] consent should be given and/or suitable security mechanisms put in place before data is transferred to another country or territory;[45] personal data should only be retained for as long as is needed for legal or business purposes;[46] and finally, an organisation must be accountable for ensuring that its measures comply with these principles.[47] Cooperation and collaboration are encouraged.[48]

B. *Constitutional Protection*

The *Australian Constitution*[49] is an artefact of another age having been proclaimed in 1900 and last amended in 1977.[50] As such, it makes no reference to the protection of privacy.

Article III—Bill of Rights of the *Philippines Constitution*[51] protects the right to privacy of communications and correspondence, unless otherwise permitted by law.[52]

The *Thai Constitution*[53] provides the right to privacy, dignity, reputation and family. However, these rights can be overridden 'by virtue of a provision of law enacted only to the extent of necessity of public interest'.[54] The *Thai Constitution* also provides the right to access public data or information in the possession of a government agency subject to legal restrictions[55] with the right for data or information to be readily accessible to the public.[56]

---

39 *ASEAN Framework on Personal Data Protection, supra* note 36, art 2.
40 *Ibid*, art 6(a).
41 *Ibid*, art 6(b).
42 *Ibid*, art 6(c).
43 *Ibid*, art 6(d).
44 *Ibid*, art 6(e).
45 *Ibid*, art 6(f).
46 *Ibid*, art 6(g).
47 *Ibid*, art 6(h).
48 *Ibid*, art 8.
49 *Commonwealth of Australia Constitution Act* (Cth) [*Australian Constitution*].
50 *Ibid*.
51 *Constitution of the Republic of the Philippines 1987* (Philippines), art III [*Philippines Constitution*].
52 *Ibid*, art III, s 3.
53 *Constitution of the Kingdom of Thailand (B.E. 2560 (2017)* (Thailand)[*Thai Constitution*], online: Office of the Council of State (translation) <http://web.krisdika.go.th/data/outsitedata/outsite21/file/Constitution_of_the_Kingdom_of_Thailand.pdf>.
54 *Ibid*, art 32.
55 *Ibid*, art 41, 59.
56 *Ibid*, art 59.

In other words, whilst the Constitutions of the Philippines and Thailand have privacy protections, they are conditional and can be overridden by any legislation. The focus should, therefore, shift to the substantive legislation of the three countries that provides some protection.

C. *Legislative Protection*

1. *Australia*

Being a federal system, Australia has both federal and state and territory legislation. Privacy is both a federal and state responsibility.[57] All of the states and territories, with the sole exception of South Australia, have enacted their own privacy legislation.[58] The Australian Capital Territory enacted the *Information Privacy Act 2014*;[59] New South Wales enacted the *Privacy and Personal Information Protection Act 1998*,[60] *Privacy Code of Practice (General) 2003*[61] and the *Health Records and Information Privacy Act 2002*;[62] The Northern Territory enacted the *Information Act 2002*;[63] Queensland enacted the *Information Privacy Act 2009*;[64] Tasmania enacted the *Personal Information and Protection Act 2004*;[65] Victoria enacted the *Privacy and Data Protection Act 2014*;[66] and Western Australia enacted the *Freedom of Information Act 1992*[67] "which includes some privacy principles related to the disclosure and amendment of personal information".[68] The application of these laws in the states is largely confined to the public sector actors in each state.[69]

This paper will focus on the federal legislation of the Commonwealth of Australia namely: *Privacy Act 1998*:[70] *Privacy Amendment (Notifiable Data Breaches) Act 2017*;[71] *Privacy Regulation 2013*,[72] and associated legal instruments where relevant to the discussion. The legislation only applies to Australian Government agencies and organisations with an annual turnover of more than $3 million and some other narrowly defined organisations, such as those related to health services and credit reporting.

---

57 Australian Government, Office of the Australian Information Commissioner, 'Privacy in your state', 6 August 2019, online: OAIC <https://www.oaic.gov.au/privacy/privacy-in-your-state/>.

58 *Ibid*.

59 (ACT) [*Information Privacy Act*].

60 (*as amended at 1 July 2019*) (NSW) [*Privacy and Personal Information Protection Act*].

61 (NSW) [*Privacy Code of Practice*].

62 (NSW) [*Health Records and Information Privacy Act*].

63 (NT) [*Information Act 2002*].

64 (Qld) [*Information Privacy Act*].

65 (Tas) [*Personal Information Protection Act*].

66 *Incorporating amendments as at 18 September 2019* (Vic) [*Privacy and Data Protection Act*].

67 (WA) [*Freedom of Information Act*].

68 OAIC, *supra* note 57.

69 *Ibid*.

70 *(as amended to 20 December 2018)* (Cth) [*Privacy Act*].

71 (Cth) [*Privacy Amendment (Notifiable Data Breaches) Act*]. These amendments have been incorporated into the latest version of the Act.

72 *(as amended to 10 April 2019)* (Cth) [*Privacy Regulation 2013*].

The *Privacy Act* (as amended)[73] is large, some 365 pages, and complex, having been amended 80 times. Personal information is defined in the Act as "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not".[74]

The *Act* has defined the following Australian Privacy Principles which must be complied with by all entities whether public or private sector under the *Privacy Act*:

(a) Principle 1 – open and transparent management of personal information;[75]
(b) Principle 2 – anonymity and pseudonymity[76]—individuals must have the option of anonymity, or of using a pseudonym;[77]
(c) Principle 3 – collection of solicited personal information[78]—an entity must only collect personal information necessary for the entities' functions and activities;[79] sensitive information shall only be collected with consent;[80]
(d) Principle 4 – dealing with unsolicited personal information[81]—if it is determined the information could not have been collected under Principle 3 or from a government record it must be destroyed or de-identified;[82]
(e) Principle 5 – notification of the collection of personal information[83]—the details of the entity collecting the data must be disclosed as must the reason for the collection of the data;[84]
(f) Principle 6 – use or disclosure of personal information[85]—data collected for one purpose must not be used or disclosed without the individual's consent;[86]
(g) Principle 7 – direct marketing[87]—personal information must not, with some exceptions be used or disclosed for direct marketing;[88]
(h) Principle 8 – cross-border disclosure of personal information[89]—the entity must take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles;[90]
(i) Principle 9 – adoption, use or disclosure of government related identifiers[91]—a government related identifier of an individual must not be used

