PERSONAL DATA PROTECTION DIGEST

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

PERSONAL DATA PROTECTION DIGEST

Editor

Yeong Zee Kin

Deputy Editors

Robin Teo

Lee Ti-Ting

Amogh Chakravarti

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

2023

CITATION
This volume may be cited as:
[2022] PDP Digest

DISCLAIMER
Views expressed by the article contributors are not necessarily those of the Personal Data Protection Commission ("PDPC"), the Editors nor the Publisher (Academy Publishing). Whilst every effort has been made to ensure that the information contained in this work is correct, the contributors, PDPC and the Publisher disclaim all liability and responsibility for any error or omission in this publication, and in respect of anything, or the consequences of anything, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication.

COPYRIGHT
© 2023 Personal Data Protection Commission

Published by Academy Publishing

Academy Publishing is a division of the Singapore Academy of Law ("SAL").

SAL is the promotion and development agency for Singapore's legal industry. Its vision is to make Singapore the legal hub of Asia. It aims to drive legal excellence through developing thought leadership, world-class infrastructure and legal solutions. It does this by building up the intellectual capital of the legal profession by enhancing legal knowledge, raising the international profile of Singapore law, promoting Singapore as a centre for dispute resolution and improving the efficiency of legal practice through the use of technology. More information can be found at www.sal.org.sg.

All rights reserved. No part of this publication may be reproduced, stored in any retrieval system, or transmitted, in any form or by any means, whether electronic or mechanical, including photocopying and recording, without the written permission of the copyright holder. All enquiries seeking such permission should be addressed to:

Publicity & Engagement
Personal Data Protection Commission
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438
E-mail: info@pdpc.gov.sg
www.pdpc.gov.sg



MCI (P) 048/04/2023

FOREWORD

BY THE FORMER PERSONAL DATA PROTECTION DEPUTY COMMISSIONER

> This therefore is an exciting area of law. What makes data protection law especially significant for Singapore and for our legal sector in particular is the opportunity it presents to forge a regime that is suited to our local context thus helping to ensure the competitiveness of our economy.[1]

When we started the *Personal Data Protection Digest* ("Digest") in 2017, we modelled it after the *Malayan Law Journal*. It collected in a single volume the cases that the Personal Data Protection Commission ("PDPC") issued, as well as articles contributed by data protection practitioners that delved into topics of interest. The objective was two-fold. First, to provide a convenient compilation of PDPC decisions – including those decisions where we found that there was no breach of the Personal Data Protection Act ("PDPA") – so that the keen student could better understand how the PDPA is interpreted and applied. Second, we wanted to provide a soapbox for data protection practitioners to share their research and to articulate their views. We hoped that these conversations would deepen the scholarship in this growing area of law and practice. It was our fervent hope that, through exchanges of ideas and views, the PDPC and the community of data protection practitioners could collaboratively shape the development of data protection law and deepen our collective expertise.

Over the course of the following years, our cases grew to become more complex and, consequently, our decisions became lengthier. The list of contributors who volunteered articles grew in tandem with the level of sophistication – not to mention length – of their articles. We made the decision last year that the Digest had outgrown its format, and that it ought to become a journal. We made sure that there were a few contributions that summarised and highlighted major developments emerging from PDPC decisions for the year, while reserving ample space for data protection practitioners to continue advancing the discussions on topics of interest to

1 The Honourable the Chief Justice Sundaresh Menon, Foreword to [2017] PDP Digest.

the community. The Digest that you hold in your hands follows this new trajectory.

In preparing for this preface, I looked through the earlier volumes. The Chief Justice articulated the objective of the Digest in his foreword to our inaugural edition. It was – and remains – our ambition to develop a data protection regime that is suited to our context. While the data protection principles that we have adopted adhere to global standards, their interpretation and application can and should be influenced by our *terroir*. A perusal of the articles over the past volumes shows that our authors are current and up to date with global developments, but the views expressed are independent, well-reasoned and eloquently articulated. They disclose the level of maturity and erudition of our community of data protection practitioners. We do not accept what others say, but critically review and provide independent commentary. I felt a swell of pride when I was told by a veteran data protection practitioner and former regulator with close to three decades' experience that the standard of the commentary in last year's Digest was impressive. This is a remarkable achievement by our community of practitioners in just half a dozen issues of the Digest.

As I pen this valedictory preface, I think that my greatest sense of achievement for this series of Digests lies not in its provision of a forum for the data protection community, but that the community responded so enthusiastically and shared their knowledge so generously. As the world enters a period where cross-border transfers of data come under increasing pressure and where advances in artificial intelligence open up new areas of concern for consumers and data protection authorities, the need for mature and constructive dialogue is all the more necessary if policy makers, regulators and practitioners are to co-create solutions. If our past trajectory provides any indication, it is the assurance that we will be able to forge our way forward collectively and collaboratively, and in a balanced and sensible manner.

Yeong Zee Kin

Deputy Commissioner (2016–2023)

Singapore

CONTENTS

	Page
Foreword by the Former Personal Data Protection Deputy Commissioner, Yeong Zee Kin	iii
China's Personal Information Protection Law and its Extraterritorial Impact on Businesses *Barbara LI*, *Amy YIN* and *Bryan TAN*	1
Consent: Making it Count *LOW Xide*, *HWANG Soon Ae* and *Doug CAMPBELL PITT*	12
Data Privacy in the Advancement of Digital Health Technologies *LEE Soo Chye*, *Cynthia Elizabeth TANG* and *TEO Yi Ting Jacqueline*	24
Data Protection as Part of an Environmental, Social and Governance Framework *Amira Nabila BUDIYANO* and *Jonathan KAO*	33
Developments in Data Privacy Litigation Globally and in Singapore: Addressing the Growing Need for Individuals to Protect Their Personal Data *Lijun CHUI*, *Allen LYE Xin Ren* and *Joseph LIM Weisheng*	47
Employer Liability and the Employee Exemption *Benjamin WONG*	62
India's Digital Personal Data Protection Bill 2022: What Singapore Privacy Practitioners Need to Know *Alexander LUONG* and *Stacey STEELE*	73
No Longer Child's Play: A Comparative Look at Children's Data Laws in Singapore, the United States, Europe and China *Charmian AW*, *Sarah BRUNO*, *Elle TODD* and *Barbara LI*	88
Privacy-Enhancing Technologies (PETs) – Opportunities & Challenges *Lanx GOH* and *Joshua KOW*	129
The Right of Private Action – Did Allowing Emotional Distress Create Real Risk? *Alexander YAP Wei-Ming*, *TAY Yong Seng* and *ANG Ann Liang*	145
Understanding How the PDPA Permits Organisations to Leverage on Personal Data in Achieving Innovation *Steve TAN* and *Victoria TAN*	159

When Data Transfer Borders Tighten: What Can Data Trusts Bring to the Table?
LIM Sui Yin, Jeffrey and *LEE Kai Xuan, Samuel* 169

Year-in-Review: Personal Data Protection Commission's Decisions in 2022
LIM Chong Kin, *Anastasia Su-Anne CHEN* and *Mark YEO* 185

CHINA'S PERSONAL INFORMATION PROTECTION LAW AND ITS EXTRATERRITORIAL IMPACT ON BUSINESSES

Barbara LI[†]
LLB (China University of Law and Political Science), LLM (King's College, University of London; China University of Law and Political Science); CIPP/E;
Solicitor (England and Wales), Qualified in China

Amy YIN[‡]
LLB (Fudan University), LLM (University of California, Berkeley); CIPM, CISP-PIP (Certified Information Security Professional – Personal Information Protection, China);
Qualified in New York, US and China

Bryan TAN[§]
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore), Solicitor (England and Wales)

I. Introduction

1 In the era of big data, data has become a strategic asset for international and Chinese companies. Chinese companies rank amongst the largest technology companies in the world by market capitalisation. The People's Republic of China ("PRC") has the largest internet population in the world, followed closely by India with the rest of the world's countries trailing quite some distance behind. With Chinese tech companies excelling in interactive digital media and artificial intelligence, the collection and use

† Barbara Li is a partner at Reed Smith LLC based in Beijing, sits on the IAPP Women Leading Privacy Advisory Board and also serves as the Vice Chair of the Cybersecurity Sub-Working Group of EU Chamber of Commerce in China. All views expressed are her own.

‡ Amy Yin is a partner at Reed Smith LLP based in Shanghai. All views expressed are her own.

§ Bryan Tan is a partner at Reed Smith LLC based in Singapore. All views expressed are his own.

of data has intensified. Accordingly, the development of PRC data laws has been gathering pace in recent years to keep up with such increased use.

2 This article seeks to understand the development of the PRC data laws and to understand the relationship between privacy and national security and how it impacts organisations within and outside China.

II. China's landmark data protection legislation including rules on cross-border data flows

3 China's comprehensive legal regime for personal data protection is constituted by the adoption of the Cybersecurity Law[1] ("CSL") in 2017, the Data Security Law[2] ("DSL") in 2021 and the Personal Information Protection Law[3] ("PIPL") in 2021, collectively known as the "Three Pillars". Apart from the Three Pillars, China has also enacted a number of regulations, industrial standards and specifications, providing specific guidance on law enforcement and presenting compliance challenges for business organisations.

A. Overview of the Personal Information Protection Law

4 As China's first comprehensive personal data law, the PIPL applies to any collection, use or processing activity of personal information within the territory of China, regardless of whether the data handler (*ie*, equivalent of data controller under the European Union's General Data Protection Regulation[4] ("GDPR")) is an entity incorporated in China or whether the data subject is a Chinese citizen or a foreigner located in China. Similar to the GDPR, the PIPL applies to foreign entities outside China, if foreign entities collect personal information from China for the purpose of selling

1 Cybersecurity Law of the People's Republic of China (effective 1 June 2017).

2 Data Security Law of the People's Republic of China (effective 1 September 2021).

3 Personal Information Protection Law of the People's Republic of China (effective 1 November 2021).

4 Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

products or services to customers based in China or for assessing or analysing behaviours of individuals located in China.

5 The PIPL lays down the legal principles of legality, appropriateness, necessity and creditworthiness. Companies can only collect, use or process personal information for specific and reasonable purposes which are directly related to the data handling activities. The principles of openness and transparency should also be followed, where the data collector is required to make public the personal data processing rules, describing the purpose, scope and method for data collection and processing.

6 The PIPL provides for the following legal grounds for collection and processing of personal information:

(a) consent by the data subject;

(b) necessity for the conclusion or performance of a contract, or necessity for carrying out HR management under an employment policy or collective contracts;

(c) necessity for performing statutory duties or obligations;

(d) necessity for responding to a public health emergency, or for protecting the life, health or property safety of a natural person in case of emergencies;

(e) for news reporting or public interest purposes;

(f) where personal information has been disclosed by an individual or otherwise legally disclosed; and

(g) other circumstances as stipulated by Chinese laws or administrative regulations.[5]

7 Please note that legitimate interest, which is one of the most commonly used legal bases under the GDPR, is not recognised under the PIPL. It is therefore important for multinational corporations ("MNCs") to review what legal basis has been adopted for collecting and processing personal information in the Chinese market to ensure addressing the local legal nuances.

8 The PIPL grants a wide range of rights to data subjects, including the right of access, accuracy and deletion. It is noted that similar to the GDPR, the PIPL recognises the right of portability, which allows a data subject to

5 Personal Information Protection Law of the People's Republic of China (effective 1 November 2021) Art 13.

request the current data controller to transfer his/her personal information to another data controller. This appears to be in line with the emerging international practice.

B. Cross-border data transfer

9 The Three Pillars provide specific requirements for data localisation, which include the requirement that personal data and important data collected or generated by critical information infrastructure operators ("CIIOs") during their operation in China should be stored within the territory of China. Such data can only be transferred out of China if the cross-border data transfer is conducted based on business necessity and has passed the security assessment (as detailed below).

10 The cross-border data transfer has been the focus of data compliance in China recently. Since June 2022, the Cyberspace Administration of China ("CAC") and other Chinese data and cyber regulators have issued a series of regulations, rules and specifications to shed more light on how to implement the cross-border data transfer in practice. The current available mechanisms for transferring data out of China include CAC-led security assessment, Chinese standard contractual clauses ("SCCs") and security certification. The relevant regulations are set forth below:

(a) The CAC released the Security Assessment Measures of Cross-Border Data Transfer[6] on 7 July 2022 ("Security Assessment Measures") and the Guidelines on Application for Security Assessment of Cross-Border Data Transfers (1st Edition)[7] on 31 August 2022 ("Security Assessment Guidelines"), both of which came into effect on 1 September 2022.

(b) Further to Version 1 of the Security Certification Specifications for Handling Cross-Border Transfer of Personal Information issued on 24 June 2022, Version 2 of the Cross-Border Certification Guidelines was promulgated by China's National Information

6 Security Assessment Measures for Outbound Data Transfers of China (effective 1 September 2022).

7 Guide to Applications for Security Assessment of Outbound Data Transfers (First Edition) (effective 31 August 2022).

Security Standardisation Technical Committee on 16 December 2022, with immediate effect.

(c) The CAC promulgated the Regulations of Standard Contracts for Cross-Border Transfer of Personal Information on 22 February 2023, which will enter into force on 1 June 2023. The Regulations provide a grace period of six months for companies to take necessary compliance actions. The template of Chinese SCCs attached in the Regulations consists of a main body of key clauses plus an appendix of supplementary clauses.

C. Cyberspace Administration of China-led security assessment

11 According to the Security Assessment Measures, the security assessment is compulsory in any of the following scenarios:

(a) cross-border transfers of important data;

(b) cross-border transfers of personal data by CIIOs;

(c) cross-border transfers by data exporter processing the personal data of one million or more individuals;

(d) any transfer (in aggregate) of the personal data of more than 100,000 individuals or the sensitive personal data of more than 10,000 individuals that has occurred since 1 January of the preceding year; and/or

(e) other situations requiring security assessment in accordance with PRC laws and regulations.[8]

12 It is usual that multinational corporations use shared IT systems or infrastructures for global business operation. Remote access of Chinese-stored data by entities outside China by way of review, download or retrieval is deemed as cross-border data transfer, which would be subject to the mandatory security assessment if any of the above thresholds is met.

13 Under the Security Assessment Measures and the Security Assessment Guidelines, business organisations which previously transferred data outside China but did not conduct the security assessment in compliance the Security Assessment Measures had a grace period of six months for rectifications, which expired on 28 February 2023. If no compliance actions

8 Security Assessment Measures of Cross-Border Data Transfer Art 4.

were taken by 28 February 2023, companies were exposed to significant non-compliance risks.

D. Security certification

14 The security certification mechanism is suitable for business scenarios where the Chinese entities of MNCs transfer Chinese-collected data to their affiliate companies outside China, or where the cross-border data transfer takes place because of the extra-territorial application of the PIPL.

15 For the purpose of certification, the cross-border data transfer agreement, processing rules on the cross-border data transfer and self-assessment on the personal information protection impact must be properly prepared. The business organisation that has successfully passed the certification process may demonstrate the certification logo on cross-border data transfer in its promotional materials.

16 Although security certification is voluntary and not compulsory, Chinese regulators have expressly encouraged companies to utilise the security certification to firm up their data governance and compliance and therefore more Chinese companies are exploring the option of the security certification to satisfy their compliance requirements.

E. Chinese standard contractual clauses

17 The Chinese SCCs regime is expected to have apparent advantages, in particular for inter-company transfers, due to more foreseeability of contract terms and time/cost efficiency. Though the parties are not allowed to make changes to the standard SCC terms, they can add supplementary terms without conflicting with the standard terms in the appendix of the agreement. Please note that the data exporter is required to prepare an impact assessment report and file the report together with the executed version of the SCC-based data transfer agreement with the provincial CAC within ten working days of effectiveness. The coming into force of the Chinese SCC-based cross-border data transfer agreement is not conditional upon filing with the CAC authorities.

18 The terms and conditions of the Chinese SCCs share certain similarities with the GDPR SCCs in terms of the obligations of the transferor, the responsibilities of the foreign data recipient and the rights of

the data subjects. However, the Chinese SCCs maintain unique Chinese features. For example, Chinese SCCs only have one universal template, deeming all the data exporters as controllers, while the GDPR SCCs cover four different models of C–C, C–P, P–P and P–C. Besides, the Chinese SCCs impose stricter requirements on onward data transfer than the GDPR SCCs. Moreover, the GDPR SCCs allow more flexibility to choose the governing law, while the governing law of Chinese SCCs must be Chinese law and the dispute resolution bodies are limited to a court in China or arbitration committee in China or other member states of the 1958 New York Convention.[9]

F. Choice of mechanism

19 The above three mechanisms are a significant part of the current cross-border data transfer regime in China. Regardless of which mechanism applies, the self-assessment must be performed and documented in an appropriate manner and available for compliance inspection by authorities. The business organisations are advised to choose the most appropriate cross-border data transfer mechanism based on comprehensive considerations from business and legal perspectives respectively. It is important to note that the security assessment is mandatory if any of the required scenarios is met, in which case security certification and Chinese SCCs mechanisms are not acceptable options.

20 It is also worth noting that, as expressly specified under Chinese data laws, data handlers are not allowed to provide any Chinese-stored personal information to a foreign judicial or law enforcement body, without prior approval by competent Chinese authorities. This would require the governmental review and approval process by CAC and/or China's Ministry of Justice, on a case-by-case basis.

III. The correlation between privacy and national security

21 In order to better understand the Three Pillars, an understanding of the issues of national security and privacy from the lens of the Chinese would be instructive. National security for the world's most populous

9 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958).

nation and a rising superpower is complex and multi-faceted, with implications for politics, geopolitics and the economy, and on which the Chinese government has clearly placed a high priority.

A. Analysis of typical scenarios where privacy protection and national security may be correlated

(1) Foreign investigations and litigation

22 Cross-border transfer of personal information may present issues of national security and the PIPL proscribes special circumstances involving other countries. Specifically, the DSL and Arts 41 and 42 of the PIPL stipulate that: (a) without the prior approval of the competent authority of China, a personal information processor shall not provide personal information stored within the territory of China to any foreign judicial or law enforcement authority; and (b) where an overseas organisation or individual engages in personal information processing activities that compromise national security or public interests of China, the national cyberspace administration may include such organisations and individuals in the list of restricted or prohibited personal information provision. Therefore, companies incorporated in China or Chinese subsidiaries of multinational companies, upon the request for transferring personal information from China overseas for the purposes of participating in an offshore investigation or litigation, should be cautious in relying on any privacy shields available under the laws of other jurisdictions.