---

73 *Privacy Act*, *supra* note 70.
74 *Ibid*, s 5.
75 *Ibid*, sch 1, cl 1.
76 *Ibid*, sch 1, cl 2.
77 *Ibid*, sch 1, cl 2.1.
78 *Ibid*, sch 1, cl 3.
79 *Ibid*, sch 1, cl 3.1, cl 3.2.
80 *Ibid*, sch 1, cl 3.3.
81 *Ibid*, sch 1, cl 4.
82 *Ibid*, sch 1, cl 4.3.
83 *Ibid*, sch 1, cl 5.
84 *Ibid*.
85 *Ibid*, sch 1, cl 6.
86 *Ibid*, sch 1, cl 6.1.
87 *Ibid*, sch 1, cl 7.
88 *Ibid*, sch 1, cl 7.1.
89 *Ibid*, sch 1, cl 8.
90 *Ibid*, sch 1, cl 8.1.
91 *Ibid*, sch 1, cl 9.

by an organisation as its own identifier of the individual unless it is required by law;[92]

(j) Principle 10 – quality of personal information[93]—personal information that the entity collects should be accurate, up-to-date and complete[94] and that the data it uses or discloses is accurate, up-to-date, complete and relevant;[95]

(k) Principle 11 – security of personal information[96]—personal information should be protected from misuse, interference, loss, from unauthorised access, modification or disclosure; [97]

(l) Principle 12 – access to personal information[98]—on request an individual must be given access to their data;[99]

(m) Principle 13 – correction of personal information[100]—an entity must ensure, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.[101]

The privacy principles clearly meet the requirements of the *APEC Privacy Framework*.[102]

Part IIIA deals in detail with the privacy of information relating to credit reporting and the penalties that apply for non-compliance.[103]

Part IIIC sets up a scheme for notification of eligible data breaches *ie*, if "there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates. An entity must give a notification if it has reasonable grounds to believe that an eligible data breach has happened; or it is directed to do so by the Commissioner."[104]

The Information Commissioner has the following functions: guidance;[105] monitoring;[106] and advising.[107] The Commissioner may conduct an assessment relating to the Australian Privacy Principles *etc* and determine whether an entity is meeting its obligations;[108] and direct an agency to give a privacy impact assessment.[109] The Commissioner may recognise alternative dispute resolution schemes.[110]

---

92 *Ibid*, sch 1, cl 9.1.
93 *Ibid*, sch 1, cl 10.
94 *Ibid*, sch 1, cl 10.1.
95 *Ibid*, sch 1, cl 10.2.
96 *Ibid*, sch 1, cl 11.
97 *Ibid*, sch 1, cl 11.1.
98 *Ibid*, sch 1, cl 12.
99 *Ibid*, sch 1, cl 12.1.
100 *Ibid*, sch 1, cl 13.
101 *Ibid*, sch 1, cl 13.1.
102 *APEC Privacy Framework*, *supra* note 11.
103 *Privacy Act*, *supra* note 70, Pt IIIA.
104 *Ibid*, s 26WA.
105 *Ibid*, s 28.
106 *Ibid*, s 28A.
107 *Ibid*, s 28B.
108 *Ibid*, s 33C.
109 *Ibid*, s 33D.
110 *Ibid*, s 35A.

If an individual lodges a privacy complaint then the Commissioner must investigate.[111] The Commissioner may also initiate an investigation where there may be interference with the privacy of an individual.[112] The investigative power of the Commissioner includes conciliating a complaint; making preliminary enquiries of any person: requiring a person to give information or documents, or to attend a compulsory conference: or under certain circumstances transferring the matters to an alternative complaint body.[113] The Commissioner may make a determination following an investigation and the entity must comply with certain declarations included in the determination with court proceedings commenced, if required, to enforce the determination.[114]

Enforcement provisions under the *Privacy Act* are enforceable civil penalty provisions;[115] enforceable undertakings;[116] and injunctions.[117] Chapter 2 of the *Criminal Code*[118] which sets out the general principles of criminal responsibility applies to all offences against the *Act*.[119] The *Act* has extra-territorial application if there is an Australian link.[120]

The Privacy Commissioner has issued a *Code* on Credit Reporting[121] as well as *Rules* and *Explanatory Statements* on Privacy and National Health;[122] Privacy and Credit Related Research;[123] Privacy and Missing Persons;[124] and Privacy and the use of Tax File Numbers.[125]

From 2011 to 31 October 2019, the Information Commissioner has completed 20 Commissioner-initiated investigations to look at specific acts or practices, systemic problems in handling personal information or practices or problems occurring at more than one entity.[126] The many issues investigated included:[127] the release of health data that allowed some health providers to be identified; inadvertent data breach at Australian Red Cross Blood Service; hacking of adult dating sites (a joint investigation with Canada); target of a cyber-attack exposing customer details; personal information of asylum seekers on the website of government department; reports of boxes of unsecured medical reports at a medical centre; personal information from a

---

111 *Ibid*, s 36A.
112 *Ibid*.
113 *Ibid*.
114 *Ibid*.
115 *Ibid*, s 80U.
116 *Ibid*, s 80V.
117 *Ibid*, s 80W.
118 *Criminal Code Act 1995 (Including amendments up to Act No. 156, 2018)* (Cth) [*Criminal Code*].
119 *Privacy Act, supra* note 70, s3A.
120 *Ibid*, s 5B.
121 *Privacy (Credit Reporting) Code 2014 (Version 2)* (Cth).
122 *National Health (Privacy) Rules 2018* (Cth); *Explanatory Statement: National Health (Privacy) Rules 2018* (Cth).
123 *Privacy (Credit Related Research) Rule 2014* (Cth); *Explanatory Statement: Privacy (Credit Related Research) Rule 2014* (Cth).
124 *Privacy (Persons Reported as Missing) Rule 2014* (Cth); *Explanatory Statement: Privacy (Persons Reported as Missing) Rule 2014* (Cth).
125 *Privacy (Tax File Number) Rule 2015* (Cth); *Explanatory Statement: Privacy (Tax File Number) Rule 2015* (Cth).
126 Australia, Office of the Australian Information Commissioner, "Investigation Reports" (23 March 2018), online: OAIC <https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/>.
127 The reports can be found on the Commissioner's website at <https://www.oaic.gov.au>.

dating website had been acquired by unauthorised persons; information on applicants for a Maritime Security Identity Card had been made publicly accessible online; personal information on Telstra's customers available online; a server holding customer information had been accessed by a hacker group; customer information held by a medical laboratory had been found on line; a data breach at a superannuation corporation's website to expose a weakness in the company's systems; a government agency held medical and pharmaceutical program information in the same database and collected individual medical records for an indeterminate time in an unsecured manner; hacking of email marketing data by the use of malware; personal information including credit card details of 77 million customers worldwide of Sony PlayStation Network and Qriocity had been compromised; a mailing list error that led to approximately 220,000 letters with the wrong addresses being mailed out; and personal information of a telecommunications company had been compromised.[128] Analysis of the reports shows that the majority of the investigations were triggered by media reports, with most of the remainder coming from information supplied directly to the Commissioner.