(2) Large-scale sensitive personal information of non-classified personnel may be relevant to national security

23 A typical scenario is that if large scale personal biometric identification, healthcare or genetic information is leaked, it could have a significant adverse impact on national security in the event that such large quantities of sensitive personal information were to be collected and used to develop biochemical viruses that target specific human races or genes of Chinese citizens.

(3) Sensitive personal information or personal information of classified personnel working in classified positions is directly related to national security

24 For example, an outdoor sports app which involves the collection of personal GPS locations, specific identity and personal whereabouts, assuming that this app records, collects and analyses the running or traveling routes of certain groups of military personnel, may lead to the disclosure of classified information such as secret national military bases and thus seriously endanger national security.

B. The key privacy protection laws and their extra-territorial effects in China

25 The three fundamental privacy protection laws, CSL, DSL and PIPL, jointly establish the overarching regime governing privacy and data protection for China with different focuses.

26 As China's first law in the cybersecurity field, governing the construction, operation, maintenance and use of internet in China, the CSL contains personal information protection requirements and establishes the framework for critical information infrastructure ("CII") protection and a multi-level protection scheme for cybersecurity. Article 75 of the CSL provides a legal basis for extra-territorial effect in prescribing that where any overseas institution, organisation or individual attacks, intrudes into, disturbs, destroys or otherwise damages CII of China, causing any serious consequence, the violator shall be liable; and the public security authority may decide to freeze the property of or take any other necessary sanction measure against the violators.

27 The DSL was enacted as the fundamental law for data security and personal information protection with a focus on the protection of broadly defined "data security" from a national security perspective. It formally introduces policies including, but not limited to, data classification, data risk controls, data security reviews and export controls. It is worth mentioning that the DSL stipulates the extra-territorial effect in Art 2. Those that conduct data processing activities outside the territory of China that harm national security, public interests or lawful rights and interests of citizens and organisations in China shall be held legally liable in accordance with the DSL. This provision significantly refines national security and data sovereignty in China. The DSL emphasised the localisation requirements

for CII operators, requiring that CII operators store the critical data collected and generated by them within China and shall not provide critical data abroad. Furthermore, the DSL provides for a data classification protection system which is classified in accordance with the importance of specific types of data to China's national economy, national security, public interest and society, as well as the degree of harm that would result from a security incident. More important critical data relating to, or that could affect, national security will be subject to stricter management and protection requirements, such as China's national security review or export control.

28 The PIPL focuses on the protection of personal information and privacy in China, which bears similarities to the GDPR. The PIPL establishes the mechanism of personal information protection in China and introduces several important concepts, such as personal information, sensitive personal information and processing. The PIPL stipulates principles of personal information processing, consent and non-consent grounds for processing, cross-border transfer mechanisms and rights of data subjects. As a general rule under the PIPL, personal information must be stored within China. Where a personal data processor needs to provide personal data to a party outside of China (including giving access to anyone based outside of China) for business reasons, it must satisfy at least one of the following conditions: passing a security assessment, obtaining personal data protection certification or concluding a model contract with the overseas recipient. The PIPL also provides that principles of lawfulness, necessity (purpose limitation, data minimisation and storage limitation), fairness, transparency, accuracy and accountability are all duly considered and met to achieve compliance. Article 3 of the PIPL stipulates the extra-territorial effect, which applies to the processing, outside the territory of China, of the personal information of natural persons located within China, if the information is processed for the purpose of providing products or services to natural persons within China, to analyse or assess the conduct of natural persons within China or under any other situation provided for by laws or regulations.

C. Enforcement and impact on businesses outside China

29 Put together, these requirements may create challenges for overseas businesses, particularly those that operate across multiple jurisdictions and

are already subject to different data protection laws and regulations. It may also lead to increased compliance costs and regulatory burdens for businesses that operate in China or process data related to Chinese citizens or entities. Furthermore, the law gives Chinese authorities broad powers to investigate and enforce data security violations, including the ability to seize equipment and assets, impose fines and penalties, and revoke business licenses. Overall, the Three Pillars are likely to have a significant impact on overseas businesses that operate in China or process data related to Chinese citizens or entities. It underscores the Chinese government's commitment to data security and national sovereignty, but may also create compliance challenges and regulatory risks for businesses operating in the country.

CONSENT: MAKING IT COUNT*

LOW Xide†
MA (Oxon), BA (Jurisprudence) (University of Oxford)

HWANG Soon Ae‡
LLB (Honours) (National University of Singapore)

Doug CAMPBELL PITT§
B.Bus.Sci (Hons), LLB (University of Cape Town)

I. Introduction

1 It is trite, by now, to say that personal data has value. However, the value that may be ascribed to personal data-sets is difficult to determine and is contingent on multiple factors, including completeness, consistency and accuracy of the data; market forces as determined by the exclusivity of the data-set, as well as relative bargaining power between the data provider and data consumer; and, perhaps most importantly, the purpose(s) and function(s) for which that data is lawfully permitted to be used.[1]

2 Complete, consistent and accurate data that cannot be used for any purpose, or can only be used in a highly restricted manner and/or for limited purposes, is of little value to organisations that have expended significant resources to collect and store that data.

3 This has led to a fundamental tension between many organisations and the customers they serve. Organisations are often incentivised to collect data with the widest permissible use-cases to create new insights and functionalities. By contrast, many customers would prefer to allow their

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Senior Counsel, Visa Worldwide Pte Limited.

‡ Senior Associate Counsel, Visa Worldwide Pte Limited.

§ Senior Managing Counsel, Visa Worldwide Pte Limited.

1 Infocomm and Media Development Authority and Personal Data Protection Commission, *Guide to Data Valuation for Data Sharing* (2019).

data to be used only by organisations that they trust and, then, only as necessary to enjoy the specific service(s) being provided.[2]

4 While regulators across jurisdictions have dealt with this tension differently depending on their priorities, one of the key gateways that most regulators agree on as a lawful basis for using personal data is with the consent of the data subject. However, consent has many faces and what may amount to valid consent in some jurisdictions may not be valid in others[3] – "yes" might not mean "yes" for everything, everywhere and all at once.[4]

5 This article examines, from a practical perspective, the means by which organisations may validly obtain and rely on customer consent as a basis for processing personal data. Accordingly, we first look at common issues that arise in practice when seeking to rely on the consent gateway with reference to recent decisions by privacy regulators. Next, we look at other valid bases for processing personal data that, from an organisational perspective, may go some way towards mitigating some of these issues. Finally, we set out practical examples as to how organisations can make the process of procuring customer consent for processing personal data effective, transparent and fit-for-purpose.

---

2 See Venky Anant *et al*, "The consumer-data opportunity and the privacy imperative" *McKinsey & Company* (27 April 2020) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> (accessed 17 May 2023).

3 For instance, while s 15 of Singapore's Personal Data Protection Act 2012 (2020 Rev Ed) ("PDPA") permits data processing on the basis of deemed consent, there is no equivalent under the European Union General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council 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) ("GDPR") which stipulates under Art 4 that consent must be express, unambiguous, explicit and freely given.

4 *Everything Everywhere All at Once* is a 2022 absurdist comedy-drama film written and directed by Daniel Kwan and Daniel Scheinert, starring Michelle Yeoh and Ke Huy Quan, and is (in the authors' opinion) a deserved winner of the Academy Award for Best Picture.

II. Common issues in relying on consent as a basis for data processing

6 The standard means by which organisations seek to obtain consent for the collection and use of personal data is through online privacy policies or notices which customers are asked to agree to. These documents are often lengthy, technical, and ultimately seek to grant broad data usage rights to organisations. However, despite the intention for these documents to be as comprehensive as possible, there exist doubts as to whether many of these policies and notices would stand up under real scrutiny from regulators.

7 Common issues that arise include: (a) the scope of data protection clause(s) not being fit-for-purpose; (b) flaws in the design of the online interface and consent procurement process; (c) failure to account for multiple data collection gateways; and (d) obfuscated data use cases. To illustrate how these issues can arise in practice, we look at several recent decisions issued by various data regulators.

A. Scope of data protection policies

8 In *Re Spring College International Pte Ltd*[5] ("*Spring*"), Singapore's Personal Data Protection Commission ("PDPC") found that Spring College had failed to notify and obtain consent from parents of students before disclosing the students' personal data online for marketing purposes. In making its decision, the PDPC rejected Spring College's argument that it could rely on a data protection clause which notified customers that one of the allowed uses for personal data collected was the "compilation and analysis of statistics for marketing purposes". The PDPC found that the clause was not fit-for-purpose, distinguishing between using data for statistical analysis to finetune marketing strategy (which was covered) and using data directly for marketing purposes (which was not covered).[6]

9 Similarly, another clause permitting Spring College to use images of students for *publicity* purposes was deemed insufficient as this was limited to using data to *publicise* organisational activities as opposed to using data to *market* the organisation.[7]

---

5 [2019] PDP Digest 230.

6 *Re Spring College International Pte Ltd* [2019] PDP Digest 230 at [18]–[19].

7 *Re Spring College International Pte Ltd* [2019] PDP Digest 230 at [21].

10 Notably, as part of its remediation measures, Spring College had informed the PDPC that it had created a Marketing Consent and Release Form which requested for consent to use personal data for "any purpose that the school deems appropriate, including promotional or advertising efforts". In determining that the scope of the new clause was too broad to be relied upon as a basis for obtaining valid consent, the PDPC emphasised the need for such clauses to be clear and specific in describing the purposes for which the personal data will be used.[8]

11 The PDPC's Advisory Guidelines on Key Concepts in the PDPA ("Advisory Guidelines") also provide detailed guidance on what constitutes valid consent and notification.[9] Aside from outlining legal requirements under the PDPA,[10] the Advisory Guidelines also touch on best practices, such as indicating to customers which personal data fields are compulsory and which are optional,[11] ensuring that data policies can be viewed before consent is provided[12] and drafting notes on data policies that are easy to understand, clear and easily accessible.[13] There are also specific guidelines for where organisations wish to use customers' personal data for marketing purposes.[14]

---

8 *Re Spring College International Pte Ltd* [2019] PDP Digest 230 at [24]–[28].

9 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at ss 12 and 14.

10 For instance, see Personal Data Protection Act 2012 (2020 Rev Ed) ss 14(2) and 14(3), which provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his/her personal data beyond what is reasonable to provide the product or service.

11 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.10.

12 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 14.13.

13 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 14.17 and 14.18.

14 See Personal Data Protection Commission, *Advisory Guidelines on Requiring Consent for Marketing Purposes* (8 May 2015).

B. User interface and data collection process

12 In the UK Information Commissioner's Office's ("ICO") decision regarding We Buy Any Car Limited[15] ("WBAC"), the ICO imposed a £200,000 fine on WBAC in light of WBAC sending 191.4 million marketing e-mails and 3.6 million marketing SMS messages to individuals without satisfying consent and/or "soft opt-in" requirements under the European Union General Data Protection Regulation ("GDPR") and associated regulations.[16]

13 In deciding that WBAC failed to obtain customer consent, the ICO focused on WBAC's failure to provide a means for customers to opt-out of marketing messages at the point where customers were initially inputting their details. Instead, it was only upon receipt of the subsequent e-mail from WBAC that customers were given the opportunity to opt-out.[17] The flawed design of this process meant that there was a temporal gap whereby customers could not provide or refuse to provide consent to their personal data being used.[18]

14 Similar issues arose in Finance Giant Ltd[19] ("FGL") where the ICO imposed a £60,000 fine on FGL in light of FGL sending more than 500,000 unsolicited direct marketing messages to subscribers. In determining that FGL had failed to validly obtain customer consent, the ICO focused on FGL's failure to provide separate opt-in and opt-out boxes to enable applicants to either consent or withdraw consent specifically in relation to marketing messages. The ICO also criticised FGL's failure to draw its customers' attention to the fact that it would be sending them

---

15 See Information Commissioner's Office (UK), *Penalty Notice: We Buy Any Car Limited* (15 September 2021).

16 See *inter alia* Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Art 4, and Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK) ("PECR") reg 22.

17 Information Commissioner's Office (UK), *Penalty Notice: We Buy Any Car Limited* (15 September 2021) at [27].

18 Information Commissioner's Office (UK), *Penalty Notice: We Buy Any Car Limited* (15 September 2021) at [28].

19 See Information Commissioner's Office (UK), *Penalty Notice: Finance Giant Ltd* (13 April 2022).

direct marketing messages (which the customers would not have been aware of unless they separately consulted the terms of FGL's privacy policy).[20]

15 The PDPC has also provided practical guidance to application and web developers on this issue over and above what has been set out in the Advisory Guidelines. In *Re Actxa Pte Ltd*[21] ("*Actxa*") (elaborated upon in more detail below), the PDPC endorsed guidance issued by authorities in other jurisdictions emphasising that organisations and developers should ensure that (a) customers are notified in a manner that is "clear, apparent and understandable";[22] (b) privacy policies are easily readable and prominent;[23] and (c) consideration is given as to whether and how to obtain specific consent for expanded use-cases dynamically.[24]

C. Multiple data collection gateways

16 In *Actxa*, the PDPC imposed a financial penalty on Actxa for failing to obtain customer consent to collect and use personal data collected through Actxa's Internet of Things ("IoT") devices (fitness trackers and smart weighing devices). While Actxa had in place a privacy policy for its mobile application, the privacy policy only referred to data collected through the mobile application and *not* data collected through any of Actxa's IoT devices. Accordingly, Actxa could not be said to have obtained valid consent for processing personal data collected through its IoT devices.

17 In making its decision, the PDPC rejected arguments from Actxa that the consent received from customers in respect of data collected from its mobile application could be extended. The PDPC was influenced by the amount and type collected by the IoT devices, which had "much higher" volume, variety and velocity of generation than the personal data collected through the mobile application[25] and accordingly would require specific and clear notification and consent, separate from the consent given by customers in respect of the mobile application.

---

20 Information Commissioner's Office (UK), *Penalty Notice: Finance Giant Ltd* (13 April 2022) at [33].

21 [2019] PDP Digest 156.

22 *Re Actxa Pte Ltd* [2019] PDP Digest 156 at [27]–[28].

23 *Re Actxa Pte Ltd* [2019] PDP Digest 156 at [37].

24 *Re Actxa Pte Ltd* [2019] PDP Digest 156 at [38].

25 *Re Actxa Pte Ltd* [2019] PDP Digest 156 at [24]–[25].

D. Obfuscated data use-cases

18 The South Korean Personal Information Protection Commission ("PIPC") announced in a press release dated 14 September 2022[26] that it had imposed an administrative penalty of KRW69.2bn and KRW30.8bn, along with corrective orders, on Google and Meta respectively. The PIPC found that Google and Meta collected and analysed users' third-party behavioural data, by inferring users' interests and using them for targeted advertisements, without either clearly notifying users or obtaining prior consent.

19 Google was found to have "used a consent method that set the default option to "I agree" while hiding the settings page ("More Options")". Similarly, Meta's full data policy was found to have been difficult to find and comprehend at the time of a user's account creation. The PIPC also noted that Google had, by contrast, implemented a step-by-step consent process in Europe for the "collection of behavioural data, targeted ads, and personal information protection, when they sign up for membership".

20 The PIPC decision shows that where additional data use-cases are not clearly outlined during the consent collection process (*eg*, where they may be hidden or grouped together with other use-cases necessary to offer the underlying service), organisations may not be able to rely on that consent as a valid basis of processing.

III. Consent as a business opportunity

21 The cases cited above show that organisations can often, even with the best of intentions, find it challenging to be clear about what personal data is collected or how such personal data may be used in the future.

22 This dilemma affects organisations in many Asia-Pacific jurisdictions, since consent is often relied upon as a valid basis of processing, with a limited number of jurisdictions permitting other bases for processing (such as legitimate interests).[27] In fact, in many jurisdictions, consent remains the

---

26 Personal Information Protection Commission, "Press Release: PIPC Sanctions Google and Meta for Illegally Collecting Personal Information" (14 September 2022) <https://www.pipc.go.kr/eng/user/ltn/new/noticeList.do> (accessed 17 May 2023).

27 Such as Singapore, Philippines, Thailand, Sri Lanka, Indonesia.

primary legal basis for processing.[28] Even in jurisdictions where alternative legal bases have been introduced (such as Singapore), many organisations still choose to rely on consent as the primary basis for processing.

23 To set minimum standards for consent that are transparent, easily understandable and fit-for-purpose, regulators have largely used the "stick" (*cf*, carrot) method by including in the regulations requirements for organisations to at least adhere to a minimum standard of transparency instead of looking for a paper "sign-off" from individuals.

24 However, to the extent organisations view consent only as a regulatory tick-box, this may overlook that customers: (a) are aware that personal data is a valuable asset that they are providing; (b) value clear explanations of why and how their personal data will be used; (c) are increasingly wary of organisations that may be seen to seek to serve their own business purposes only without regard for customer interests; and (d) accordingly, may be distrustful of such organisations which can, in certain cases, lead to customer churn.

25 It is with that in mind that we describe below some suggestions as to how organisations can seek to obtain consent in a manner that is not only effective, but also builds trust with their customers.

IV. Practical guidance on obtaining effective consent

A. Standardised requests

26 Regulators are increasingly offering "carrots" to organisations by collaborating with them to create privacy notices and consent requests that are more easily understandable by consumers. One increasingly common example of this is standardised requests.

27 In the Australian Attorney-General's Department's Privacy Act Review Report 2022 ("Australia Report"), one proposal discussed was whether to "require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a

28 Such as Korea, Hong Kong, China, Malaysia, Japan, India, Myanmar, Vietnam, Cambodia, amongst others.

child".[29] The Australia Report also went on to recommend that the "use of visual and graphical communication methods (including infographics or standardised icons) be encouraged as a method to enhance comprehension, noting that some young people may be less likely to engage with purely written privacy information".[30]

28 Similarly, Art 12(7) of the GDPR states that information provided to data subjects may be "provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing".[31]

29 Having standardised requests for consent in the form of easily digestible infographics and icons, preventing the customer from having to go through pages of legalese to understand the headline points of what they are agreeing to, can be an effective means of ensuring not only that the consent obtained can be relied on, but also convey clearly to customers that organisations have their interests in mind and are respectful of the customers' decision to entrust that organisation with their personal data.

B. Effective summaries and/or highlights of key information

30 Given the increasing amount of personal data collected, and the purposes for processing becoming more varied, organisations need to ensure that their privacy policies and practices are not only clear but also are formulated in a way that an individual customer can fairly understand.

31 To that end, it is unlikely to be fair to expect individual customers to sift through long privacy policies, and organisations may wish to consider means by which their customers can be fairly put on notice as to what they

---

29 Australian Government Attorney-General's Department, *Privacy Act Review Report 2022* (16 February 2023) Proposal 16.3.

30 The Australia Report cited that the UK Age-Appropriate Design Code and Ireland's Fundamentals for a Child-Oriented Approach to Data Processing also encourage organisations to "use diagrams, cartoons, graphics, video and audio content rather than relying solely on written communications".

31 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Art 12(7).

are agreeing to. In that regard, organisations may wish to consider the following:

(a) having a prominent summary or highlights section, the positioning of which will depend on the precise process of how the organisation seeks to acquire customer consent – for instance, this may form part of the privacy notice itself, or a consent form that incorporates that privacy notice as a separate document;

(b) structuring privacy policies in tabular (or other digestible) form to clearly set out the different types of personal data, purposes for processing, use and disclosure rights;

(c) incorporating direct user-controlled webpages or sections, where the customer can easily determine and control what personal data has been provided for the purposes of a particular service, what personal data has been provided for other purposes and/or what forms of marketing communications have been consented to, *etc*; and

(d) setting out clearly when other bases for processing (*eg*, legitimate interest or business improvement) are being relied upon and in relation to which use-cases and/or what kind of personal data.

C. Granular consent that gives data subjects more control

32 In June 2021, Visa conducted a Consumer Empowerment & Digital Audit Survey in Singapore. In the survey, Visa tested various models of obtaining consent on a mobile user interface, consisting of:

(a) Terms and Conditions ("T&Cs") only (participants were only presented with an "I agree" option, positioned below standard language providing that upon clicking the button, the customer would be agreeing to their personal data being processed pursuant to the terms of a hyperlinked privacy policy);

(b) T&Cs plus (as per the above, save that a short summary of the privacy policy was also included);

(c) Opt-Out (participants were presented with two pre-selected tick-boxes, with one providing consent for the main service, and the other providing consent for receiving marketing offers);

(d) Opt-In (as per the above save that the two tick-boxes were unselected); and

(e) Granular (participants were presented with multiple unselected tick-boxes for the purpose of providing consent to the types of

personal data collected and different uses of that data (*eg*, marketing, analytics, third party sharing and data use periods)).

33 Notably, participants responded that the granular consent model was not more inconvenient than the other models and gave more positive feedback (as compared to the other models) on user control, comfort and as a way to conduct business. Interestingly, the participants also indicated that they are least likely to *not* agree based on a granular consent model. In other words, being upfront about additional data use cases and providing customers with the means to control the use of their personal data may, in some cases, have a positive effect both in terms of obtaining the consent required and in building customer trust for organisations.

34 Another benefit of the granular consent model is the avoidance of consent-fatigue. If the customers clearly understand what they had provided consent to (or rejected) in the past, any incremental changes that may be needed when seeking to offer an additional service or functionality can be made easily and quickly. This may not only speed up the consent collection process, it may also help to build customer trust by not making it incumbent on the customers to re-read lengthy privacy notices to see how they might differ from the previous version they had agreed to.

35 Individuals, organisations and the broader ecosystem can benefit from a cohesive approach that puts individuals at the centre of the consent process. There are guidelines, such as Visa's Consent Management Guidelines,[32] available online to help organisations across industries offer and implement granular consent management experiences – driving towards consistency, transparency and clarity for consumers.

V. Conclusion

36 Despite the increased availability of other bases for data processing, there will inevitably be cases where organisations will still need to be able to rely on the consent gateway when collecting and using the personal data of their customers. This is particularly true where organisations want to be able to use customer data for the purposes of marketing or developing new

32 Visa, "Visa Consent Management Guidelines" <https://globalclient.visa.com/ConsentManagement> (accessed 17 May 2023).

products and services that they believe would benefit and/or be in the interest of customers in the future.

37 In such cases, it is especially important for organisations to carefully and holistically look at their privacy policies or notices, and the precise sequence and means by which these are introduced and notified to their customers, to make sure that the entire process is fair, appropriately calibrated and ultimately fit-for-purpose. It is not enough for organisations to take a "kitchen-sink" approach which can often be counter-productive rather than helpful.

38 For organisations, reviewing and re-working the consent process can be used not only to strengthen statutory compliance but also as an important mechanism to build customer trust by providing a positive and differentiated user experience.

DATA PRIVACY IN THE ADVANCEMENT OF DIGITAL HEALTH TECHNOLOGIES*

LEE Soo Chye
LLB (Hons) (NUS), MTax (SUSS);
Advocate and Solicitor, Singapore

Cynthia Elizabeth TANG
LLB (Hons) (NUS);
Advocate and Solicitor, Singapore

TEO Yi Ting Jacqueline
LLB (Hons) (NUS);
Advocate and Solicitor, Singapore

I. Introduction

1 Digital health is, broadly speaking, the use of digital technologies for healthcare purposes. The Health Sciences Authority of Singapore refers to digital health as the "usage of connected devices, wearables, software including mobile applications and artificial intelligence to address various health needs via information and communication technologies".[1] Terms such as "mHealth" (short for mobile heath), telehealth and telemedicine, are commonly associated with digital health.

2 The digital healthcare industry is surging in growth worldwide. The global digital health market was over US$195bn in 2021 and is poised to depict a compounded annual growth rate of more than 16% from 2022 to 2030.[2] The growth is driven by the developments in and deployment of IT technologies and the corresponding increase in usage of such technologies

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the legal views or policy positions of their employers. All errors remain the authors' own.

1 Health Sciences Authority, "Digital Health" (7 March 2022) <https://www.hsa.gov.sg/medical-devices/digital-health> (accessed 18 May 2023).

2 Rupali Swain & Sumant Ugalmugle, "Digital Health Market Size & Share: Trends Report, 2022–2030" *Global Market Insights Inc.* (September 2022).

by consumers, which have accelerated rapidly as a result of the COVID-19 pandemic. According to the Asia-Pacific Front Line of Healthcare Report 2022 by Bain & Company, consumers are increasingly more proactive about managing their health and well-being which is reflected in the rising sales of fitness wearables and downloads of health and fitness mobile applications.[3]

3 This burgeoning industry has opened the healthcare space to more players such as technology companies, mobile application developers and IT solution developers, beyond the traditional players such as pharmaceutical companies and hospitals. The escalating development and use of artificial intelligence will also change the landscape of healthcare delivery and further boost the growth of the digital healthcare industry.[4]

II. Resultant creation of data privacy concerns

4 Patient confidentiality is the cornerstone of the healthcare industry. Traditionally, patients share personal information with doctors and traditional healthcare service providers to receive appropriate medical care. Laws have developed such that these traditional players are subject to higher standards of care for the medical information that they come to possess, for example the duty to maintain medical and patient confidentiality is imposed on medical professionals.

5 While there are numerous benefits in the advancement of digital health, the introduction of digital health into the healthcare landscape and the influx of non-traditional players from the digital health industry generates persistent concerns that revolve around the collection, use and disclosure of data relating to the health of individuals (broadly referred to as "health data") and the adequacy of security safeguards in place to protect such health data by these non-traditional players. These concerns threaten to erode patient confidentiality. The mounting ease of collection of health data is the main underlying cause for such concerns.

---

3 Vikram Kapur *et al*, "Asia-Pacific Front Line of Healthcare Report 2022" *Bain & Company* (14 January 2022).

4 Ministry of Health, *Artificial Intelligence in Healthcare Guidelines* (October 2021).

6 Health data that can be collected by digital health products now goes beyond traditional medical records and are far more voluminous. Wearable devices, such as the Fitbit, Apple Watch and Amazon Halo Band, were produced for fitness and general tracking and have sensors to monitor movement, heart rates, blood oxygen levels, temperatures and sleep health. mHealth applications which allow the tracking of health data such as step and calorie counters, and the checking or tracking of health conditions or symptoms or prescriptions, require its users to permit the collection of health data by the application either through trackers in linked devices or through disclosure by its users. These digital health products (in particular, mHealth applications) that can be made available globally via the Internet have also vastly expanded the cross-jurisdictional reach of non-traditional players to health data.

7 Additionally, there is intrinsic value in health data and with the advent of data analytics, health data is now even more valuable. This has unfortunately made it vulnerable to becoming commodified. The inconsistency in regulatory enforcement across the globe has also resulted in a consequent lack of accountability on such non-traditional players. A combination of all these factors have made the pool of health data larger, more valuable, which has increased it susceptibility to not only misuse or misappropriation by industry players but also to fraudulent attacks by hackers.

8 Data privacy and security risks accompanying digital health technologies are real and pervasive. In 2020, Glow, Inc. – a technology company that operates a fertility tracking mobile application that stores personal and medical information – was investigated for serious privacy and basic security failures that placed their users' highly sensitive medical information at risk, by failing to adequately safeguard health information and allowing access to users' information without the user's consent.[5] In 2021, Flo Health Inc, another company that operates a fertility tracking mobile application, allegedly shared sensitive health data from millions of

5 State of California Department of Justice, Office of the Attorney-General, "Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information" (17 September 2020) <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93> (accessed 18 May 2023).

users of its Flo Ovulation & Period Tracker app with marketing and analytics firms, including Facebook and Google, without obtaining the users' consent.[6] In a study funded by the Optus-Macquarie University Cyber Security Hub to investigate the associated risks in mHealth applications, it was found that data collection in mHealth apps was far from transparent and secure and often exceeded what is publicly disclosed by developers of the application.[7]

III. Singapore's regulatory landscape

A. General protection under the Personal Data Protection Act 2012

9 The main legislation governing data privacy and protection is the Personal Data Protection Act 2012[8] ("PDPA"). The PDPA requires organisations to notify an individual of the purposes for the collection, use and disclosure of personal data.[9] In situations where an individual voluntarily provides his/her personal data to an organisation for a purpose, and it is reasonable that he/she would voluntarily provide the data, the individual may be deemed to consent to the collection, use or disclosure of the personal data.[10] The PDPA generally prohibits organisations from collecting, using or disclosing personal data of individuals for purposes other than as notified. The PDPA also imposes a general obligation that an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or

6 Stephanie T Nguyen, "FTC Finalizes Order with Flo Health, a Fertility-Tracking App That Shared Sensitive Health Data with Facebook, Google, and Others," *Federal Trade Commission* (22 June 2021) <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google> (accessed 18 May 2023).

7 Gioacchino Tangari *et al*, "Mobile Health and Privacy: Cross Sectional Study"(2021) 373 BMJ at 1248.

8 2020 Rev Ed.

9 Personal Data Protection Act 2012 (2020 Rev Ed).

10 Personal Data Protection Act 2012 (2020 Rev Ed) s 15(1).

disposal or similar risks, as well as the loss of any storage medium or device on which personal data is stored.[11]

10 The Personal Data Protection Commission ("PDPC") issued Advisory Guidelines for the Healthcare Sector in September 2014, which were subsequently revised in March 2017.[12] This set of advisory guidelines seeks to outline the application of the provisions in the PDPA to scenarios faced mainly by traditional players in the healthcare sector.

11 In 2021, amendments were made to the PDPA to provide that organisations are required to notify of data breaches which are either of significant scale or may cause significant harm to an affected individual.[13] The PDPA provides that there are certain prescribed classes of data which would invoke the data breach notification requirements on the basis that it would result in or is likely to result in significant harm to an affected individual – such classes of data include medical data relating to the assessment, diagnosis, treatment, prevention or alleviation of specified medical conditions including sexually transmitted diseases, HIV infections, schizophrenia or delusional disorder, substance abuse and addiction, provision of treatment relating to contraception or abortion procedures, and organ transplants and donations.[14]

12 The PDPA applies to personal data which includes health data. Unlike the European Union General Data Protection Regulation ("GDPR") which classifies personal data related to the physical or mental health of a natural person as a special category of data (for which the purposes for processing are limited unless consent is obtained and permits the introduction of further conditions and limitations by member countries for the processing of such data),[15] the PDPA generally does not make a

11 Personal Data Protection Act 2012 (2020 Rev Ed) s 24.

12 Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised 28 March 2017).

13 Personal Data Protection Act 2012 (2020 Rev Ed) s 26B.

14 Personal Data Protection (Notification of Data Breaches) Regulations 2021 s 3(1)(a).

15 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 L119/33.

distinction between health data and other types of personal data or specifically impose more stringent obligations on organisations handling health data.

13 Nevertheless, the PDPC has taken the position in several enforcement cases that a higher standard of protection is required for more sensitive personal data, which includes insurance, medical and financial data.[16] The PDPC Advisory Guidelines on Enforcement for Data Protection Provisions[17] also provide that failure to put in adequate safeguards for large volumes of sensitive personal data may be an aggravating factor in calculating the level of financial penalty to be imposed on an organisation.

B. Regulatory oversight for organisations providing healthcare services

14 Private hospitals, clinics and healthcare service providers are subject to strict control and licensing requirements under the Healthcare Services Act 2020[18] ("HCSA"). The HCSA, which was passed on 6 January 2020, is intended to repeal the Private Hospitals and Medical Clinics Act 1980[19] and is to be implemented in three phases from January 2022 to December 2023.

15 The motivation behind the Healthcare Services Bill is the recognition by the regulators that new care models for patients have emerged with healthcare services being increasingly delivered through mobile and online channels, such as telemedicine, which was rapidly adopted during the COVID-19 pandemic. Unlike its predecessor, which licenses healthcare providers based on different types of premises, the HCSA seeks to license providers based on the type of healthcare services provided, which will include telemedicine providers. The updates to the legislation on this front are welcomed as it is intended to permit the development of new and innovative healthcare services.[20]

---

16 *Aviva Ltd* [2018] PDP Digest 245.

17 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of Data Protection Provisions* (revised 1 February 2021).

18 Act 3 of 2020.

19 2020 Rev Ed.

20 Ministry of Health, "About Healthcare Services Act (HCSA)" (25 January 2023) <https://www.moh.gov.sg/hcsa/about-hcsa#:~:text=HCSA%20better%20

(*continued on next page*)

16 Like its predecessor, the HCSA imposes requirements on the licensees to keep and maintain proper medical records, including ensuring that the medical records are kept accurate, complete and up-to-date for the purposes for which they are to be used, implementing adequate safeguards to protect the medical records and periodically monitoring and evaluating such safeguards, maintaining the confidentiality, availability and integrity of the medical records and taking reasonable care in the disposal or destruction of the medical records.[21] It goes further to clarify that such obligations apply to patient health records in the form of an extract or aggregate compilations which may contain patient identifiers and clinical information.

C. Regulatory oversight for "telehealth products" that are regulated as medical devices

17 Certain types of "telehealth" (or digital health) products (including hardware, software and mHealth applications) may, if they are medical devices under the Health Products Act, fall within the purview of the Health Sciences Authority ("HSA").[22]

18 The HSA released a set of guidelines in April 2019 to provide clarity on its regulatory approach towards digital health products.[23] As a general rule, a digital health product that is intended for medical purposes such as investigation, detection, diagnosis, monitoring, treatment or management of any medical condition, disease, anatomy or physiological process, may be regulated.[24] Similar to its approach in relation to other medical devices, the HSA stated that it employs a rule-based approach to classify digital health products into four risk classes based on their nature and intended functions, and then apply the appropriate level of scrutiny and regulatory requirements.[25] Digital health products that are intended to be used only as

---

safeguards%20patient%20safety,continuity%20of%20care%20to%20patients> (accessed 18 May 2023).

21 Private Hospitals and Medical Clinics Act 1980 (2020 Rev Ed) s 12.

22 Health Products Act 2007 (2020 Rev Ed).

23 Health Sciences Authority, *Regulatory Guidelines for Telehealth Products* (April 2019).

24 Health Sciences Authority, *Regulatory Guidelines for Telehealth Products* (April 2019).

25 Health Sciences Authority, *Regulatory Guidelines for Telehealth Products* (April 2019).

a "wellness device" to enable or encourage the user to adopt or maintain a healthy lifestyle or for general wellbeing will not be regulated by the HSA, even if it may be able to perform medical functions or purposes.[26] The HSA requires manufacturers of "wellness devices" to include a clarification statement to clearly inform users that the product is not intended to be used for any medical purposes and that the user should consult a physician if medical advice is required.[27]

19 If a digital health product is a medical device, there may be product registration requirements, licensing requirements for persons dealing with such devices and post-market obligations to be complied with. The HSA also provides pre-market consultation to researchers, developers and manufacturers of digital health medical devices to advise on the regulatory requirements during the development phase.

20 In April 2020, the HSA released a set of guidelines for software medical devices on regulatory requirements in relation to cybersecurity, data integrity and data security. These guidelines also set out additional regulatory considerations where medical devices incorporate artificial intelligence technology.[28] Subsequently, in 2021, in recognition that artificial intelligence is increasingly being used in the healthcare continuum, the Ministry of Health ("MOH"), together with the HSA and the Integrated Health Information Systems, co-developed the MOH Artificial Intelligence in Healthcare Guidelines based on principles adapted from the Model AI Governance Framework prepared by the PDPC with the Monetary Authority of Singapore, to codify good practice and support and guide the safe growth of artificial intelligence in healthcare.[29]

---

26 Health Sciences Authority, *Regulatory Guidelines for Telehealth Products* (April 2019).

27 Health Sciences Authority, *Regulatory Guidelines for Telehealth Products* (April 2019).

28 Health Sciences Authority, *Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach* (Revision 2.0) (April 2022).

29 Ministry of Health, *Artificial Intelligence in Healthcare Guidelines* (October 2021).

IV. Conclusion

21 The regulatory landscape for the digital health industry in Singapore is supported by the interplay of the Personal Data Protection Act, the Healthcare Services Act and the Health Products Act and within the purview of various regulatory authorities such as the PDPC, MOH and the HSA. Singapore's regulatory approach, where the digital health industry is not regulated by a single bespoke legislation but by several different legal regimes, is similar to the approach taken in jurisdictions such as the US, member states in the EU, and the UK.

22 The recent changes to the Healthcare Services Act and the publication of guidelines by the PDPC, HSA and MOH demonstrate that the local regulators are endeavouring to keep abreast of the rapid developments in the ever evolving and dynamic digital health industry and its impact on the healthcare landscape, despite the challenges posed.