There have been 33 privacy determinations under section 52 of the *Privacy Act* from 1 November 2010 to 1 November 2019.[129] Privacy determinations are made where conciliation between the parties has failed.[130]

Enforceable Undertakings can be accepted from an entity under the *Regulatory Powers Act*[131] and a person under the *Personally Controlled Electronic Health Records Act*[132] where the Commissioner "considers there is a reasonable basis to suggest that the person or entity has interfered with the privacy of an individual".[133] Enforceable undertakings are generally accepted where the respondent has cooperated with an investigation, an enquiry into a data breach or an investigation and the Commissioner considers it would provide an appropriate regulatory outcome,[134] If the Commissioner considers that there is a breach of the undertaking, court action may be undertaken to enforce the undertaking and *Regulatory Powers Act*[135] or the *Personally Controlled Electronic Health Records Act,*[136] as appropriate.[137]

In the case of malicious access to data, Division 477 of the *Criminal Code*[138] establishes the following serious computer data related offences: unauthorised access to data, unauthorised modification of data, or any unauthorised impairment of electronic communication to or from a computer:[139] unauthorised modification of data to

---

128 *Ibid*.

129 Australia, Office of the Australian Information Commissioner, "Privacy Determinations" (28 June 2019), online: OAIC <https://www.oaic.gov.au/privacy/privacy-decisions/privacy determinations/>.

130 *Ibid*.

131 *Regulatory Powers (Standard Provisions) Act 2014 (including amendments up to 7 November 2017)* (Cth), s 114 [*Regulatory Powers Act*].

132 (Cth), s 94.

133 Australia, Office of the Australian Information Commissioner, "Enforceable undertakings" (28 June 2019), online: OAIC <https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/>.

134 *Ibid.*

135 *Regulatory Powers Act, supra* note 131, s 115.

136 *Personally Controlled Electronic Health Records Act supra* note 132, s 95.

137 OAIC, *supra* note 133.

138 *Criminal Code*, *supra* note 118, div 477.

139 *Ibid*, s 477.1(1)(a).

cause impairment;[140] unauthorised access to, or modification of, restricted data;[141] unauthorised impairment of data held on a computer disk;[142] possession or control of data with intent to commit a computer offence;[143] producing, supplying or obtaining data with intent to commit a computer offence.[144]

2. *Philippines*

The Philippines has enacted two substantive laws in relation to data privacy and data protection, namely the *Data Privacy Act of 2012*[145] with its *Implementing Rules and Regulations of the Data Privacy Act of 2012*[146] issued in 2016; and the *Cybercrime Prevention Act of 2012*[147] in 2012 with its *Implementing Rules and Regulations*[148] issued in 2015. Thus, it was three to four years between the proclamation of the Acts and them becoming effective.

The *Data Privacy Act* commences with the following *Declaration of Policy*:

> It is the policy of the state to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth, The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure the personal information in information and communication systems are secured and protected.[149]

Personal information is defined as:

> any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[150]

Protections accorded to journalists and their sources remain protected under the *Act*.[151] There is extra-territorial jurisdiction when an entity undertakes an act or engages in a practice where the subject is a Philippines citizen or resident or where the entity has a link with the Philippines.[152]

---

140 *Ibid*, s 477.2(1)(a).
141 *Ibid*, s 478.1.
142 *Ibid*, s 478.2.
143 *Ibid*, s 478.3.
144 *Ibid*, s 478.4.
145 (Philippines).
146 (Philippines) [*Implementing Rules and Regulations 2012*].
147 (Philippines) [*Cybercrime Act*].
148 *Implementing Rules and Regulations of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012" 2015* (Philippines) [*Implementing Rules and Regulations 2015*].
149 *Data Privacy Act of 2012, supra* note 145, s 2.
150 *Ibid*, s 3(g).
151 *Ibid*, s 5.
152 *Ibid*, s 6.

The *Act* established the National Privacy Commission to administer and implement the provisions of the *Act*.[153] Amongst its key roles are: ensure compliance of personal information controllers; receive and act on complaints; take action when data processing will be detrimental to national security and public interest; compel any entity, public or private to abide by its orders; monitor compliance of government entities and instrumentalities; coordinate with government agencies and the private sector to strengthen the protection of personal information; recommend the prosecution and imposition of penalties; assess the suitability of privacy codes adhered to by personal information controllers; provide assistance on privacy or data protection issues to any entity or individual; comment on, or propose legislation, amendments or modifications to privacy or data protection laws.[154] In addition, the commission is tasked with coordinating data privacy regulators in other countries; negotiate and contract cross-border application and implementation of respective privacy laws; and facilitate cross-border enforcement of data privacy protection.[155]

Personal information must be: collected for specified and legitimate purposes; processed fairly and lawfully; accurate, relevant and, where necessary kept up to date; adequate and not excessive; retained only for as long as necessary; and, kept in a form which permits identification of data subjects for no longer than is necessary.[156] Unless specific conditions apply, data should only be collected with the consent of the subject.[157] Collection of sensitive personal information,[158] which includes information such as an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations, health, education and genetic or sexual life, is prohibited and can only be collected in restricted circumstances.[159]

The data subject is entitled to be informed about the processing of their personal information; be provided with reasonable access to their personal information; dispute the accuracy of their personal information and have it corrected; suspend, withdraw or order the blocking, removal or destruction of their personal information if it is incomplete, outdated, false, unlawfully obtained, used for unauthorised purposes or are no longer necessary for the purposes for which they were collected and be indemnified for any associated damages.[160] "The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights."[161]