23 However, the cross-jurisdictional reach of these new non-traditional players outside of our jurisdiction, particularly in mHealth applications which are easily downloadable regardless of location, inevitably challenges the reach of regulators. Coupled with the inconsistency in regulatory enforcement across the globe, beyond the local regulators' control, these factors perpetuate the lack of accountability for such players. In order to safeguard the local population, perhaps the best way is to equip and educate its people by increasing awareness of such data privacy and security risks.

24 As a regional medical hub, Singapore must continue to keep close watch and be ahead of new players in the progressively changing digital health space, in order to foster and maintain high levels of consumer and practitioner trust by assurance that data security will be taken seriously.

DATA PROTECTION AS PART OF AN ENVIRONMENTAL, SOCIAL AND GOVERNANCE FRAMEWORK*

Amira Nabila BUDIYANO†
LLB (Singapore Management University), Grad Dip (IP and Innovation Management) (Singapore University of Social Sciences);
CIPP/A;
Advocate and Solicitor (Singapore)

Jonathan KAO‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

1 The phrase "Environmental, Social and Governance" ("ESG") appears to be first coined in a report produced for the Asset Management Working Group of the United Nations Environment Protection Finance Initiative and published in October 2005.[1] Consumers and investors have increasingly been using ESG indicators to guide their decision-making, supporting companies and conduct that are sustainable and socially conscious.

2 Customarily, ESG as applied in disclosures and other reporting instruments for an organisation is seen as a segment where organisations discuss their own narrative in other non-financial aspects of the business. It is presented together with other efforts that may not necessarily be profit-making in nature but can reflect well for the organisation's reputation and improve general public perception. Put simply, it makes the organisation more personable. When discussing ESG, different ideas would come to

---

* The views expressed in this article are the authors' personal views and may not be representative of the views of their respective employers.

† Attorney at Kyndryl (Singapore) Pte Ltd.

‡ Counsel, Bird & Bird ATMD LLP, Singapore.

1 Freshfields Bruckhaus Deringer, *A legal framework for the integration of environmental, social and governance issues into institutional investment* (Produced for the Asset Management Working Group of the UNEP Finance Initiative) (October 2005).

mind including corporate social responsibility ("CSR"); environmental awareness and conservation efforts; and workplace inclusion, diversity and balance. There was little structure or consensus on what defines ESG. That is, until more listing bodies started to include the requirement for ESG reporting in listing rules and annual reports, elaborating on some form of standards to adhere to.

3 At the time of writing, there is yet to be a single set of reporting standards for ESG. In 2022, the International Sustainability Standards Board ("ISSB") formally commenced work on developing a baseline for sustainability-related disclosure standards building upon standards by members of the ISSB such as the Global Reporting Initiative ("GRI") and the Sustainability Accounting Standards Board ("SASB"). These standards are expected to give insights into an organisation's resilience through its governance and practices, as well as its exposure to climate-related risks and management of resources. These currently do not include data protection or privacy as an area to be expressly addressed.

4 Nevertheless, the importance of data protection is no longer in doubt with legislation being enacted and revised in all major jurisdictions and ongoing efforts to harmonise obligations across jurisdictions. The collection, processing, storage and sharing of data, personal or otherwise, has been growing exponentially as more services and experiences move online, a trend exacerbated by the COVID-19 pandemic and the push for more "smart" initiatives and proliferation of Internet of Things ("IoT") technologies.

5 So where does data protection or privacy fit into the picture? And is there a more worthy purpose for data protection or privacy to be included within the ESG framework than mere glorification of the organisation? This article seeks to first explore how ESG and personal data protection obligations can intersect. It then explores how data protection or privacy as a standalone component can and should be an integral part within any ESG framework. The authors conclude with several recommendations and proposals on how various bodies can enable this holistic integration. To be clear, this article does not discuss nor makes recommendations as to whether ESG reporting ought to be a mandatory practice in Singapore and much less worldwide. This article is premised on when ESG is indeed reported, to consider inclusion of data protection or privacy items.

II. Intersection with the Environmental, Social and Governance framework

6 Data protection or privacy is not just about compliance with relevant laws and regulations as well as mitigating risks. At its heart across various jurisdictions, it is about recognising the right of individuals to protect their personal data.[2] At the same time, ESG is about accountability to investors, capital market players and consumers about the performance of a company in terms of risks and strategies against certain benchmarking metrics and standards. Therein is the intersection between data protection or privacy and the ESG framework at the very outset: upholding the user or consumer's sovereignty in a capitalistic environment.

A. Environmental

7 The environmental element in ESG broadly focuses on climate-related risks and opportunities. These can include direct and indirect emissions and offsets, resource use and management, pollution and waste, resilience to climate change, risks arising from climate change and opportunities that may arise from climate change.[3]

8 A common theme that perpetuates in data protection obligations or privacy obligations is the need to be clear and precise on the reason for collecting or processing personal data, which is known as "transparency". The principle of frugality in the collection and processing of personal data is also central to privacy or data protection by design. Take not what you do not need, and waste not what you have. Apart from transparency and

2 Under s 3 of the Singapore Personal Data Protection Act 2012 (2020 Rev Ed) ("PDPA"), the purpose of the Act includes the right of individuals to protect their personal data. Whereas under Art 1(2) of the European Union ("EU") General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council 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) ("GDPR"), it is described that the GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3 See MSCI ESG Research LLC, *ESG Ratings Methodology* (November 2022).

data minimisation,[4] another closely related principle of data protection by design is "risk minimisation". In the Singapore context, it has been recommended that good practices in the collection of personal data could include collecting the least sensitive types of personal data when different types of personal data are used to achieve the same purpose. Other good practices would be to consider not collecting metadata or removing them if they are not needed, as well as to provide options for users to input selected personal data instead of automatically obtaining it.[5] In turn, "unnecessary personal data" would not be collected by the organisation resulting in no burden of having to protect them, and thereby the organisation is better able to allocate resources effectively.

9 Data protection by design in the General Data Protection Regulation ("GDPR") context speaks about incorporating appropriate technical and organisational measures within an organisation to implement data protection principles in an effective manner and integrate safeguards into processing.[6] A form of certification mechanism can be used to demonstrate compliance.[7] At present, Europrivacy is the only approved certification scheme. What it does is to enable companies to assess and formally certify their data processing compliance for each process. Europrivacy certificates are to be formally recognised in all European Union Member States and will be taken into account by data protection supervisory authorities in case

4 Under the *Guide to Data Protection by Design for ICT Systems* (2019), jointly issued by the Singapore Personal Data Protection Commission ("PDPC") and Hong Kong Privacy Commissioner for Personal Data, data minimisation is defined as to "strictly collect, store and use personal data that is relevant and necessary for the intended purpose for which data is processed".

5 See "Collection of Personal Data by ICT Systems" – Singapore Personal Data Protection Commission and Hong Kong Privacy Commissioner for Personal Data, *Guide to Data Protection by Design for ICT Systems* (2019) at pp 13–14.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council 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, Art 25.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council 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, Art 42(5).

of litigation.[8] A positive benefit for users could potentially be that such certification could help to alleviate concerns as to data protection compliance and dispense with the requirement to conduct full due diligence checks on organisations.

10 Even for the "Environmental" component, we argue that there is not just a strong but also natural intersection between data protection or privacy and ESG in terms of mandating effective resource use and management.

B. Social

11 The social aspect of ESG touches on an organisation's human capital and engagement with the community. This includes health and safety and human capital development, product liability, stakeholder engagement and engagement with society at-large. On the other side, personal data protection or privacy is principally about protecting the interests of individuals and balancing an individual's autonomy over his/her personal data and legitimate business and social interests. The intersection between the two cannot be more obvious. Engagement is key.

12 Data protection or privacy programmes and regimes generally support three concepts. The first is the right of an individual to access, correction and erasure/withdrawal. The second is to enable individuals to engage and exercise these rights by first understanding how that data is used by an organisation and for what end. The third is to hold the organisation accountable to what they have committed themselves to. Employees of an organisation will hold the organisation to these standards, whilst consumers will demand such engagement with the organisation for every transaction.

13 The intersection under the "Social" component is easy to visualise. The intersection for the last component is probably even easier to see.

---

8 Europrivacy, "Press Release: The GDPR European Protection Seal Approved by the EU, a New Era for Privacy and Data Protection Compliance" (12 October 2022) <https://europrivacy.org/en/news/2022-10-14/europrivacy-gdpr-european-data-protection-seal-approved-eu-new-era-privacy-and-data> (accessed 5 March 2023).

C. Governance

14 Governance broadly refers to corporate governance and behaviour, such as the organisation's corporate policies and practices, as well as its conduct. Data protection laws such as the Personal Data Protection Act ("PDPA") and related regulations will dictate the statutory framework for organisations to operate within, but organisations will necessarily have to adopt policies and practices specific to their circumstances to ensure compliance.

15 The Singapore Exchange ("SGX") has come up with a list of core ESG metrics[9] that can be referred to when preparing disclosures to better align between users and reporters of ESG information. Whilst data protection is not yet part of the existing metrics, it can easily fit into three out of the six topics, namely "Certifications", "Alignment with Frameworks" and "Assurance". Legislation already necessitates organisations to have data protection policies and frameworks in place. The Singapore experience also makes local certification, such as the Data Protection Trust Mark, available for organisations to report on the same should they procure them.

16 Another aspect of data protection that enables it to go hand-in-hand with the objective of reporting under "Governance" is the very fact that because of the importance of employee and consumer data to businesses, effective governance of data protection programmes is becoming a board-level responsibility. There are already predictions in various commentaries online of boards assuming responsibility for the performance and success of the organisation's data protection programme and steady adoption of binding corporate rules, and thereby contributing to this component of ESG metrics.

III. Championing data protection or privacy obligations as part of the Environmental, Social and Governance framework

17 It is widely accepted that the "Governance" component is the most likely place where data protection or privacy would reside very well.

9 Singapore Exchange, *Starting with a Common Set of Core ESG Metrics* (December 2021).

However, we propose that data protection or privacy would find a home in every component of any ESG framework.

A. Environmental

18 While not immediately apparent, personal data protection obligations can play a role in an organisation's response to and performance in relation to the Environmental component. The most direct opportunity here is that by promoting data minimisation and reducing data footprint as discussed in the earlier section, there will be a decreasing demand and need for data storage, and the energy required to store data in physical servers at data centres will also decrease.

19 In this section, we discuss what other opportunities there can be under the environmental component. Still with the data centre example, in Singapore alone, the total available data centre capacity was about 1,000Mw across more than 70 operational data centres as of 2021.[10] Accounting for about 7% of electricity consumption in Singapore, there has been a strong push for more efficient data centres with a three-year moratorium that was lifted for pilot applications for data centres that meet stringent efficiency and decarbonisation standards.[11]

20 While the choice of a more efficient data centre would not come within any of the personal data protection obligations, there is the potential for an indirect link from the actual use of data centre capacity and even internal IT systems and equipment. These can extend throughout the life-cycle of the equipment beyond just operations, from production to transport and end-of-life/disposal.

---

10 See Ministry of Trade and Industry, "Written Reply to Parliamentary Question on Data Centres" (11 January 2022) <https://www.mti.gov.sg/Newsroom/Parliamentary-Replies/2022/01/Written-reply-to-PQ-on-data-centres> (accessed 5 March 2023).

11 See Infocomm and Media Development Authority, "EDB and IMDA Launch pilot Data Centre – Call for Application (DC-CFA) to Support Sustainable Growth of DCs" (20 July 2022) <https://www.imda.gov.sg/Content-and-News/Press-Releases-and-Speeches/Press-Releases/2022/Launch-of-pilot-Data-Centre---Call-for-Application-to-support-Sustainable-Growth-of-DCs> (accessed 5 March 2023).

21 We suggest that the Purpose Limitation, Protection and Retention Limitation, and Data Portability obligations can play a key role in an organisation's response to and performance in relation to the Environmental component.

(1) Purpose Limitation, Protection and Retention Limitations

22 The Purpose Limitation obliges organisations to only collect, use or disclose personal data for the purposes that a reasonable person would consider appropriate under the given circumstances and for which the individual has been informed of.[12] On its own, the Purpose Limitation should reduce the personal data collected, used or disclosed by an organisation and the resources required to do so.

23 The Protection and Retention Limitations oblige organisations to take reasonable security arrangements to protect personal data in their possession or under their control, and to cease to retain personal data as soon as the purpose is no longer being served or no longer required for legal or business purposes. Together with the Purpose Limitation these obligations, if judiciously applied, should also reduce the resources required in implementing security arrangements and the need for personal data to be retained or processed.

24 Another area for potential resource efficiencies is in avoiding duplication of efforts in collecting, using or disclosing personal data. The potential for duplication can also come under the Data Portability obligations.

(2) Data Portability

25 The Data Portability obligation is part of the PDPA but will only come into effect when the relevant regulations are issued. Very generally, this obliges organisations to transmit individuals' data in their possession or under their control to another organisation in a machine-readable format.

26 The key intention of the Data Portability obligation was to give individuals greater control over their personal data by enabling their data to

---

12 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the PDPA*, para 13.1.

be transmitted between organisations in a commonly used machine-readable format, enabling personal data to be moved across services and enabling greater access to more data by organisations.[13]

27 This has the potential to improve efficiencies and innovation by enabling greater access and transmissibility of personal data but conceptually poses significant risks of duplicating and multiplying datasets across organisations and ultimately their IT resources and service providers.

(3) An opportunity for resource efficiency

28 Taken to a potential logical extreme, the foregoing obligations can be read and applied to enable a common pool of data resources accessible and available to organisations; the assumption being that "at-scale" data resources should be more efficient than having multiple individual resources.

29 Organisations that interface directly with the individuals can already go a long way in fulfilling their Purpose Limitation, Protection and Retention Limitations by engaging the services of trusted service providers. Such service providers are then bound by similar Purpose Limitation, Protection and Retention Limitations in relation to each organisation that engages them, and the data for each organisation should presumably not be co-mingled.

30 By changing the arrangement between organisations and the service providers to one more akin to that of the organisation obtaining data and services from the service provider(s) as a central repository, it is proposed that the service provider(s) should be able to provide better efficiencies in consolidating and deduplicating data resources. The proposed solution would be a cross between data brokers and central identity authorities.

31 A similar approach has been explored in a Practical Guidance issued by the Personal Data Protection Commission ("PDPC") on data collaboration using a common data intermediary. Where data is to be shared between data controllers through the data intermediary the guidance

13 See Personal Data Protection Commission, *Public Consultation On Review Of The Personal Data Protection Act 2012 – Proposed Data Portability And Data Innovation Provisions* (22 May 2019) at para 1.4.

is that, for such sharing to occur, data controllers should establish that an exception to consent applies or otherwise obtain individuals' consent.[14]

32 Having personal data consolidated among a handful of organisations presents significant concerns over data monopoly or oligarchy and most significantly data security. This would somewhat circuitously have to be mitigated by some degree of data segregation potentially by industry and function. More importantly, in order to minimise concerns about monopolies or oligarchies and to establish trust, such service providers should not be privately-held or for-profit but supported by and serving the target individuals and organisations.

33 Government-led examples would be Singapore's "SingPass" and "CorpPass" services that provide a central service for identity verification and personal data retrieval, and "SGFinDex" that provides a centrally-managed system to access and share financial information across different government agencies and financial institutions. Services offered by the industry service providers could be ancillary and pertain to less sensitive personal data.

34 In summary, under the "Environmental" component of any ESG framework, for the reasons discussed above, what may potentially be relevant data protection or privacy metrics could be:

(a) whether energy used for data storage needs is at widely accepted efficient and sustainable levels;

(b) whether data minimisation and transparency as encapsulated under the Purpose Limitation, Protection and Retention Limitations are upheld;

(c) whether data is portable; and

(d) whether data is obtained through resource-efficient means.

B. Social

35 Personal data protection obligations fall neatly within the Social component of ESG as explained above.

---

14 See Personal Data Protection Commission, *Guidance to Data Collaboration Arrangement Involving Common Data Intermediary* (March 2021).

36 Taking the PDPA as a reference point, it is noted that the PDPA obligations are by design primarily intended to protect individuals while providing flexibility for organisations to innovate and conduct business. Compliance with PDPA obligations and responsible use of the bases and additional bases for collection, use and disclosure without consent, as well as exceptions in the PDPA, can promote and be beneficial to society at-large.

37 These include the various bases in the Schedules of the PDPA that allow collection, use and disclosure on the bases of being in the vital interests of individuals, affecting the public or the public interest, legitimate interests (with necessary safeguards and assessments), business asset transactions and business improvement, research purposes and evaluative purposes.

38 The PDPC has also issued various Advisory Guidelines, Guides and Practical Guidance for specific industries and topics including responsible use of biometrics, data collaboration, application to social services, anonymisation and securing of personal data in electronic media just to name a few.

39 The significance of such obligations can be found in the response of consumers to a breach. This can include reputation loss and loss of company value, with certain surveys suggesting that consumers would not do business with a company if there are concerns over data security practices and some 70% would stop doing business with a company if personal data is given away without permission.[15] This has a direct impact on the values of intangible assets such as trade names and marks, and intellectual property.

40 Other instances providing a more concrete illustration of the impact of failure to protect personal data can be seen from record fines imposed on Amazon and Meta for failing to report breaches under the GDPR,[16] the

15 Venky Anant *et al*, "The consumer-data opportunity and the privacy imperative" *McKinsey & Company* (27 April 2020) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> (accessed 5 March 2023).

16 Amazon was fined €746m by the Luxembourg National Commission for Data Protection and Meta was fined €405m by the Ireland Data Protection Commission.

lowered sale price in Verizon's acquisition of Yahoo, as well as settlement offers with long-term effects by Equifax.[17]

41 The social demands are clear, and so are the implications of failing to engage as demanded. We therefore propose, under the "Social" component of any ESG framework, the inclusion of minimally the following data protection or privacy metrics:

(a) whether rights of individuals to access, correction, withdrawal/erasure are upheld;
(b) what efforts are being undertaken to further the data security agenda; and
(c) whether incident response policies have been implemented.

C. Governance

42 We argue that the fundamental principle of the PDPA is accountability. This obliges organisations to develop and implement policies, communicate and ensure that such policies are implemented within the organisation, appoint a Data Protection Officer or team to ensure compliance, as well as implement processes and practices to fulfil obligations under the PDPA. As a governance matter, these obligations typically fall upon the directors and key executives to prepare and implement the relevant policies and practices for the organisation, but staff and administrators handling the day-to-day operations are the key in actual and practical compliance.

43 A key focus of recent personal data protection principles is the "by design" approach, where personal data protection principles are considered and incorporated at the time of conceptualising and planning for a system and implemented throughout the life-cycle of the relevant data and system. The "by design" approach requires overall transparency of the relevant system within the organisation so directors, key executives and relevant staff

17 Alejandro Romero, "Brand Exposure: How Exposed Personal Data Impacts Corporate Digital Risk" *Forbes Technology Council* (31 March 2022) <https://www.forbes.com/sites/forbestechcouncil/2022/03/31/brand-exposure-how-exposed-personal-data-impacts-corporate-digital-risk/?sh=1740ba762159> (accessed 5 March 2023).

can be made aware of the potential risks involved and implement the necessary policies and safeguards.

44 Apart from the broader data protection obligations, there is also a push for greater public disclosures and accountability. For example, the US Securities and Exchange Commission has proposed that material cybersecurity incidents are to be disclosed by publicly listed companies, and in Singapore breaches that result in, or are likely to result in, significant harm or are of significant scale must now be reported to the PDPC.

45 Prior to breaches or incidents occurring, pre-emptive measures ought to be taken to minimise the likelihood of such breach or incident, to the extent possible. Data Protection Impact Assessments ("DPIA") or Privacy Impact Assessments ("PIA") would be helpful in this sense. DPIA or PIA are founded upon risk-based assessments of a processing activity, and it is usually up to an organisation to decide if it ought to be conducted. Since this places a lot of autonomy on the organisation with regards to how to check itself, there are other ways that regulations can and have been introduced in order to compel an organisation to remain accountable. For example, in the Philippines, the requirement of mandatory registration of a personal data processing system for a controller or processor that employs 250 persons or more, or those processing sensitive personal information of 1,000 individuals or more, or those processing data that will likely pose a risk to the rights and freedoms of data subjects, was recently introduced with the National Privacy Commission ("NPC").[18]

46 Given the above, there is no greater message on the importance of an organisation's accountability to its consumers and investors in respect of its data protection obligations than if they were taken seriously and driven at board-level. For the "Governance" component of any ESG framework, we propose including at least the following data protection or privacy metrics:

(a) extent of commitment given to data protection programmes and governance of the same;

(b) whether the organisation has data protection policies and frameworks in place and how often they are reviewed;

18 See Republic of the Philippines National Privacy Commission, NPC Circular No. 2022-04 (5 December 2022, effective on 11 January 2023).

(c) whether the organisation has obtained any certification for its processes or what DPIA or PIAs have been done; and

(d) what measures are in place to account to the consumers and public of its data security practices.

IV. Recommendations and conclusion

47 We have discussed at the beginning of this article how ESG and personal data protection obligations intersect at each component. We have made a case for the inclusion of data protection or privacy into any ESG frameworks, as well as proposals for each component. How can we now take the agenda forward to bring data protection as essential reporting items into ESG?

48 Locally, integration can happen at three levels. One is with the support of listing bodies like SGX. As discussed, the core ESG metrics can be expanded to include the points we raised in this article. The second is through an Advisory Guideline, potentially falling under the chapter of Accountability. The third is through industry-led guidelines. For example, for financial institutions, the Monetary Authority of Singapore ("MAS") could include such requirements within its relevant guidelines and circulars for disclosure of sustainability approaches.

49 Beyond Singapore, it can be an uphill task with so many other variables in the picture. However, a good starting point can be a continued revision and update to the ISSB's work, which already holds so much promise, keeping various stakeholders eager for what it can deliver.

50 Nevertheless, what is clear is that although it took almost 20 years for ESG to be a globally accepted concept that is now becoming more uniform and standardised, it will take data protection much less time to be an integral part of it. The time for it will be soon, if not now.

DEVELOPMENTS IN DATA PRIVACY LITIGATION GLOBALLY AND IN SINGAPORE: ADDRESSING THE GROWING NEED FOR INDIVIDUALS TO PROTECT THEIR PERSONAL DATA*

Lijun CHUI†
LLB (National University of Singapore);
Advocate and Solicitor (Singapore); Solicitor (England & Wales)

Allen LYE Xin Ren‡
LLB (National University of Singapore);
Advocate and Solicitor (Singapore)

Joseph LIM Weisheng§
LLB (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

1 Data privacy litigation is rising globally, with claims being brought not only in relation to breaches of the "protection" obligation,[1] but also, among other things, the violation of child privacy and the failure to ensure accuracy of personal data. In this article, we will explore several recent developments and themes in the global data privacy litigation landscape and analyse how these may shape data privacy litigation in Singapore. We will also consider how, aside from potential statutory causes of action, the common law may be able to provide relief to affected individuals. Finally,

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner, Bird & Bird ATMD LLP, Singapore.

‡ Senior Associate, Bird & Bird ATMD LLP, Singapore.

§ Associate, Bird & Bird ATMD LLP, Singapore.

1 *Ie*, the obligation to make reasonable security arrangements to protect personal data within an organisation's possession or under its control.

we will briefly consider the valuation of data for determining loss in the context of data privacy.

II. Right of private action under statute

2 In Singapore, the starting point is s 48O(1) of the Personal Data Protection Act 2012[2] ("PDPA"), which provides an individual who has suffered loss or damage, directly as a result of a contravention of the PDPA by an organisation or a person, with the right to commence a private action for civil relief. Potential civil reliefs that may be granted by the court include, among other things, damages, injunctions, or declarations.[3]

3 The right of private action operates in parallel to the enforcement regime administered by the Personal Data Protection Commission ("PDPC").[4]

4 Notably, the administrative penalties under the enforcement regime are punitive in nature and do not provide compensation or restitution to the claimant. The claimant must, generally, commence a private action under s 48O of the PDPA for compensation and restitution for his/her losses or damages.

A. Emotional distress

5 The Singapore Court of Appeal recently delivered a landmark judgment concerning the scope of "loss or damage" for which the right of private action may be exercised pursuant to s 48O(1) of the PDPA. It was held in *Michael Reed v Alex Bellingham*[5] ("*Bellingham*") that "loss or damage" for which a private action may be brought encompasses the emotional distress suffered by the victim (in addition to the traditional pecuniary heads of loss).

---

2 2020 Rev Ed.

3 Personal Data Protection Act 2012 (2020 Rev Ed) s 48O(3).

4 Under the regime, the PDPC is empowered to investigate and impose administrative penalties on the organisation or person if they are found to have contravened the provisions of the PDPA.

5 [2022] SGCA 60.

6 In *Bellingham*, the defendant was a marketing consultant who obtained the claimant's personal data through his former employers and used the data to market a new investment product to the claimant. The claimant brought a claim for "loss or damage" on account of the emotional distress he suffered from the defendant's misuse of his personal data.

7 The court ruled in favour of the claimant and found that the Singapore Parliament had, by enacting s 48O (or then-s 32) of the PDPA, intended to include emotional distress as an actionable head of loss for commencing a private action.[6] The PDPA was intended to address the increasing misuse of personal data occasioned by the "vast and ever-increasing volume of personal data being collected and processed", which, in most cases, would result in emotional distress as the only loss or damage suffered.[7] If emotional distress was not an actionable head of loss or damage, the effectiveness of the right of private action under the PDPA would be significantly neutered and antithetical to its intended objectives of protecting personal data.[8]

8 *Bellingham* therefore aligns Singapore's position regarding emotional distress as an actionable head of loss or damage with other jurisdictions such as Hong Kong,[9] the People's Republic of China,[10] Canada, New Zealand, the European Union ("EU") and the UK.[11]

9 There are additional issues which would benefit from further clarification:

---

6 *Michael Reed v Alex Bellingham* [2022] SGCA 60 at [107].

7 *Michael Reed v Alex Bellingham* [2022] SGCA 60 at [99].

8 *Michael Reed v Alex Bellingham* [2022] SGCA 60 at [95]–[96].

9 In *Tsang Po Mann v Tsang Ka Kit* [2021] HKCU 665, the Hong Kong District Court awarded HK$70,000 as damages for the emotional distress suffered by a claimant in relation to the misuse of CCTV footages that contained personal data.

10 In *Zhang et al v A Merchant* Online Infringement Liability Dispute, the Guangzhou Internet Court ordered the defendant shop owner, who had posted his WeChat history with the claimants and the claimants' WeChat account information online, to pay damages to the claimants on account of the emotional distress suffered by the latter from the breach of privacy.

11 See *Vidal-Hall v Google Inc* [2016] QB 1003.

(a) First, the right of private action under the PDPA allows, among other things, recovery for damages. As emotional distress is a fundamentally qualitative experience, it remains to be seen how the Singapore courts will handle such a quantification exercise.

(b) Second, the court observed that one of the "control mechanisms" in s 32(1) of the PDPA (now s 48O(1)) was that the "loss or damage" must be *directly* suffered as a result of a contravention of the obligations under the PDPA.[12] It remains to be seen how the concepts of factual causation, legal causation and remoteness will form part of the court's inquiry.

B. Violation of child privacy

10 The ubiquity of social media has created enhanced risks with respect to child privacy. There are already several cases concerning the violation of child privacy.

11 In the US,[13] a class of children (appearing through their legal guardians) had brought an action against, among others, Google LLC and YouTube LLC alleging that they had used persistent identifiers[14] to collect their information and track their online behaviour surreptitiously and without their consent.[15] The action is currently in its interlocutory stages.

12 In China, the Hangzhou Yuhang District People's Procuratorate recently filed a civil public interest lawsuit against a video platform company for failing to obtain the express consent of the legal guardians of the children using its video platform to collect and store each child's personal information on the platform. The suit was settled after the company cooperated with the relevant authorities and made the necessary rectifications to the platform.

---

12 *Michael Reed v Alex Bellingham* [2022] SGCA 60 at [93].

13 *Jones v Google LLC, et al*, No. 21-16281 (9th Cir, 2022).

14 This refers to information that can be used to recognise a user over time and across different websites or online services.

15 Regulations were passed in 2013 under the federal Children's Online Privacy Protection Act that prohibited the collection of children's "persistent identifiers" without parental consent.

13 In the UK, there are also indications that the Children's Commissioner for England may commence a suit on behalf of a 12-year-old girl for misusing and processing the latter's personal information, in breach of duties owed under the European Union General Data Protection Regulation[16] ("GDPR").[17]

14 Notably, there are statutory protections introduced in these jurisdictions to provide "special protection" for children. For example:

> (a) In the GDPR, children are expressly stated to be "vulnerable natural persons", and there is a stipulation requiring that "specific protection should … apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child".[18]
>
> (b) Articles 28 and 31 of the Chinese Personal Information Protection Law provide that the personal information of minors under the age of 14 is sensitive personal information, and where the personal information of minors under the age of 14 is handled, special rules for handling personal information shall be formulated and the consent of the minor's parents or other guardians shall be obtained.[19]

15 By contrast, the statutory protections in the PDPA specifically pertaining to children are narrower, requiring organisations to notify the PDPC of a data breach involving information that identifies or is likely to identify children who are involved in certain statutory or legal processes (such as court proceedings) ("PDPA Child Data Categories").[20] Aside from

---

16 Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

17 *SMO (A Child) v TikTok Inc.* [2021] 2 FLR 917.

18 Regulation (EU) 2016/679 of the European Parliament and of the Council 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, recital 38.

19 Personal Information Protection Law of the People's Republic of China (effective 1 November 2021).

20 Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) Rg 3 and Pt 1, para 5.

this, the PDPA does not recognise children as a vulnerable category of individuals or protect the personal data of children any differently from that of other individuals. It appears that the availability of a private right of action under s 48O of the PDPA for a data breach involving the PDPA Child Data Categories would therefore be predicated on a contravention of the data breach notification obligations.

16 However, the Singapore government has signalled its intention to:

> … put in place additional safeguards to protect young users, including minimising their exposure to inappropriate content and providing tools for children or their parents to manage their safety online. The code also requires that **services provide differentiated accounts to children, whereby safety settings are robust and set to more restrictive levels that are age-appropriate by default**.[21] [emphasis added in bold]

17 It may therefore be a matter of time before applicable legislation and/or regulations pertaining to child privacy are introduced in Singapore.[22]

C. Accuracy of personal information

18 Section 23 of the PDPA provides that an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is: (a) likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) likely to be disclosed by the organisation to another organisation (the "Accuracy Obligation").

19 At present, the only reported PDPC decision concerning the Accuracy Obligation was decided mainly on its facts, and the PDPC did not explain the principles which were applicable in determining whether there was a breach of the Accuracy Obligation.[23]

---

21 The Second Reading of the Online Safety (Miscellaneous Amendments) Bill, *Singapore Parliamentary Debates, Official Report* (9 November 2022), vol 95 (Mrs Josephine Teo, Minister for Communications and Information).

22 With the enactment of such legislation and/or sub-legislation, the likelihood of data privacy litigation arising on such issues will increase.

23 *Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227.

20 Notwithstanding the above, the English case of *Aven v Orbis Business Intelligence Ltd*[24] ("*Orbis*") may offer some insight into how claims in private action may be made with reference to the Accuracy Obligation. In this case, the defendant released an intelligence dossier containing personal information of the claimants that were allegedly inaccurate. The claimants commenced proceedings seeking, among other things, an order that the defendants rectify the records and correct the inaccuracy. It was the claimants' case that the defendants had breached the fourth data protection principle in the UK's Data Protection Act 2018 (*ie*, the obligation to ensure that personal data processed for law enforcement purposes is accurate and up-to-date) ("Fourth Principle").

21 The outcome of *Orbis* is immaterial for the purpose of this article. However, the following points in the judgment of Warby J in determining if the Fourth Principle had been breached are notable:

(a) First, to circumvent the Fourth Principle, the defendants argued that the statements containing the personal data were statements of opinion and not of fact. Warby J noted that there was no guidance from the UK Data Protection Act 2018 and proceeded to apply the common law defamation principles regarding whether a statement was a fact or comment.[25] He found that the statements were facts and not opinions as they were capable of verification.[26]

(b) Second, Warby J considered whether reasonable steps had been taken to ensure the accuracy of the claimants' personal data. His Honour opined that "reasonableness" must be assessed having regard to the purpose(s) for which the personal data was obtained and further processed.[27] Regarding the broad and generalised statements, Warby J accepted that reasonable steps had been taken as no adverse action would have been taken on the claimants based on those statements, and the defendants were similarly entitled to rely on his source which had a proven track record.[28] However, regarding the allegation of criminal wrongdoing, His Honour found the defendants'

24 [2020] EWHC 1812 (QB).

25 *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) at [150].

26 *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) at [151].

27 *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) at [184].

28 *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) at [185].

> approach lacking; the alleged wrongdoing spanned 15 to 20 years of which the defendants' informant had no personal knowledge of. Given the gravity of the allegation, further checks ought to have been made.[29]

22 *Orbis* will be helpful for the Singapore courts and litigating parties if the subject-matter of the dispute concerns the Accuracy Obligation.

23 The devil, however, would be in the details. While the Fourth Principle requires that personal data be "accurate" and "up to date", the Accuracy Obligation requires personal data to be "accurate and complete". Further, the Fourth Principle refers to the processing of personal data for law enforcement purposes, while the Accuracy Obligation relates to the use of the personal data to "make a decision that affects the individual to whom the personal data relates".[30] It remains to be seen whether and how such differences in wording will be dealt with by the Singapore courts.

III. Right of private action under common law

24 Aside from the legislation discussed above, there are various common law causes of action that could provide relief for the victims of disclosure and misuse of private information against an individual.

25 Jurisprudence has evolved in other jurisdictions to provide greater protection for an individual's private information.[31] In the UK, the Supreme Court developed the traditional tort of breach of confidence into a tort of misuse of private information, where the key question is whether a claimant had a reasonable expectation of privacy to the information.[32] In New Zealand, the New Zealand Court of Appeal recognised the existence of a privacy tort that addresses the wrongful publication of private information.[33]

26 In Singapore, the common law causes of action relevant to data privacy litigation are still under development, and some reference can be drawn from the following cases.

---

29 *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) at [186].

30 Personal Data Protection Act 2012 (2020 Rev Ed) s 23.

31 *ANB v ANC* [2015] 5 SLR 52 at [19].

32 *ANB v ANC* [2015] 5 SLR 52 at [19].

33 *Hosking v Runting* [2005] 1 NZLR 1.

27 In *Ngiam Kong Seng v Lim Chiew Hock*[34] ("*Ngiam*"), the Singapore Court of Appeal accepted that the wilful communication of false information would be actionable if it causes physical, including psychiatric, harm. A claimant suffering such harm could pursue a cause of action in the tort of infliction of emotional distress. In *Ngiam*, the first appellant was seriously hurt in a traffic accident allegedly caused by the respondent. The second appellant, who initially believed that the respondent was a good Samaritan, claimed that she suffered from depression from the respondent's allegedly deceitful conduct in his communication of matters relating to the accident to her.

28 The Court of Appeal stated the claimant must have suffered a recognisable psychiatric illness (which was to be distinguished from sorrow and grief) and it had to be factually foreseeable that the claimant could sustain such psychiatric harm as a result of the defendant's negligence.[35] In *Ngiam*, it was held to be not factually foreseeable that the respondent's mere communication of matters relating to the accident to the second appellant, without more, could result in such harm.[36] The Court of Appeal also recognised that there could be possible remedies for psychiatric harm resulting from the communication of information where there is a professional relationship between the parties.[37]

29 Some forms of encroachment of privacy may therefore be vindicated through the tort of intentional infliction of emotional distress. However, this will only succeed if a recognised psychiatric illness is suffered and not

34 [2008] 3 SLR(R) 674.

35 *Ngiam Kong Seng v Lim Chiew Hock* [2008] 3 SLR(R) 674 at [97]–[131].

36 *Ngiam Kong Seng v Lim Chiew Hock* [2008] 3 SLR(R) 674 at [132]. It is noted that in *Ngiam*, the Court of Appeal had proceeded on the assumption that the second appellant had a recognisable psychiatric illness. Further, the respondent was not found to have lied to the second appellant in the respondent's communications with the second appellant: see *Ngiam Kong Seng v Lim Chiew Hock* [2008] 3 SLR(R) 674 at [124]–[130].