The personal data controller is required to implement appropriate measures to ensure the security of the personal information.[162] Each personal data controller is responsible for data under their control or custody including third party processing

---

153 *Ibid*, s 7.
154 *Ibid*.
155 *Ibid*.
156 *Ibid*, s 11.
157 *Ibid*, s 12.
158 A full definition of sensitive personal information: *Ibid*, s 3(l).
159 *Ibid*, s 13.
160 *Ibid*, s 16.
161 *Ibid,* s 17.
162 *Ibid*, s 20.

whether domestically or internationally.[163] Heads of government agencies are responsible for the security of the data within their organisation.[164]

To enforce the *Act*, the Commission may: issue compliance or enforcement order; issue cease and desist orders; recommend the prosecution of crimes; compel or petition a party to abide by its orders; and impose administrative fines.[165] All serious offences under the Act are criminal and carry a fine and/or a term of imprisonment.[166] "If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime."[167] Finally, restitution to the aggrieved party is governed by the *New Civil Code*.[168] The authors consider that the *Act* is in conformity with the ASEAN Framework on Personal Data Protection.[169]

There are at least another 23 Acts in the Philippines that include some privacy provisions.[170] As of October 2019, the National Privacy Commission has published four cases on its website. In December 2017, Jollibee Foods Corporation reported that persons unknown appeared to have gained access to the delivery customer database website.[171] After investigations, the Commission ordered that the operations of the Jollibee delivery website be suspended until the site's identified vulnerabilities are addressed; submit a security plan; re-engineer the data infrastructure; conduct a new Privacy Impact Assessment and file a monthly progress report until all of the matters are resolved.[172]

A much more serious data breach occurred on 23 April 2018 when the entire database of the website of Wendy's, another Philippines restaurant chain, was published online with the Commission receiving a copy on the same day.[173] It took

---

163 *Ibid*, s 21.

164 *Ibid*, s 22.

165 *Implementing Rules and Regulations 2015*, *supra* note 148, s 9(f).

166 *Data Privacy Act of 2012, supra* note 145, ss 25-32.

167 *Ibid*, s 34.

168 *Ibid*, s 37.

169 ASEAN, "Framework on Personal Data Protection" (16 November 2016), online: ASEAN <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>.

170 These include: *Anti-Photo and Video Voyeurism Act (2009)*; *Rape Victim Assistance and Protection Act (1998)*; *Department of Information and Communications Technology Act (2015)*; *Family Courts Act (1997)*; *The Alien Social Integration Act (1995)*; *Accessible Polling Places Act (2013)*; *Domestic Workers Act (2013)*; *Magna Carta for Homeowners and Homeowner's Associations (2010)*; *Children's Emergency Relief and Protection Act (2016)*; *Microfinance NGOs Act 2015*; *Rare Diseases Act of the Philippines (2016)*; *Postal Service Act (1992)*; *Expanded Anti-Trafficking in Persons Act (2012)*; *Anti-Child Pornography Act (2009)*; *Anti-Trafficking in Persons Act (2003)*; *Philippine AIDS Prevention and Control Act (1988)*; *Philippine Act on Crimes Against International Humanitarian Law, Genocide, and Other Crimes Against Humanity (2009)*; *Anti-Violence Against Women and Their Children Act (2004)*; *Juvenile Justice and Welfare Act (2006)*; *Electronics Engineering Lae (2004)*; *Credit Information System Act (2008)*; *Secrecy of Bank Deposits Act (1955)*.

171 Philippines, National Privacy Commission: Legal and Enforcement Office, "Re: Jollibee Foods Corporation: CID BN No. 17-043: Order 4 May 2018", online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/pospp/CIDBN_17-043_ORDER_May042018.pdf>.

172 *Ibid* at 2.

173 Philippines, National Privacy Commission, "RE: Wendy's Restaurant Inc Philippines Representative Office) Data Breach (2018) CIDBN no. 18-058: Order - 2 May 2018", online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/pospp/CIDBN_18-058_ORDER_May022018.pdf>.

three days for Wendy's to report the breach to the Commission and when they met the officers of the Commission on 2 May they had not advised data subjects details of the breach.[174] An order was issued on that date requiring Wendy's to "notify all affected data subjects with exposed sensitive personal information or information that can be used to enable identity fraud,"[175] and explain why further action should not be taken for their failure to notify the data subjects within the proper period of 72 hours.[176] They were also required to provide a copy of all logs prior to the data breach and the Privacy Policy at the time of the breach an update of internal investigations conducted as well as recommendations for information security measures that were not implemented".[177] Finally, they were required to conduct a new Privacy Impact Assessment.[178]

Facebook Inc. was part of an ongoing investigation in September 2018 concerning the exploitation of the "View As" feature to extract a user's access tokens without their consent.[179] Nearly 780,000 Philippines Facebook users were affected and were notified via an online application. The Commission argued that:

> The level of awareness for spam, phishing and identity theft in the Philippines is not the same as those of the United States and the other developed nations; considerations of risk must always consider the cultural milieu in which the risk is appreciated. For instance, this Commission takes notice that identity verification systems throughout the Philippines are quite weak.
>
> As a milieu, the increase in risk for phishing and/or identity theft is self-evident for those persons who were exposed through the unauthorized use of the access tokens.
>
> The Commission therefore deems it necessary that Facebook contemplate this cultural gap when notifying the affected data subjects. Facebook should modify its approach and provide a more conducive method that enables affected Filipino data subjects to better grasp the risks they face.[180]

The Order required Facebook to submit a more comprehensive Data Breach Notification Report and to notify the affected subjects through an appropriate Data Breach Notification.[181] In addition, they were required to provide identity theft and phishing insurance for affected Filipino data subjects or establish a dedicated helpdesk/help centre for Filipino data subjects on privacy related matters concerning Facebook.[182] Finally, they were to implement a program directed to Filipino data subjects to increase awareness on identity theft and phishing.[183]

---

174 *Ibid.*
175 *Ibid.*
176 *Ibid.*
177 *Ibid.*
178 *Ibid*.
179 Philippines, National Privacy Commission, "In Re: Facebook Forced Logout CID Case No. 18-J-162: Order - 17 October 2018", online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/pospp/CIDBN_18-J-162_ORDER_Oct172018b.pdf>.
180 *Ibid*.
181 *Ibid*.
182 *Ibid*.
183 *Ibid*.