37 *Ngiam Kong Seng v Lim Chiew Hock* [2008] 3 SLR(R) 674 at [141]. The Singapore Court of Appeal cited the Supreme Court of New Zealand decision in *Furniss v Fitchett* [1958] NZLR 396, where the plaintiff succeeded in an action against her doctor for nervous shock caused by his negligent disclosure to her husband of his opinion on her mental stability.

where the misuse of private information or infringement of data privacy results only in lesser harm (*eg*, embarrassment, annoyance and/or distress).

30 The tort of private nuisance may afford relief to claimants whose private information is misused (such as being surreptitiously photographed) while they are on another person's premises. However, the claimant must be the titleholder of the land. In *AXA Insurance Singapore Pte Ltd v Chandran s/o Natesan*,[38] the plaintiff company sought an injunction to restrain the defendant from harassing its staff based on, *inter alia*, the tort of nuisance. However, the tort was held to be inapplicable as the defendant's acts only allegedly caused discomfort to persons who were non-occupiers of the plaintiff's land.[39]

31 Finally, in *Lim Oon Kuin v Rajah & Tann Singapore LLP*[40] ("*Lim Oon Kuin*"), the Singapore Court of Appeal clarified the tort of breach of confidence in Singapore as extended by its decision in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting*[41] ("*I-Admin*").

32 First, the interest to be protected must be determined.[42] This refers to the:

> (a) wrongful gain interest, where the defendant has made unauthorised use or disclosure of confidential information and thereby gained a benefit; or
>
> (b) wrongful loss interest, where the claimant seeks protection for the confidentiality of the information in itself, which is loss suffered so long as the defendant's conscience has been impacted.

33 In a wrongful gain interest scenario, the traditional approach in *Coco v AN Clark (Engineers) Ltd*[43] applies (the "Coco Approach"). This requires the claimant to establish that:

---

38 [2013] 4 SLR 545.

39 *AXA Insurance Singapore Pte Ltd v Chandran s/o Natesan* [2013] 4 SLR 545 at [6].

40 [2022] 2 SLR 280.

41 [2020] 1 SLR 1130.

42 As summarised in *Shanghai Afute Food and Beverage Management Co Ltd v Tan Swee Meng* [2023] SGHC 34 at [100(a)].

43 [1969] RPC 41.

(a) The information had the necessary quality of confidence about it. Therefore, the information cannot be common or public knowledge.

(b) The information was imparted in circumstances importing an obligation of confidence. An obligation of confidence may arise in contract or be implied from the parties' relationship.[44] It may also arise in equity when a reasonable defendant knows that the information in question was confidential and imparted in confidence.

(c) There is unauthorised use of the information to the detriment of the party from whom the information originated.

34 In a wrongful loss interest scenario, the modified approach in *I-Admin* applies instead ("I-Admin Approach"). Under this approach, if the first two limbs of the Coco Approach are proven, there would instead be a presumption of an action for breach of confidence.[45] This presumption shifts the legal burden to the defendant to prove that his/her conscience had not been affected in the circumstances of the claimant's loss (for example, by demonstrating that the defendant came across the information by accident).[46] The I-Admin Approach removed the requirement for the claimant to prove unauthorised use of the confidential information in a wrongful loss interest scenario, making it easier for a claimant to claim for breach of confidence once the claimant's private information is taken.

35 The rationale for the development of the I-Admin Approach was to safeguard the wrongful loss interest, which was not adequately safeguarded under the Coco Approach.[47] However, it is important to note that the I-Admin Approach only applies to "taker" cases (*ie*, involving unauthorised acquisition of the confidential information).[48]

36 The developments of the tort of breach of confidence in Singapore have provided greater scope for a claimant whose private information has been taken to succeed in such a claim. The tort can be used to restrain a

---

44 Such an implied relationship may include a relationship between lawyer and client, and an employer and employee.

45 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61]–[62].

46 *Lim Oon Kuin v Rajah & Tann Singapore LLP* [2022] 2 SLR 280 at [40]; *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61].

47 *Lim Oon Kuin v Rajah & Tann Singapore LLP* [2022] 2 SLR 280 at [37].

48 *Lim Oon Kuin v Rajah & Tann Singapore LLP* [2022] 2 SLR 280 at [41].

defendant from disclosing or using confidential information about a claimant even in the absence of any contractual (or other legal) relationship if an equitable duty of confidence arises on the defendant's part.

37 However, the limitation of the I-Admin Approach to "taker" cases means that a claimant who originally consented to providing his/her private information to the defendant will still have to prove unauthorised use of the private information under the Coco Approach to succeed in a breach of confidence claim.

38 Further, as the tort is intended to protect confidential information, it will be unavailable where the confidential information has lost its quality of confidence through no fault of the defendant.[49] A claim for breach of confidence will also likely fail where the information disclosed was imparted without any obligation of confidence.[50]

IV. Valuation of data

39 With the rise of data privacy litigation, another key issue is the valuation of the data lost. This will be crucial in data privacy litigation given the recent court decisions affirming that loss must be more than *de minimis*.[51]

---

49 If the confidential information becomes widely published in the media (not due to the defendant), the claim for breach of confidence will fail.

50 See *X Pte Ltd v CDE* [1992] 2 SLR(R) 575 where the Singapore High Court held there was no duty of confidence requiring a defendant not to disclose information on an extramarital relationship with the plaintiff, even though such disclosure would cause distress to the plaintiff.

51 See *Lloyd v Google LLC* [2021] UKSC 50 ("*Lloyd*") generally, where the UK Supreme Court opined that it was necessary for the claimant to prove the individual circumstance for the assessment of damages. See also *Rolfe v Veale Wansbrough Vizards LLP* [2021] EWHC 2809 (QB) at [5]. Further, in *Michael Reed v Alex Bellingham* [2022] SGCA 60, the Singapore Court of Appeal affirmed *Lloyd* and held that "loss of control" of personal data, *per se*, would not constitute "loss or damage" under s 48O of the PDPA.

40 The issue is further complicated given that data privacy is valued differently across jurisdictions.[52]

41 In Singapore, the PDPC, in conjunction with the Infocomm and Media Development Authority ("IMDA"), released a *Guide to Data Valuation for Data Sharing* setting out three different approaches for valuing data.[53]

A. Approach 1: the "Income Approach"

42 This approach assumes that the value of the data asset is equivalent to the value of the expected future cash flow generated over a specified period.[54]

43 The value of data would be derived by determining the difference between: (a) the revenue generated by the organisation with access to the data; and (b) the revenue generated by the organisation without such access.[55]

B. Approach 2: the "Cost Approach"

44 The value of data would be derived by determining the costs required to replace or reproduce the lost data. The "replacement" cost would be the current cost of replacing a similar data asset with equivalent utility to the data asset being valued,[56] while the "reproduction" cost would be the current cost of producing or reproducing the data in-house using similar inputs and methods.

---

52 This is evident from the differences in the administrative penalties to be met out for data breaches across different jurisdictions. For example, while the penalties for a data breach under the GDPR may go up to €20m or 4% of the total global turnover of the preceding fiscal year (whichever is higher), the penalties for a data breach in Vietnam are between VND10m to VND20m (*ie*, approximately SGD500 to SGD1,100).

53 Personal Data Protection Commission and Infocomm and Media Development Authority, *Guide to Data Valuation for Data Sharing* (2019).

54 For example, this may refer to the remaining useful lifespan of the data.

55 This approach requires the incremental cash flow to be generated by the data to be reasonably forecasted and quantified.

56 This will involve looking at transactions involving similar data assets.

C. Approach 3: the "Market Approach"

45 The value of data would be determined with reference to the market price of the lost data. This, however, requires an available active market for the said data.[57]

D. Is there a "best" approach?

46 There is no "best" approach in the valuation of data. Ultimately, the key determinant is whether the approach used accurately captures the value of the data lost.[58]

47 Other considerations which can be taken into account when calculating the value of data may include:[59]

> (a) the average and/or marginal value to the business of the sale, collection or deletion of a consumer's data;
> (b) the aggregate value to the business of the sale, collection or deletion of a consumer's data divided by the total number of consumers;
> (c) the profit and revenue generated by the business from and the expenses related to the sale, collection, retention or deletion of a consumers' personal information; and
> (d) any other practical and reasonably reliable calculation method used in good faith.

---

57 This approach was applied in the US case of *De Medicis v Ally Bank*, 21 Civ 6799 (NSR). In this case, the plaintiffs alleged that the defendant had negligently disclosed their customers' account usernames, passwords and other private information to unnamed third parties, and that they had suffered "actual injury in the form of damages to and diminution in the value of [their] private information – a form of intangible property". However, the US District Court for the Southern District of New York dismissed the suit on the basis that the plaintiffs had failed to establish that he had an alleged "diminution in the value" of his private information as he failed to prove that there was a market for such information.

58 For example, the permanent loss of a digital transcript of the biography of a deceased person would be irreplaceable. In such circumstances, using the "income approach" to value data would be more sensible than the "cost approach" or the "market approach".

59 See California Consumer Privacy Act Regulations (2020) § 7081.

V. Conclusion

48 Data privacy litigation is likely to increase, particularly as personal data is increasingly collected and used in ways that may not have been contemplated by the owner of the data. While data privacy is conceptually complex and difficult to define, it is anticipated that the law would rise to the challenge and provide adequate relief. The Singapore Court of Appeal's decision in *Bellingham* is a step in the right direction and displays an appreciation for the growing need for legal protection of data privacy. It remains to be seen how legislation and case law will develop to address this need.

EMPLOYER LIABILITY AND THE EMPLOYEE EXEMPTION*

Benjamin WONG†
LLB (Hons) (National University of Singapore), LLM (London School of Economics);
Advocate and Solicitor (Singapore)

I. Introduction

1 When an employee does something which appears to breach a data protection obligation under the Personal Data Protection Act 2012[1] ("PDPA"), two questions typically arise.

2 First, is the *employee* liable for breaching the PDPA? In this regard, the PDPA contains an "employee exemption" provision under s 4(1)(*b*) which operates, under certain circumstances, to exempt employees from the data protection obligations of the PDPA.

3 Second, is the *employer* liable for breaching the PDPA? In this regard, the PDPA contains an "employer liability" provision under s 53(1), which ascribes the doings of an employee to his or her employer, thereby potentially causing the employer to face liability for breaching the PDPA.

4 The purpose of this article is to discuss the application of both ss 4(1)(*b*) and 53(1). Part II of this article addresses the definitions of "employee" and "employment". Part III will examine s 4(1)(*b*), and Pt IV will discuss s 53(1). Part V focuses on the phrase "in the course of his or her employment", and Pt VI marks the interaction between the ss 4(1)(*b*) and 53(1). Part VII concludes.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors are the author's own.

† Lecturer, National University of Singapore.

1 2020 Rev Ed.

II. "Employee" and "employment"

5 As a preliminary matter, it is important to note that the PDPA takes an expansive definition of the terms "employee" and "employment". In particular, the PDPA defines "employee" to include a volunteer, and "employment" to include "working under an unpaid volunteer work relationship".[2] Thus, a person who is undertaking unpaid work for an organisation may be regarded as an employee employed by the organisation.

6 A practical implication of this expansive definition of "employee" and "employment" is that both ss 4(1)(*b*) and 53(1) are likely to apply even in the context of an organisation that is run wholly or mainly by unpaid volunteers. For example, in the case of *Singapore Taekwondo Federation*,[3] the Personal Data Protection Commission ("PDPC") found that an organisation had breached the Accountability Obligation and the Protection Obligation. The organisation (which was a registered society involved in promoting the sport of taekwondo in Singapore) represented that it was "managed mostly by a team of volunteers"; nevertheless, the PDPC pointed out that under the PDPA, volunteers are also regarded as employees, and therefore pursuant to s 53(1) the organisation was responsible for their actions.[4]

III. Employee exemption: section 4(1)(*b*)

7 Section 4(1)(*b*) provides for the employee exemption:

> **4.**—(1) Parts 3, 4, 5, 6, 6A and 6B do not impose any obligation on —
>
> …
>
> (*b*) any employee acting in the course of his or her employment with an organisation;
>
> …

8 Parts 3 to 6B of the PDPA are the Parts that set out the data protection obligations, such as the Consent Obligation under s 13 and the Protection Obligation under s 24. So, in effect, s 4(1)(*b*) offers a general

---

2 Personal Data Protection Act 2012 (2020 Rev Ed) s 2(1).

3 [2019] PDP Digest 247.

4 *Singapore Taekwondo Federation* [2019] PDP Digest 247 at [19].

exemption from the data protection obligations, in favour of employees acting in the course of their employment.

9 One question that may arise in relation to s 4(1)(*b*) is whether the burden of proving the applicability of the provision lies with the plaintiff or with the defendant. This question was answered in the recent case of *Reed, Michael v Bellingham, Alex*[5] ("*Reed v Bellingham*"), where the Court of Appeal held that the burden of proof lies with the defendant pleading s 4(1)(*b*). This was because s 4(1)(*b*) (and, indeed, the other exemption provisions under s 4(1)) were *defences* which the defendant "may invoke to avoid liability for the putative breach", and therefore it was incumbent on the defendant to prove that he or she fell within the ambit of the exemption.[6] Reading s 4(1)(*b*) as a defence was "consistent with principles of statutory construction", consistent with a similar defence under s 48(1), and consistent with the general legislative purpose of the PDPA under s 3.[7]

IV. Employer liability: section 53(1)

10 Section 53(1) provides for employer liability:

> Any act done or conduct engaged in by a person in the course of his or her employment (called in this section the employee) is treated for the purposes of this Act as done or engaged in by his or her employer as well as by the employee, whether or not it was done or engaged in with the employer's knowledge or approval.

11 Thus, s 53(1) attributes the doings of an employee (if done in the course of his or her employment) to his or her employer, and if those doings constitute a breach of a data protection obligation then the employer would be liable for that breach.

12 Does an employer have any defence against liability ascribed to it under s 53(1)? Section 53(2) does provide for such a defence:

> In any proceedings for an offence under this Act brought against any person in respect of an act or conduct alleged to have been done or engaged in (as the case may be) by an employee of that person, it is a defence for that

5 [2022] 2 SLR 1156.

6 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [42].

7 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [42]–[45].

> person to prove that the person took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his or her employment, acts or conduct (as the case may be) of that description.

13 Thus, as stated by the PDPC in the case of *Progressive Builders Private Limited*,[8] s 53(2) provides the employer with a "defence of reasonable diligence": "where the employer had taken reasonable steps to prevent or reasonably reduce the risk of the occurrence of the employee's action or conduct that resulted in an unauthorised collection, use and/or disclosure of personal data", such reasonable diligence on the part of the employer can be used as a defence against s 53(1) liability.[9]

14 However, it must be highlighted that s 53(2) is limited to proceedings for *offences* under the PDPA. Therefore, s 53(2) cannot apply in cases where the employer has been made liable for a breach of a data protection obligation (for example, the Purpose Limitation Obligation), as breaches of such data protection obligations do not generally constitute a criminal offence. That being said, the employer's reasonable diligence may yet be taken into account in determining whether the employer should be liable under s 53(1).[10]

V. "In the course of his or her employment"

15 A key phrase in both ss 4(1)(*b*) and 53(1) is the phrase "in the course of his or her employment". Both provisions will only operate if the employee in question was acting "in the course of his or her employment". Thus, in the context of s 4(1)(*b*), it is not sufficient for the employee merely to prove that he or she was an employee at the time he or she acted in breach of the PDPA – the employee must also establish that he or she was acting "in the course of his or her employment".[11] Similarly, in the context of s 53(1), the doings of an employee will not be attributed to the employer unless it is shown that the employee was acting "in the course of his or her employment".

---

8 [2021] SGPDPC 2.

9 *Progressive Builders Private Limited* [2021] SGPDPC 2 at [12].

10 See paras 17–24 below.

11 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [54].

16 It is submitted that the interpretation of this phrase should be consistent across both provisions. Accordingly, this phrase will be examined in this article in a coherent fashion, within a single chapter drawing both from cases dealing with s 4(1)(*b*) and from cases dealing with s 53(1).

A. Some common situations

17 To begin with, it will be helpful to highlight some of the situations in which employees have been found to have acted in the course of their employment. This will serve to illustrate the interpretation of this phrase in practice.

(1) Executing administrative functions

18 There have been cases where employees executing an administrative function for the organisation were regarded as acting in the course of their employment. These cases tend to be fairly straightforward.

19 For example, in the case of *Re Habitat for Humanity Singapore Ltd*,[12] the organisation sent letters to its volunteers, to acknowledge their participation in an event that had been organised by the organisation. Ordinarily, the organisation's practice was to separate the letters into individual PDF documents and send each letter via individual e-mail to the respective volunteer; however, in this instance, the inexperienced employees concerned (namely a manager and an administrative staff member) sent a mass e-mail to all the volunteers, attaching a PDF document containing all the letters. As a consequence, the volunteers' names, National Registration Identification Card numbers and e-mail addresses were inadvertently disclosed. The PDPC found that the organisation was responsible for the conduct of the employees in this incident, pursuant to s 53(1).[13]

20 A similar case was *Re GrabCar Pte Ltd*.[14] In this case, the organisation operated a carpooling service and imposed penalties on its drivers if they committed certain stipulated offences. An employee set up an online form

12 [2019] PDP Digest 200.

13 *Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [8].

14 [2019] PDP Digest 295.

using Google Forms to allow drivers to appeal their penalties. However, the employee chose an incorrect setting for the form, thereby allowing respondents to view not only their own responses but those of other respondents as well. The PDPC found that, under s 53(1), the organisation was responsible for the acts of the employee in this incident.[15]

(2) Resolving disputes involving organisation

21 There have also been cases where employees (typically, senior employees) were found to have acted in the course of their employment when resolving disputes involving the organisation. The facts of these cases are more penumbral, and attention must be paid to the *context* and *intent* of the processing of the personal data, to determine whether the employee in question was in fact acting "in the course of his or her employment".