A major initiative was undertaken by the Commission in October 2019 against online lenders who were using applications available on Google Play.[184] The identities and whereabouts of the lenders were unknown and although being served with notice via the press, none of the companies responded to the summons to appear before the Commission.[185] As a result, a Stop Processing Personal Data Order was issued against 17 entities where the name and URL were known, and against a further six where only their name was known.[186] In total, there were 103 Case Dockets covered by the Order.[187] The Stop Processing Order required the companies to immediately take down their online lending applications and stop personal online processing activities including those outsourced to third parties. The Order was to remain in effect until the resolution of the cases.[188] A copy of the Order was to be provided to Google LLC, the operator of the Google Play Store, 'for their compliance in accordance with the terms and conditions of their platform'.[189]

The National Privacy Commission also issues Advisory Opinions in relation to specific requests.[190] Whilst many of these are fairly straight forward and cite the privacy legislation, others are more complex. For instance, *Advisory Opinion No 2018-050*[191] cites the *GDPR*, and the author notes that the Philippines legislation was influenced by the *GDPR*.[192] It also cites the Office of the Privacy Commissioner for Personal Data, Hong Kong, in relation to personal data in the public domain,[193] as well as the Information Commissioner's Office of the United Kingdom with regard to personal information controllers ("PICs") having a declared and specified purpose for processing of personal information for marketing purposes.[194] In other words, the opinions are not restricted to considering only the jurisprudence of the Philippines.

The Philippines also has in place legislation to prosecute those who illegally access data. The *Cybercrime Prevention Act*[195] makes it an offence to act against the confidentiality, integrity, and availability of computer data and systems including illegal access;[196] illegal interception;[197] data interference;[198] and system interference.[199]

---

184 Philippines, National Privacy Commission, "In Re: Violations of the the Data Privacy Act by Companies operating Online Lending Applications: Order to Stop Online Data Processing" (18 October 2019), online: National Privacy Commission <https://www.privacy.gov.ph/2019/10/order-violations-of-the-data-privacy-act-by-several-companies-operating-online-lending-applications>.

185 *Ibid*.

186 *Ibid*.

187 *Ibid*.

188 *Ibid*.

189 *Ibid*.

190 Philippines, National Privacy Commission, "Advisory Opinions", online: National Privacy Commission <https://www.privacy.gov.ph/advisory-opinions/>.

191 Philippines, National Privacy Office, "Privacy Policy Office Advisory Opinion No 2018-050 – Cold Calls and Emails" (16 October 2018), online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-050.pdf>.

192 *Ibid* at 2.

193 *Ibid* at 1.

194 *Ibid* at 3.

195 *Cybercrime Act*, *supra* note 147.

196 *Ibid*, s 4(a)(1).

197 *Ibid*, s 4(a)(2).

198 *Ibid*, s 4(a)(3).

199 *Ibid*, s 4(a)(4).

The *Act* is supported by the *Implementing Rules and Regulations*.[200] Section 4(a)(1) and section 4(a)(3), amongst other sections of the Act, were appealed in the Supreme Court of the Philippines.[201] The court ruled both section 4(a)(1) and section 4(a)(3) valid and constitutional.[202]

3. *Thailand*

It must be borne in mind at the outset that there are complications when translating laws from one language to another, as many of our language constructs are tied to the jurisdiction's culture, norms and general understanding.[203] This commentary is based on the English version of the *Personal Data Protection Act, B.E. 2562 (2019)* as posted on the Electronic Transactions Development Agency ("ETDA") website.[204] It is "unofficial" as it is not in the Thai language.

Thailand has enacted four substantive laws in relation to data privacy and data protection, namely: *Computer Crime Act B.E. 2550 (2007)*,[205] *Computer Crime Act (No 2) B.E. 2560 (2017),*[206] *Personal Data Protection Act B.E. 2562 (2019)*[207] and the *Cybersecurity Act B.E. 2562 (2019).*[208]

The preamble of the *Personal Data Protection Act*[209] notes that the Act restricts the rights and freedoms of a person as protected by the Constitution with such action allowed by virtue of a law.[210] The Act applies to collection, use or disclosure of personal data where the controller or processor is in Thailand regardless of the location that the collection, use or disclosure takes place.[211] If the controller or processor is outside of Thailand it shall still protect Thai subjects who are in Thailand and who are offered goods or services to data subjects regardless as to whether payment has been made;[212] or monitoring behaviours of data subjects where such behaviour takes place in Thailand.[213] The *Act* defines personal data as any information relating

---

200 *Implementing Rules and Regulations 2012*, *supra* note 146; *Implementing Rules and Regulations 2015*, *supra* note 148.

201 Supreme Court of the Philippines *en banc*, 21 February 2014, *Jose Jesus M Disni et al v The Secretary of Justice et al*, G.R. No 203335 (Philippines).

202 *Ibid*, p 47, 2a and 2b respectively.

203 Robert Brian Smith, *Harmonisation of Laws in ASEAN: The Issue of English*, International Seminar on Politics, Administration and Development 2019 273 Conference Paper: online <https://www.researchgate.net/publication/343178725_CODE_026_HARMONISATION_OF_LAWS_IN_ASEAN_THE_ISSUE_OF_LANGUAGE.>.

204 (Thailand), online: EDTA <https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf.>.

205 (Thailand), online: <https://advox.globalvoices.org/wp-content/downloads/Act_on_Computer_Crime_2550(2007).pdf>[*Computer Crime Act*].

206 (Thailand), online: Wikisource <https://en.wikisource.org/wiki/Translation:Computer_Crimes_Act_(No._2)_2017> [*Computer Crime Act 2017*].

207 *Data Protection Act*, *supra* note 3.

208 (Thailand), online: <https://www.cc.kmutt.ac.th/Files/cybersecrutiy-act-2019-en.pdf> [*Cybersecurity Act*].

209 *Data Protection Act*, *supra* note 3, preamble.

210 *Ibid*, *Thai Constitution*, *supra* note 53, ss 26, 32, 33, 37.

211 *Data Protection Act*, *supra* note 3, s 5.

212 *Ibid*, s 5(1).

213 *Ibid*, s 5(2).

to a natural person which directly or indirectly leads to the identification of that person.[214]

The *Act* establishes a Personal Data Protection Committee.[215] Its mandate is extensive and includes:[216]developing a masterplan; promoting personal data protection and supporting government agencies and the private sector; determine measures or guidelines for the operation of the *Act*; issue notifications or rules for execution of the *Act*; develop criteria for providing protection of personal data to be transferred to a foreign country; establish guidelines to which the data controller and data processor must conform; recommend changes to legislation and review the *Act* every five years; provide consultancy services on compliance with the *Act* to government and private agencies; to interpret and render rulings arising from the *Act*; public promotion of understanding of the protection of personal data; and promote and support research and development of personal data protection technologies.

The data controller shall not collect, use or disclose personal data without consent.[217] In the case of minors, special provisions apply.[218] Personal data shall only be collected, used or disclosed according to the purpose notified to the subject at the time of collection.[219] Data shall only be collected to the extent necessary in relation to a lawful purpose.[220] Data from any other source than the subject shall only be collected with the informed consent of the subject[221] with heightened requirements:

> Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject, except where:
>
> it is to prevent or suppress a danger to life, body or health of the Person, where the data subject is incapable of giving consent by whatever reason;
>
> it is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or any other not-for-profit bodies with a political, religious, philosophical, or trade union purposes for their members, former members of the bodies, or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes, without disclosing the Personal Data outside of such foundations, associations or not-for-profit bodies;
>
> (1) it is information that is disclosed to the public with the explicit consent of the data subject;

---

214 The English translation is unclear, but it implies that it does not apply to deceased persons: *Ibid*, s 6.
215 *Ibid*, ch 1.
216 *Ibid*, s 16.
217 *Ibid*, s 19.
218 *Ibid*, s 20.
219 *Ibid*, s 21.
220 *Ibid*, s 22.
221 *Ibid*, s 25.

(2) it is necessary for the establishment, compliance, exercise or defence of legal claims;
(3) it is necessary for compliance with a law…[222]

Personal data sent overseas should have adequate standards of data protection and be carried out in accordance with the rules set by the Personal Data Collection Committee.[223] The data controller must ensure that the is accurate, up-to-date complete and not misleading.[224]

The *Act* establishes an Office of the Personal Data Protection amongst whose objectives is the protection of personal data.[225] It is tasked with appointing one or more expert committees to consider complaints, investigate data breaches and settle disputes.[226]

The subject receives compensation for a privacy breach[227] and the court may also award punitive damages.[228] Criminal liability applies to misuse of data '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',[229] sending data overseas without appropriate security protections[230] or disclosing personal data.[231] Administrative liability applies to the failure to comply with the requirements of the relevant sections of the *Act*.[232]

The *Act* looks to be in conformity with the *ASEAN Framework on Personal Data Protection*.[233] The data protection principles, on data controller obligations or the rights of data subjects "include many elements which reflect those in EU law (whether the 1995 Directive or the 2016 GDPR)".[234] Many of the obligations can, however, be overridden by Ministerial Regulations.[235]

The question then becomes what protections Thailand has in place for prosecuting offences by those illegally accessing data. Thailand enacted its *Computer Crime Act*[236] in 2007, amended it in 2017,[237] and its *Cybersecurity Act*[238] in 2019.

The *Computer Crime Act* specifies a number of data-related and computer-related crimes: illegally accessing computer data protected by specific security measures;[239]

---

222 *Ibid*, s 27.
223 *Ibid*, s 28.
224 *Ibid*, s 35.
225 *Ibid,* s 43.
226 *Ibid,* s 72.
227 *Ibid,* s 77.
228 *Ibid,* s 78.
229 *Ibid,* s 79.
230 *Ibid*.
231 *Ibid,* s 80.
232 *Ibid,* ss 82-90.
233 *ASEAN Framework on Personal Data Protection*, *supra* note 169.
234 Graham Greenleaf & Arthit Suriyawongkul, "Thailand's Draft Data Protection Bill: Many Strengths, Too Many Uncertainties" (2018), 153 Privacy Laws & Business International Report 23, online: SSRN <https://ssrn.com/abstract=3227862>.
235 *Ibid*.
236 *Computer Crime Act*, *supra* note 205.
237 *Computer Crime Act (No 2)*, *supra* note 206.
238 *Cybersecurity Act*, *supra* note 208.
239 *Computer Crime Act*, *supra* note 205, s 7.

illegally intercepting the transmission of computer data;[240] unauthorised damaging, destroying, altering, modifying or adding in whole or in part computer data of another person;[241] or sending computer data to another person so as to infer it is the normal computer usage of another person.[242] Whilst some provisions of the *Computer Crime Act (No 2)*[243] may be considered by some to be draconian[244] its main impact on data privacy protection is in relation to an increase in criminal sanctions, especially in relation to cyber-attacks on critical infrastructure data.[245]

The *Cybersecurity Act*[246] contains certain provisions in relation to the restriction of rights and freedom of a person, under the Thai Constitution so that the *Act* can "efficiently protect cybersecurity and to establish approaches to protect, cope with, and mitigate the risk of Cyber Threats which affect the national security and public order".[247] Amongst other functions, the *Act* established the Office of the National Cybersecurity Committee.[248] The Committee is tasked with developing a policy and plan on maintaining security which is required to include: integration of management of maintaining cybersecurity; develop capability to prevent, cope with and mitigate cyber threats; establish measure to protect critical information infrastructure; cooperate between public and private sectors as well as developing international cooperation for maintaining cybersecurity; research and development of personnel in public and private sectors; creating awareness and knowledge in maintaining cybersecurity; and develop rules and laws for maintaining cybersecurity.[249]

Critical information infrastructure under the *Act* includes: banking and finance, information technology and telecommunications, and public health.[250] All three are potential targets as they contain vast amounts of personal data. The Act also sets out the procedures for dealing with a cyber threat.[251] Offences for not complying with the requirements of the Act to maintain cybersecurity are criminal and can result in a term of imprisonment, a fine and/or both.[252]

In summary, then, Thailand has a three-pronged approach to personal data security. A specific data protection Act which describes how personal data is to be collected and stored with criminal or administrative penalties for non-compliance depending on their severity; a cybercrime law which provides criminal sanctions on those who misuse computer systems to access data; and an Act to enhance cybersecurity which provides criminal sanctions on those who do not take appropriate action to cope with cyber threats.