22 For example, in *Re Executive Coach International Pte Ltd*,[16] the organisation was a company that provided coaching services; and the complainant was the personal assistant of "Mr L" (a director of the organisation). At some point, the relationship between the complainant and the organisation grew acrimonious, and the complainant left the organisation on unamicable terms. As it happened, the complainant and Mr L were participants in a WhatsApp group chat, along with other employees of the company. Mr L disclosed certain "highly sensitive information" about the complainant over the WhatsApp group chat, including her "past drug problem and issue with infidelity in her amorous relationship".[17]

23 Although at first glance it might appear that Mr L had disclosed the personal data outside the course of his employment, the PDPC nevertheless correctly found that Mr L had disclosed the personal data in the course of his employment with the organisation. In its reasoning, the PDPC looked to the context and intent of the disclosure: the PDPC noted that the disclosure was "made in the context of an ongoing dispute arising from the unamicable departure" of the complainant, and was not made by Mr L in

15 *Re GrabCar Pte Ltd* [2019] PDP Digest 295.

16 [2017] PDP Digest 188.

17 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [5].

his personal or individual capacity; further, the intent behind the disclosure was to discredit the complainant who was allegedly trying to undermine Mr L's authority as director and encourage others to leave the organisation.[18] Therefore, Mr L's conduct was attributable to the organisation, pursuant to s 53(1).

24 Context and intent was also crucial in *My Digital Lock Pte Ltd*.[19] In this case, the organisation and the complainant got into a legal dispute regarding remarks that the complainant had made about the organisation. The organisation's director ("Mr A") took screenshots of a WhatsApp conversation between himself and the complainant, and uploaded those screenshots on his own Facebook page. In doing so, Mr A disclosed the complainant's mobile phone number and home address.

25 During the PDPC's enforcement proceedings against the organisation, the organisation represented that Mr A had disclosed the complainant's personal data in his personal or domestic capacity. However, the PDPC disagreed with this representation, finding that Mr A was acting in the course of his employment with the organisation. This was because the stated intent of uploading the screenshots on Facebook was (a) to transfer the screenshots from Mr A's WhatsApp mobile app to Mr A's desktop, thereby (b) allowing Mr A to send the screenshots to the organisation's solicitors, in the context of the legal dispute between the complainant and the organisation.[20] Thus, the disclosure of the complainant's personal data by Mr A was treated as having been done by the organisation, pursuant to s 53(1).

B. Types of evidence that may be relevant

26 It will also be useful to consider the types of evidence that may be relevant in the assessment of whether an employee had acted "in the course of his or her employment".

---

18 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [11].

19 [2016] SGPDPC 20.

20 *My Digital Lock Pte Ltd* [2016] SGPDPC 20 at [5]–[13].

(1) Generally

27 In the context of s 4(1)(*b*), the Court of Appeal in *Reed v Bellingham* identified some of the relevant evidence that an employee could adduce to establish that he or she was acting "in the course of his or her employment", namely: what the employee did, what the employee was required to do as part of his or her employment, and "whether the employee deliberately evaded practices set up by the employer" to deter the employee's actions.[21] It is submitted that these would also be relevant evidence in the context of s 53(1).

(2) Employer's knowledge and approval

28 What if the employer did not know of the employee's actions, or disapproved of the employee's actions? In this regard, what seems clear is that the lack of knowledge or approval on the part of the employer does not necessarily mean that the employee's actions were not done "in the course of his or her employment".[22]

29 That being said, the employer's knowledge or approval (or lack thereof) may be relevant factors in the assessment of whether the employee had acted "in the course of his or her employment". A case in point is *Progressive Builders Pte Ltd*.[23] This case involved two organisations, which were in the construction business. One of the organisations ("PBPL") had banned the complainants (who were crane operators) from its worksite, and its Workplace Safety & Health Officer ("WSHO") had been directed to create a list containing the complainants' details (the "Banned Operators List"). However, unbeknownst to PBPL, the WSHO shared this Banned Operators List in a WhatsApp group chat with other workplace safety professionals. One question that arose was whether the WSHO's disclosure was done in the course of his employment with PBPL.

---

21 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [51].

22 See s 53(1) of the Personal Data Protection Act 2012 (2020 Rev Ed) which expressly stipulates that an employee's doings can be attributed to his or her employer "whether or not it was done or engaged in with the employer's knowledge or approval".

23 [2021] SGPDPC 2.

30 The PDPC found that the WSHO was not acting in the course of his employment with PBPL, and therefore PBPL was not made liable under s 53(1). Two reasons, in particular, were given for this finding: first, PBPL had not directed the WSHO to share the Banned Operators List, nor did PBPL know of the WhatsApp group chat; second, by sharing the Banned Operators List, the WSHO was acting in breach of his contractual obligation of confidence with PBPL.[24] Thus, this case suggests that, where the employee's act was done without the knowledge or approval of the employer, it becomes less likely that the employee's act was done in the course of his or her employment.

(3) Employer's reasonable diligence

31 Where the employer has undertaken reasonable diligence to prevent its employees from breaching the PDPA, such reasonable diligence may be taken into account in the assessment of whether the employee had acted "in the course of his or her employment".

32 The standard of reasonable diligence was laid out in *Progressive Builders Private Limited*. The PDPC noted that, whereas s 53(2) provided for a defence of reasonable diligence for employers in relation to criminal offences, there was a "similar standard of diligence" applicable to "breaches of the PDPA that are not offences", which would look to "whether the organisation had acted reasonably in meeting its responsibilities under the PDPA".[25]

33 Subsequently, the Court of Appeal in *Reed v Bellingham* agreed that "employer's liability under the PDPA is … fault based", and cited the standard of reasonable diligence as set forth in *Progressive Builders Private Limited*.[26] Notably, the Court of Appeal provided a clear example of how

24 *Progressive Builders Private Limited* [2021] SGPDPC 2 at [13].

25 *Progressive Builders Private Limited* [2021] SGPDPC 2 at [12].

26 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [49]. This brings the Singapore position close to that of the New Zealand Privacy Act: see s 211(2) of the Privacy Act 2020 (NZ).

the reasonable diligence of the employer could lead to a finding that the employee had *not* acted "in the course of his or her employment":[27]

> By way of an example, if an employer has developed and implemented policies and practices necessary for the organisation to meet its obligations under the PDPA (see s 12 PDPA), but a rogue employee takes pains to evade such supervision and thereby breaches the PDPA, it appears highly artificial to say that the rogue employee was nevertheless acting within the course of his employment. Such an errant individual should properly be regarded as having acted outside the course of his employment, thereby precluding his having recourse to s 4(1)(*b*).

VI. Interaction between the two provisions

34 Both ss 4(1)(*b*) and 53(1), when taken together, serve to allocate responsibility for breaches of the PDPA in the employment context. In other words, the two provisions determine who is to be held liable for an employee acting in breach of the PDPA.

35 It is suggested that, in practice, the two provisions create an "either/or" situation: for any particular act done by an employee in breach of the PDPA, it is either the employer or the employee who will potentially end up being held liable. This is because, practically speaking, the two provisions are coterminous (that is, in any particular case, either both provisions apply or neither of them apply). To wit:

> (a) if it is established that the employee was acting in the course of his or her employment when he or she acted in breach of the PDPA, then both provisions will operate, with the end result being that the employee is exempt from liability and the employer is held liable;
>
> (b) conversely, if the employee is found not to have acted in the course of his or her employment when he or she acted in breach of the PDPA, then neither provision will operate, with the end result being that the employee is not exempt from liability and the employer is not held liable.

---

27 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [49].

VII. Conclusion

36 Sections 4(1)(*b*) and 53(1) serve an important function of placing primary responsibility for data protection on employers, recognising that it is the employers who are best placed to implement practices to protect individuals' personal data. At the same time, the two provisions also ensure that responsible employers are not unfairly saddled with liability when, in spite of their efforts, their employees act in breach of the PDPA. In this way, the two provisions strike a balance between the rights of individuals and the interests of organisations.

INDIA'S DIGITAL PERSONAL DATA PROTECTION BILL 2022: WHAT SINGAPORE PRIVACY PRACTITIONERS NEED TO KNOW*

Alexander LUONG†
BCom LLB (Deakin University);
CIPM, CIPP/A, FIP;
Solicitor and Barrister (Victoria, Australia)

Stacey STEELE‡
BA (University of Queensland), MA (Monash University), LLB (Hons) LLM (University of Melbourne);
CIPP/E;
Solicitor and Barrister (Victoria, Australia)

I. Introduction: why compare India and Singapore?

1 The Indian Ministry of Electronics and Information Technology ("MEIT") released its draft Digital Personal Data Protection Bill 2022 ("Bill") in November 2022. The Bill is the Indian Government's latest attempt to enact an omnibus privacy law. This article analyses the Bill's key provisions and policy objectives as set out in the accompanying explanatory note and compares them to provisions in the Singapore Personal Data Protection Act 2012[1] ("PDPA"). The analysis is divided into six sections, examining the scope of the Bill, key definitions, provisions relating to collection and other processing, security and cross-border data transfers, and provisions that are unique to the Bill.

2 An understanding of the Bill and its key similarities and differences with the PDPA is important for privacy and data protection practitioners in

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer or any other party. All errors remain the authors' own.

† Head of Privacy, APAC, Olympus.

‡ Regional Privacy Officer, Japan and APAC, Olympus and Associate Professor, Melbourne Law School.

1 2020 Rev Ed.

Singapore. Bilateral trade between India and Singapore was valued at approximately US$30.11bn from 2021 to 2022.[2] With around 9,000 Indian companies registered in Singapore and more than 440 Singapore companies registered in India,[3] practitioners in Singapore are increasingly likely to have to consider the impact of Indian privacy requirements as part of their roles.

3 The India Bill and the Singapore PDPA have broad similarities, such as both being consent-based regimes. Indeed, Singapore was one of four jurisdictions whose privacy and data protection laws were explicitly referenced by the Indian Government in its explanatory note.[4] Yet, the Bill contains several provisions that distinguish India's approach from that of the Singapore PDPA and many other jurisdictions. This article discusses the Bill's use of the term "fiduciaries" and imposition of additional accountability requirements on significant data fiduciaries ("SDFs"). If this version of the Bill is enacted, even organisations with established privacy programs will need to review and uplift compliance efforts to the extent that they have business interests in India to which the Bill applies.

II. Scope

A. "Digital" personal data only?

4 The addition of "digital" to the title of this latest version of India's draft omnibus privacy law is a key difference from previous iterations. The word "digital" suggests that the Government aims to exclude personal data which may exist in physical form (such as paper records) while still being organised in some meaningful and structured form which could be indexed, searched and retrieved.

---

2 High Commission of India, Singapore, "India-Singapore Bilateral Relations Brief" (November 2022) <https://www.hcisingapore.gov.in/> (accessed 24 May 2023).

3 High Commission of India, Singapore, "India-Singapore Bilateral Relations Brief" (November 2022) <https://www.hcisingapore.gov.in/> (accessed 24 May 2023).

4 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at para 9.

5 However, "personal data" is still defined in the Bill as "any data about an individual who is identifiable by or in relation to such data" and does not specifically exclude physical records.[5] Meanwhile, the definition of "processing" has been narrowed from previous versions. In the last draft, "processing" was defined as "an operation or set of operations performed on personal data",[6] whereas the latest Bill is limited to "an *automated* operation or set of operations performed on *digital* personal data" [emphasis added].[7]

6 Moreover, the term "digital" has not been defined in the Bill; however, s 4(1) does provide some clarity, stating that the Bill applies to digital personal data collected from data principals online, and where it is collected "offline, is digitised". "Offline personal data" is explicitly excluded from the scope of the Bill.[8] The Indian Government's emphasis on "digital" personal data and its deliberate exclusion of traditional physical records (or "offline" personal data) recognises the importance of having an omnibus privacy and data protection law at a time when the Indian data economy is expected to reach 1.2 billion active online users in coming years.[9]

7 The rationale for this focus on "digital" in the Bill could be seen from the explanatory note:

> Data in general and Personal Data in specific are at the core of this fast-growing Digital Economy and eco-system of digital products, services and intermediation. It has become very clear over the last few years whilst this data is used by platforms and intermediaries, the data and personal data must be subject to a framework of rules and dos and don'ts.[10]

8 The Singapore PDPA does not distinguish "digital" aspects of personal data. For example, "processing" is defined as "the carrying out of any operation or set of operations in relation to personal data".[11]

---

5 Digital Personal Data Protection Bill 2022 (India) s 2(13).
6 Personal Data Protection Bill 2019 (India) s 3(36).
7 Digital Personal Data Protection Bill 2022 (India) s 2(16).
8 Digital Personal Data Protection Bill 2022 (India) s 4(3).
9 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at p 1.
10 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at p 1.
11 Personal Data Protection Act 2012 (2020 Rev Ed) s 2.

B. Extraterritoriality

9 The Bill also contains provisions with extraterritorial effect. The Bill applies to the processing of digital personal data outside of India if such processing is related to the profiling of, or activity of offering goods and services to data principals within India.[12] This provision makes the application of the Bill likely wider than other data protection laws such as the European Union General Data Protection Regulation ("GDPR"),[13] potentially capturing entities established outside of India that may be processing personal information related to data principals in India for a commercial purpose irrespective of the location of concerned individuals.

10 The Singapore PDPA also has potential extraterritorial effect because its obligations are applicable to any "organisation", regardless of whether the organisation was formed or is recognised under Singapore law, or is resident or has an office or a place of business in Singapore.[14] Moreover, the PDPA applies to the collection, use and disclosure of personal data of "individuals",[15] which have been defined broadly as any "natural person, whether living or deceased".[16]

III. Key definitions

11 The Bill continues to use the terms "data fiduciary" and "data principal", which were introduced in earlier versions. A "data fiduciary" is the Indian legislative equivalent of a "controller",[17] defined as "any person

12 Digital Personal Data Protection Bill 2022 (India) s 4(2).

13 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Direct 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ("GDPR").

14 Personal Data Protection Act 2012 (2020 Rev Ed) s 2.

15 Personal Data Protection Act 2012 (2020 Rev Ed) ss 3–4.

16 Personal Data Protection Act 2012 (2020 Rev Ed) s 2.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Direct 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Art 4.

who alone or in conjunction with other persons determines the purpose and means of processing personal data".[18] In turn, a "data principal" is akin to a "data subject" under the GDPR,[19] referring to the "individual to whom the personal data relates".[20]

12 The use of "fiduciary" as a term is a unique aspect of the Bill and a deliberate choice by the Indian Government. The "data fiduciary" term was first adopted in the previous version of the Bill in 2019. The term was reflective of the Government's view that the expectations of data principals and the relationship of trust created between an individual and data controllers were highly similar to fiduciary relationships created in equity, and should therefore be subject to similar standards of trust and fairness in respect of the use of the data.[21] The Indian Government confirmed this decision again in the explanatory note: "The deliberate choice of "Fiduciary" underlines that the relationship between the Data Principal and Data Fiduciary is expected to be one based on mutual trust."[22]

13 By comparison, the PDPA applies to an "organisation" and an "individual". The PDPA defines "organisation" broadly – basically any individual, company or entity, regardless of whether it is formed or recognised under Singapore law, or is resident or has a place of business in Singapore.[23] This definition avoids descriptions around the ability to determine the overall purpose and means of processing personal data like the Bill, and as also seen in the GDPR. Accordingly, "joint controllership" of personal data is not a concept explicitly set out in the PDPA, at least not in the way that the Bill deals with this concept.

---

18 Digital Personal Data Protection Bill 2022 (India) s 2(5).

19 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Direct 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Art 4.

20 Digital Personal Data Protection Bill 2022 (India) s 2(6).

21 Mark J Taylor and Jeannie Marie Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection" (2020) 16 *Indian Journal of Law and Technology* 72 at 82.

22 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at para 3.

23 Personal Data Protection Act 2012 (2020 Rev Ed) s 2.

14 Other key definitions in the PDPA and the Bill are quite similar in language and effect. For example, the Bill defines a "data processor" as any person who processes personal data on behalf of a data fiduciary,[24] while the equivalent in the PDPA is a "data intermediary" – an organisation which processes personal data on behalf of another organisation.[25]

15 Another key similarity between the two regimes is the omission of "sensitive" personal data or "special-category data". It is common in other jurisdictions to recognise certain types of personal data as being especially sensitive in respect of data subjects' fundamental rights and freedoms, and thus deserving further protections.[26] Such special provisions are not found under the PDPA in Singapore. The Indian Bill does not have this concept either, though there is a reference to the potential sensitivity of personal data processed by a data fiduciary, which is a relevant factor for the Indian Government when considering whether to designate entities as SDFs (which attract further compliance requirements).[27] The omission of "sensitive personal data" from the latest India Bill is interesting, given that it was present in previous Bills.[28]

IV. Collection and processing

16 The India Bill and the Singapore PDPA are both consent-based regimes, meaning that obtaining and relying on consent from a data principal or individual respectively is the primary lawful basis for collecting and otherwise processing personal data. While there are other lawful bases to process personal data, such provisions are framed as secondary alternatives to consent.

---

24 Digital Personal Data Protection Bill 2022 (India) s 2(7).

25 Personal Data Protection Act 2012 (2020 Rev Ed) s 2.

26 See, *eg*, Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Direct 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Recital 51.

27 Digital Personal Data Protection Bill 2022 (India) s 11.

28 See, *eg*, Personal Data Protection Bill 2019 (India) s 3(41).

A. Express or explicit consent

17 Under the India Bill, personal data may only be processed if consent has been obtained from a data principal or consent is "deemed" to have been given by a data principal in prescribed circumstances. Clear notice of the personal data being collected and the purposes of the processing must first be provided by the data fiduciary to the data principal, and must be in itemised form in clear and plain language.[29] Consent under s 7 of the Bill mirrors the definition under the GDPR: "… any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement of her personal data for the specified purpose".[30]

18 By contrast, the Singapore PDPA does not define the "consent" to be obtained from individuals. The PDPA sets out notice requirements under s 20 and requires that the individual provides their consent for that purpose.[31]

B. Deemed consent

19 Rather than provide a definitive definition of consent, the PDPA contemplates consent having several forms – express consent, either verbally or in writing, and where consent is implied or inferred under specific circumstances.[32] "Express consent" is not actually a term used in the PDPA; however, the legislation distinguishes between "consent" and "deemed consent".[33] Furthermore, the PDPA distinguishes between "deemed consent" provided under s 15 and "deemed consent by notification" under s 15A.