---

240 *Ibid*, s 8.
241 *Ibid*, s 9.
242 *Ibid*, s 11.
243 *Computer Crime Act (No 2)*, *supra* note 206.
244 See *eg*, Mong Palatino, "Thailand's draconian cyber law sparks rights fears" (23 December 2016), *ASEAN Beat* (blog), online: <https://thediplomat.com/2016/12/thailands-draconian-cyber-law-sparks-rights-fears/>.
245 *Computer Crime Act (No 2), supra* note 206, s 5.
246 *Cybersecurity Act*, *supra* note 208.
247 *Ibid*, preamble.
248 *Ibid*, ss 20-40.
249 *Ibid*, s 42.
250 *Ibid*, s 49
251 *Ibid*, ss 58-69.
252 *Ibid*, ss 70-77.

IV. Discussion

Whilst each set of privacy legislation has its own unique characteristics, there are some common threads—the privacy principles that form the backbone of personal information protection, whether based on APEC's or those of ASEAN are very similar. This is best illustrated in Table 1 where the Philippines and Thai legislation is related to the 13 Australian Privacy Principles.

Table 1 Comparison of the Privacy Legislation of the Philippines and Thailand with the Privacy Principles of Australia.

Australian Privacy Principle[253]	Philippines (Data Privacy Act)[254]	Thailand (Personal Data Protection Act)[255]
Australian Privacy Principle 1 Open and transparent management of personal information	Section 11 (General Data Privacy Principles) Section 12 (Criteria for Lawful Processing of Personal Information) Section 13 (Sensitive Personal Information and Privileged Information) Section 16 (Rights of the Data Subject)	Chapter III (Rights of the Data Subject)
Australian Privacy Principle 2 Anonymity and pseudonymity	See for instance: Privacy Policy Office Advisory Opinion No 2017-27[256] Privacy Policy Office Advisory Opinion No 2018-029[257]	Section 33 (re right of data subject to request erasure, destruction, or anonymization of data)
Australian Privacy Principle 3 Collection of solicited personal information	Section 12 (Criteria for Lawful Processing of Personal Information) Section 13 (Sensitive Personal Information and Privileged Information)	Section 24 – section 26 (re collection of personal data)

[253] Australia, Office of the Australian Information Commissioner, "Australian Privacy Principles—a summary for APP entities" (2018), online: OAIC <https://www.oaic.gov.au/assets/privacy/guidance-and-advice/app-quick-reference-tool.pdf.>

[254] *Data Privacy Act of 2012*, *supra* note 145.

[255] *Data Protection Act*, *supra* note 3.

[256] National Privacy Commission (Philippines), "Privacy Policy Office Advisory Opinion No 2017-27: Anonymized data for marketing analytics" (23 June 2017), online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-027.pdf >.

[257] National Privacy Commission (Philippines), *Privacy Policy Office Advisory Opinion No 2018-029*: *Pseudonymization of Personal and Sensitive Personal Information*, 6 June 2018, online: National Privacy Commission <https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AdOpNo.2018-029.pdf>.

Table 1 (*Continued*)

Australian Privacy Principle 4 Dealing with unsolicited personal information	Section 12 (Criteria for Lawful Processing of Personal Information) **and** penalties under Section 25 (Unauthorised Processing of Personal Information and Sensitive Personal Information)	Not explicitly stated but section 24 – section 26 (re collection of personal data) would apply **and** penalties under chapter VII would also apply.
Australian Privacy Principle 5 Notification of the collection of personal information	Section 12 (Criteria for Lawful Processing of Personal Information)	Section 19 (re consent) Section 20 (re consent for a minor)
Australian Privacy Principle 6 Use or disclosure of personal information	Section 11 (General Data Privacy Principles)	Part 2 (Personal Data Collection) Part 3 (Use or Disclosure of Personal Data)
Australian Privacy Principle 7 Direct marketing	See, for instance: Privacy Policy Office Advisory Opinion No 2018-050[258]	Part 2 (Personal Data Collection)
Australian Privacy Principle 8 Cross-border disclosure of personal information	Section 21 (Principle of Accountability)	Section 5 (re collection, use or disclosure of personal data)
Australian Privacy Principle 9 Adoption, use or disclosure of government related identifiers	Not explicitly stated **but** section13 (Sensitive Personal Information and Privileged Information) **and** penalties under section 25 (Unauthorised Processing of Personal Information and Sensitive Personal Information) would apply	Not explicitly stated **but** section 24 – section 26 (re collection of personal data) would apply **and** penalties under chapter VII would also apply.
Australian Privacy Principle 10 Quality of personal information	Section 11(c) (re accurate, relevant and up to date information)	Section 35 (re obligation of Data Controller to ensure data is accurate, up to date, complete and not misleading)

[258] Philippines, National Privacy Commission "Privacy Policy Office Advisory Opinion No 2018-050: Cold Calls and Emails" (16 October 2018), online: National Privacy Commission<https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-050.pdf>.

Table 1 (*Continued*)

Australian Privacy Principle 11 Security of personal information	Section 20 (Security of Personal Information)	Section 37 (re duties of the Data Controller)
Australian Privacy Principle 12 Access to personal information	Section 16(c) (Reasonable Access to Personal Information)	Section 30 (re right of data subject to request and obtain personal data)
Australian Privacy Principle 13 Correction of personal information	Section 16(d) (re dispute accuracy and require correction of personal information) and Section 16(e) (re suspend, withdraw, order blocking, removal or destruction of personal information)	Section 35 (re obligation of Data Controller to ensure data is accurate, up to date, complete and not misleading) **and** section 36 (re data subject request action be undertaken by Data Controller to comply)

As can be seen, most of the Australian Privacy Principles are also an integral part of the Philippine and Thai legislation. However, where they are not explicit, they are certainly implied. The legislation only applies to individuals and not to legal persons. Unusually, under the legislation of the Philippines, the personal information privacy protection is passed down to the individual's heirs and successors.

Australia's legislative framework is relatively mature, that of the Philippines is new but proving very effective, whilst that of Thailand is still in its infancy. On 21 May 2020, a Royal Decree postponed the effective date of some of the Thai provisions from 27 May 2020 to 1 June 2021.[259] The Decree exempts data controllers, but not data processors, from their obligations allowing them more time to prepare as "the rules, procedures and conditions that are detailed, complicated and have high technology requirements" and the delay will allow more time for the Thai public and private sectors to comply.[260] On 17 July 2020 the *Notification of the Ministry of Digital Economy and Society Prescribing Security Measure Standards for Personal Data B.E. 2563* was published in the Government Gazette.[261] It prescribes that "data controllers must arrange and implement security measure standards for personal data, covering the following three types of safeguards for accessing or controlling the use of personal data: (a) administrative, (b) technical, and (c) physical".[262]

Each jurisdiction has established a Commission tasked with guidance, monitoring, and advising on privacy issues. Amongst their monitoring activities are investigating personal information data breaches, imposing civil remedies and recommending

[259] PricewaterhouseCoopers, *Enforcement of some PDPA Provisions Postponed to 1 June 2021 and Security Measure Standards Implemented in the Interim Period* (3 August 2020), online: PwC Legal Insight <https://www.pwc.com/th/en/pwc-tax-insights/2020/legal/eng/2020-pwc-legal-insight04.pdf>.

[260] *Ibid*.

[261] *Ibid*.

[262] *Ibid*.

criminal prosecutions. The roles of each similar but not identical. The Commissions in all three jurisdictions have civil and administrative penalties available, the ability to order enforceable undertakings and injunctions, as well as criminal prosecution for unauthorised access to data and computer-related cybercrime.

Unfortunately, Thailand, as is common in several Southeast Asian jurisdictions, establishes complex administrative structures involving a number of interdependent committees rather than vesting the roles and responsibilities in one independent authority. As pointed out by Greenleaf and Suriyawongkul the complex structure defined in the Thai legislation has established a complex data protection authority lacking independence.[263] This can readily be seen from the composition of the Personal Data Protection Committee, namely:

(a) An independent Chairperson selected by a committee of which two members each are nominated by the Prime Minister, President of the Parliament, Ombudsman and the National Human Rights Commission;[264]
(b) the Permanent Secretary of the Ministry of Digital Economy and Society as Vice-Chairperson;[265]
(c) five directors consisting of the Permanent Secretary of the Prime Minister Office, the Secretary-General of the Council of State, the Secretary-General of the Consumer Protection Board, the Director-General of the Rights and Liberties Protection Department, and the Attorney General;[266] and
(d) Nine honorary directors as nine members, "having distinguished knowledge, skills, and experience in the field of personal data protection, consumer protection, information technology and communication, social science, law, health, finance, or any other field that must be relevant to, and useful for the protection of personal data".[267]

This committee's role is essentially to set policy.[268] The statutory authority tasked with protecting personal data and, encouraging and supporting the development of personal data protection is the Office of the Personal Data Protection Committee.[269] The Office, in turn, will be supervised by a Commission.[270] Complaints are handled by an expert committee appointed by the Personal Data Protection Committee.[271]

Whilst the jurisprudence associated with the Australian legislation is relatively mature, that of the Philippines is still evolving. It will be interesting to see how the Philippines judiciary rules on appeals against the legal arguments included in the Advisory Opinions of the National Privacy Office. As of October 2019, there have been no decided cases by the Supreme Court on the Act or the Implementing

---

263 Greenleaf & Suriyawongkul, *supra* note 234 at 3.
264 *Data Protection Act*, supra note 3, s 9.
265 *Ibid*, s 8(2).
266 *Ibid*, s 8(3).
267 *Ibid*, s 8(4).
268 *Ibid*, s 16.
269 *Ibid*, s 43.
270 *Ibid*, s 48.
271 *Ibid*, s 71.

Rules and Regulations.[272] The jurisprudence of Thailand is more complex as it is essentially a civil law jurisdiction. Judicial precedents of decisions of the Supreme Court of Justice 'have significant influence' but are not binding on either the Supreme Court or the lower courts. [273] A further complication in the case of Thailand is that decisions are often brief and courts only "maintain basic records of previous cases on file".[274]

All three have robust legislation to prosecute computer-related cybercrime including obtaining data with dishonest intent. The Australian legislation is extensive with a significant focus on the privacy of information relating to consumer credit reporting and the penalties that apply for non-compliance. The legislation of the other two jurisdictions is more succinct.

V. Conclusion

The personal data privacy legislation of the three jurisdictions is robust and are considered to have components that cover the 13 Australian Privacy Principles, either explicitly or implied.

The legislation can be summarised in short:

- The Australian *Privacy Act 1988* (as amended), whilst very comprehensive is also extremely complex and requires an understanding of disparate but overlapping legislation, both federal and state, ranging from the *Fair Work Act* 2009 to the *Assistance and Access) Act* 2018 or the New South Wales *Privacy and Personal Information Protection Act* 1998. The federal *Privacy Act* has to provide the overarching principles, and deal with fine granular issues, such as credit reporting in separate legislation or by regulation;
- The *Data Privacy Act of 2012* of the Philippines has been used effectively and proactively, through taking decisive actions against those violating the privacy of its citizens by both national and international corporations, such as Facebook;
- Thailand's *Personal Data Protection Act 2019* is fairly robust but has a major deficiency in its complex administrative structures and process, which has led to a lack of independence of the data protection authority and the potential for excessive use of exemptions under the *Act*.

These legislative provisions of the three countries can be seen as a starting point for providing citizens with more comprehensive frameworks that meaningfully protect privacy and aspects of data.

---

[272] Mary Thel Mundin, "Philippines - Data Protection Overview", *OneTrust DataGuidance* (blog), online: Data Guidance <https://www.dataguidance.com/notes/philippines-data-protection-overview-0> at para 1.3.

[273] Joe Leeds & Chaninant Leeds, "Update: Introduction to the Legal System and Legal Research of the Kingdom of Thailand" (New York: Hauser Law, 2020) (GlobaLex), online: GlobaLex <http://www.nyulawglobal.org/globalex/Thailand1.html> at s 3.2.

[274] Nandana Indananda, Suebsiri Taweepon & Alec Wheatley, "Copyright Litigation in Thailand: Overview" (Thailand, Tilleke & Gibbins, 2017) (Thompson Reuters Practical Law), online: Thompson Reuters Practical Law <https://uk.practicallaw.thomsonreuters.com/w-011-3581?transitionType=Default&contextData=(sc.Default)&firstPage=true> at para 39.