20 Under s 15(1), an individual is deemed to have consented to the collection, use or disclosure of personal data for a purpose if the individual had voluntarily provided the personal data for that purpose and it is

29 Digital Personal Data Protection Bill 2022 (India) s 6.
30 Digital Personal Data Protection Bill 2022 (India) s 7.
31 Personal Data Protection Act 2012 (2020 Rev Ed) s 14(1).
32 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (16 May 2022) at para 12.4.
33 Personal Data Protection Act 2012 (2020 Rev Ed) ss 14–15A.

reasonable that the individual would voluntarily provide that data.[34] This concept could be referred to as "deemed consent by conduct".[35] Section 15(3) provides grounds for "deemed consent for contractual necessity",[36] in effect, deeming consent in situations where an individual provides personal data to an organisation for the purposes of a transaction and it is reasonably necessary for that organisation to disclose that data to other organisations in order to conclude or perform the contract. Under s 15A, an individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that they had been notified of and had not taken any actions to object and opt out of.[37] This provision is subject to the organisation conducting an assessment on the potential adverse effects of the proposed collection, use or disclosure and taking reasonable steps to ensure that notification provided to individuals is adequate.[38]

21 The concept of "deemed consent" under the India Bill is similar, yet different in significant ways.

22 Deemed consent under the Bill is provided for under s 8, which prescribes nine situations where consent could be "deemed" to have been given. Section 8(1) of the Bill is equivalent to deemed consent under s 15(1) of the PDPA – deeming consent to have been given where the relevant processing activity is necessary, and the data principal had voluntarily provided the personal data and it is reasonably expected that they would do so.

23 The remaining eight grounds under s 8 of the Bill go beyond deeming or implying consent through, for example, the conduct or actions of the data principal, and instead assume that consent would have been obtained in situations where it would otherwise be impractical to request it. The underlying rationale for this approach is alluded to in the accompanying explanatory note: "In several situations, seeking consent of [the] Data

34 Personal Data Protection Act 2012 (2020 Rev Ed).

35 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (16 May 2022) at paras 12.20–12.21.

36 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (16 May 2022) at para 12.22.

37 Personal Data Protection Act 2012 (2020 Rev Ed).

38 Personal Data Protection Act 2012 (2020 Rev Ed) s 15A.

Principal is impracticable or inadvisable due to pressing concerns. Clearly defined situations wherein insisting on consent would be counterproductive have been listed under the Deemed Consent provision in the Bill."[39]

24 Examples of these situations include where the data fiduciary is required to process personal data in order to comply with court orders or other legal obligations, when responding to a medical emergency, or for employment-related purposes.[40] In other jurisdictions, the lawful basis for handling personal data in these types of situations are not typically categorised as forms of consent (or even deemed consent) but would often be separate lawful bases in themselves and where personal data may be collected or otherwise processed without consent being required.

25 Under the Singapore PDPA, consent from an individual is not required where it is necessary to respond to an emergency that threatens the life, health or safety of that individual or others.[41] "Legitimate interests" is recognised under the Bill but as a situation where consent may be deemed.[42] By contrast, legitimate interests is provided under the PDPA as an alternative lawful basis to consent.[43]

26 The approach taken in the latest Bill is a departure from previous versions. For example, processing personal data related to employment and legitimate interests, inter alia, were grouped "as grounds for processing of personal data without consent" under Chapter III of the previous Bill.[44]

---

39 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at para 10.

40 Digital Personal Data Protection Bill 2022 (India) ss 8(3)–8(7).

41 Personal Data Protection Act 2012 (2020 Rev Ed) First Sch s 2.

42 Digital Personal Data Protection Bill 2022 (India) s 8(9).

43 Personal Data Protection Act 2012 (2020 Rev Ed) First Sch. For the GDPR position, see Regulation (EU) 2016/679 of the European Parliament and of the Council 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 Direct 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Art 6(1)(f).

44 Personal Data Protection Bill 2019 (India) ss 12–15.

V. Security

27 Section 9(3) of the Bill requires data fiduciaries to implement appropriate technical and organisational measures to ensure compliance with the provisions of the Bill. Section 9(4) requires data fiduciaries and processors to protect personal data in its possession or control by implementing "reasonable security safeguards" to prevent a "personal data breach".

28 The Singapore PDPA contains similar requirements through the Protection Obligation, requiring organisations to implement "reasonable security arrangements" to prevent:

> (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
> (b) the loss of any storage medium or device on which personal data is stored.[45]

29 A "data breach" is defined under s 26A and uses identical language as that under the Protection Obligation. In the India Bill, a "personal data breach" is defined in very similar language: "… means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data."[46]

30 In terms of breach notification requirements, the India Bill requires "[i]n the event of a personal data breach, the Data Fiduciary or Data Processor … [to] notify the [regulator] and each affected Data Principal, in such form and manner as may be prescribed".[47] Since a "personal data breach" has been defined broadly, in the absence of any further threshold requirements being prescribed, the notification requirement under s 9(5) may be potentially onerous for data fiduciaries and processors.

31 By comparison, the Singapore PDPA requires "notifiable data breaches" to be notified to the regulator or affected individuals: that is,

45 Personal Data Protection Act 2012 (2020 Rev Ed) s 24.
46 Digital Personal Data Protection Bill 2022 (India) s 2(14).
47 Digital Personal Data Protection Bill 2022 (India) s 9(5).

where the data breach results in (or is likely to result in) significant harm or is (or is likely to be) of a significant scale.[48]

VI. Cross-border data transfers

32 Section 17 of the Bill restricts cross-border data transfers by adopting a "whitelist approach", stating that: "The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified."[49]

33 There are no current indications on which countries may be included in the list or are under consideration by the Indian Government. The Bill is also currently silent on the types of legal mechanisms that data fiduciaries may rely on to facilitate transfers of personal data outside of India. Previous versions of the Bill contained stringent restrictions on cross-border data transfers and localisation requirements for categories of "sensitive personal data" and "critical personal data".[50] These impediments to transfer generated concern from industry, especially in respect of the potential compliance burden involved in meeting such requirements within their business and operational setup.[51]

34 Singapore takes a different approach in the PDPA by prohibiting cross-border data transfers unless the transferring organisations can provide a "standard of protection" to the transferred data that is comparable to the PDPA.[52] Generally, this involves ensuring that the recipient of the personal data being transferred is subject to "legally enforceable obligations" that provide a comparable standard of protection, such as binding corporate rules or appropriate contractual clauses.[53]

---

48 Personal Data Protection Act 2012 (2020 Rev Ed) ss 26A–27D.

49 Digital Personal Data Protection Bill 2022 (India) s 17.

50 See, *eg*, Personal Data Protection Bill 2019 (India) ss 33–34.

51 Aditya Kalra, "US-India Business Groups Plan to Lobby for Dilution of India's Privacy Bill" *Reuters* (18 December 2019) <https://www.reuters.com/article/us-india-dataprivacy-idUSKBN1YM0GL> (accessed 14 May 2023).

52 Personal Data Protection Act 2012 (2020 Rev Ed) s 26(1).

53 Personal Data Protection Regulations 2021 regs 10–11.

VII. Other provisions

A. Significant data fiduciaries

35 The India Bill imposes additional obligations on significant data fiduciaries ("SDFs") under s 11. This concept is not new, having appeared in the preceding Bill in 2021.[54] The provision empowers the Indian Government to designate any individual data fiduciaries or a class of data fiduciaries as an SDF, based on an assessment of at least seven factors such as volume and sensitivity of the personal data collected and processed, or the potential impact of such on India's sovereignty and security.[55]

36 SDFs are subject to three additional requirements that ordinary data fiduciaries are not subject to. SDFs are required to appoint data protection officers, appoint "independent data auditors" to evaluate their privacy compliance programmes, and undertake data protection impact assessments and other periodic audits that may be prescribed under the Bill.[56]

37 The Singapore PDPA does not differentiate between different types of organisations or impose varying or additional compliance requirements as a result.

B. Children's personal data

38 The India Bill contains specific provisions in respect of the processing of personal data of children, defined as any individual under 18 years of age.[57] Section 10 requires data fiduciaries to obtain "verifiable parental consent" before any children's personal data may be processed. Section 10 also contains prohibitions on processing of personal data that is likely to cause harm to a child or any tracking, behavioural monitoring of or targeted advertising directed at children.[58]

39 The Singapore PDPA does not have any specific provisions relevant to children and the collection and processing of children's personal data.

---

54 Personal Data Protection Bill 2019 (India) s 26.

55 Digital Personal Data Protection Bill 2022 (India) s 11(1).

56 Digital Personal Data Protection Bill 2022 (India) s 11(2).

57 Digital Personal Data Protection Bill 2022 (India) s 2(3).

58 Digital Personal Data Protection Bill 2022 (India) ss 10(2)–10(3).

However, the regulator has adopted a "practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf".[59]

C. *Consent manager*

40 The India Bill explicitly allows Data Principals to "give, manage, review or withdraw [their] consent to the Data Fiduciary through a Consent Manager".[60] In turn, a "Consent Manager" has been defined as a "Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform", and is accountable to the Data Principal and acts on behalf of the Data Principal.[61]

41 The concept of a manager for consent is novel. The explanatory note provides further explanation for the use of such managers:

> The proliferation of Digital Economy has meant that the number of organisations one engages with, has increased exponentially. It is not always possible to keep track of the instances in which one has given consent to processing of personal data. Addressing this issue, an ecosystem of consent managers has emerged. A consent manager platform enables an individual to have a comprehensive view of her interactions with Data Fiduciaries and consent given to them. The Bill has recognised Consent Managers.[62]

42 The "ecosystem" could operate over a common network based on specifications set by the Indian Government.[63] MEIT have already issued specifications around user consent management.[64] A framework for

---

59 Personal Data Protection Commission, *Advisory Guidelines on the PDPA for Selected Topics* (17 May 2022) at para 8.6.

60 Digital Personal Data Protection Bill 2022 (India) ss 7(6)–7(7).

61 Digital Personal Data Protection Bill 2022 (India) ss 7(6)–7(7).

62 Explanatory Note, Digital Personal Data Protection Bill 2022 (India) at para 9.

63 Arijita Kakati, "Consent Manager Framework under India's Personal Data Protection Bill" *The Privacy Advisor* (26 January 2022) <https://iapp.org/news/a/consent-manager-framework-under-indias-personal-data-protection-bill/> (accessed 14 May 2023).

64 Ministry of Electronics and information Technology, "Electronic Consent Framework: Technology Specifications, Version 1.1" *Digital Locker Authority*

(*continued on next page*)

certifying new consent managers should follow and an industry of firms offering consent management services may emerge. These trends would follow developments in India's financial sector involving account aggregators to facilitate consented transfer of financial data.[65]

VIII. Conclusion: where to from here?

43 The latest Bill contains many similarities with the Singapore PDPA. Both regimes do not have the concept of "sensitive personal data". Both are consent-based and recognise similar lawful bases for the collection and other processing of personal data (though the India Bill conceptualises "deemed consent" differently).

44 However, the India Bill also contains several provisions that distinguish it from the Singapore PDPA and many other jurisdictions, such as its approach to imposing additional accountability requirements on SDFs and the recognition of the role of consent managers in its digital economy in the future.

45 Public consultation on the Bill closed on 2 January 2023 and the Bill was due to be introduced to Parliament in the second half of its budget sessions commencing 13 March 2023.[66] However, at the time of finalising this article for publication, the Bill is expected to be tabled in Parliament's monsoon session in July 2023.[67] The delay is likely due to the significant

---

<https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf> (accessed 14 May 2023).

65 Arijita Kakati, "Consent Manager Framework under India's Personal Data Protection Bill" *The Privacy Advisor* (26 January 2022) <https://iapp.org/news/a/consent-manager-framework-under-indias-personal-data-protection-bill/> (accessed 14 May 2023).

66 Indu Bhan, "Digital Personal Data Bill to be Introduced in Second Half of Budget Session: Govt to SC" *The Economic Times* (1 February 2023) <https://economictimes.indiatimes.com/news/india/digital-personal-data-bill-to-be-introduced-in-second-half-of-budget-session-govt-to-sc> (accessed 14 May 2023).

67 Krishnadas Rajagopal, "New Digital Personal Data Protection Bill in Monsoon Session" *The Hindu* (12 April 2023) <https://www.thehindu.com/news/national/new-data-protection-bill-likely-to-be-introduced-in-monsoon-

(*continued on next page*)

volume of submissions received during the public consultation period.[68] If the Bill is passed, it will introduce a new regime of privacy obligations in a jurisdiction with at least one billion active users online. Privacy professionals in Singapore will need to assess the extent to which their organisations have interests in India impacted by the Bill. In particular, organisations will need to assess whether they have appropriate and equivalent lawful bases for their processing activities and any potential cross-border transfers.

---

session-in-parliament-centre-to-supreme-court/article66723887.ece> (accessed 14 May 2023).

68 Deeksha Bhardwaj, "Over 20k Suggestions Sent on Data Privacy Law: Officials" *Hindustan Times* (1 May 2023) <https://www.hindustantimes.com/india-news/over-20-000-public-submissions-received-on-controversial-digital-data-protection-bill-set-to-be-introduced-in-parliament-this-year-dataprotection-privacy-india-101682880124389.html> (accessed 14 May 2023).

NO LONGER CHILD'S PLAY: A COMPARATIVE LOOK AT CHILDREN'S DATA LAWS IN SINGAPORE, THE UNITED STATES, EUROPE AND CHINA

Charmian AW[†]
LLB (National University of Singapore);
CIPP/A, CIPP/E, CIPP/US, CIPM, FIP;
Advocate and Solicitor (Singapore)

Sarah BRUNO[‡]
BS (Pennsylvania State University), JD (American University, Washington College of Law);
CIPP/US;
Attorney (District of Columbia, Maryland, California)

Elle TODD[§]
BA (University of Cambridge), GDL (College of Law, London);
Solicitor (England and Wales)

Barbara LI[¶]
LLB (China University of Political Science and Law), LLM (King's College London);
CIPP/E;
Solicitor (England & Wales; China (non-practising))

I. Introduction

1 When it comes to the collection of personal data from children, there are surprisingly still very few laws worldwide that deal exclusively with such kids' online privacy protection. To top it off, the requirements imposed on organisations that process children's data are extremely nuanced and differ from jurisdiction to jurisdiction. As it is neither possible nor helpful to dissect all of the laws pertaining to kids' data across the globe, this article

† Charmian Aw is a Partner with Squire Patton Boggs.
‡ Sarah Bruno is a Partner with Reed Smith.
§ Elle Todd is a Partner with Reed Smith.
¶ Barbara Li is a Partner with Reed Smith.

discusses only several key ones for comparative purposes; namely, those of Singapore, the US, the UK and the European Union ("EU") and the People's Republic of China.

II. The current law in Singapore

2 In Singapore, there are several age thresholds that apply when establishing legal capacity of a child. To be able to enter into a legally valid contract, a child must be at least 18 years of age.[1] Under the Employment Act 1968[2], a child is defined as one below 15 years of age and a young person as one between 15 and 16 years of age for the purposes of according varying protections in respect of the different age groups. A child must be 13 or older to be employed in light work suited to their capacity in a non-industrial undertaking. No child below the age of 13 can be lawfully employed in any occupation (with a limited exception). The Children and Young Persons Act 1993[3] defines a child as one who is below 14 years of age and a young person as one who is between 14 and 16 years of age for purposes of according varying protections under that Act. Some film and video classification ratings set out age thresholds for watching particular content, such as Parental Guidance 13 ("PG13").

3 With regard to data activities pertaining to children, a practical rule of thumb will be applied such that children must be at least 13 years old to be regarded as having the requisite capacity to consent to any processing of their own data.[4] If an organisation has reason to believe that a child is incapable of understanding the nature and consequences of their consent, then it will need to obtain consent from that child's parent or legal guardian on their behalf.[5]

4 All other obligations under the Personal Data Protection Act 2012[6] ("PDPA") including individuals' rights of access, correction and withdrawal

1 Civil Law Act 1909 (2020 Rev Ed) s 35.
2 2020 Rev Ed.
3 2020 Rev Ed.
4 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 17 May 2022) at para 8.6.
5 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 17 May 2022) at para 8.6.
6 2020 Rev Ed.

of consent, and having to notify the Personal Data Protection Commission ("PDPC") and affected individuals of certain specified breaches, will continue to apply. The Protection Obligation, which requires organisations to make reasonable security arrangements to protect personal data which they control or possess, will also apply, save that a higher level of standard would generally be expected if the data involves children. In the PDPC's enforcement decisions of *Re Singapore Taekwondo Federation*,[7] *Re Spring College International Pte Ltd*[8] and *Re Cognita Asia Holdings Pte Ltd*,[9] particular consideration was given to the fact that the personal data affected in the various breaches was that of children and/or students.

III. China

5 Chinese legislators and enforcement authorities have put significant emphasis on the protection of children's personal information and privacy. The legal requirements in China are mainly specified in the Provisions on the Cyber Protection of Children's Personal Information 2019[10] ("PCPCPI") and the Personal Information Protection Law 2021[11] ("PIPL"), and also mentioned by the Minors Protection Law 2021[12] ("MPL") and national guidelines.

A. Personal Information Protection Law

6 The PIPL, which came into force on 1 November 2021, is China's first comprehensive personal data law. All of the obligations to which data controllers are subject under the PIPL apply to the collection and processing of children's personal data. Under the PIPL, the personal information of minors below the age of 14 is deemed as sensitive personal information and subject to more stringent requirements, including having

7 [2019] PDP Digest 247.

8 [2019] PDP Digest 230.

9 [2022] SGPDPCS 14.

10 The Regulations on the Cyber Protection of Children's Personal Information Network (effective 1 October 2019).

11 Personal Information Protection Law of the People's Republic of China (effective 1 November 2021).

12 The Law of the People's Republic of China on Protection of Minors (effective 1 June 2021).

to obtain separate consent from the minors' parents (or other legal guardians) and conducting an impact assessment. Any violation of these requirements will trigger a wide array of administrative penalties including fines of up to RMB50 m or 5% of the company's last annual turnover. The company's senior management is also subject to fines of up to RMB1 m and can be barred from holding senior positions for a certain period of time. With the increased public awareness of privacy laws in China coupled with strong enforcement actions for any violations of the law, non-compliant entities should be aware that they could potentially end up facing civil lawsuits and criminal liabilities.

B. Provisions on the Cyber Protection of Children's Personal Information 2019

7 The PCPCPI specifically focus on the collection and processing of children's personal information via online activities. The obligations of data controllers under the PCPCPI are consistent with those in the PIPL, but the PCPCPI highlights further enhanced compliance requirements ranging from formulating special rules and user agreements for the collection and processing of children's personal information, designating personnel in charge of children's information and establishing stricter controls over access to children's personal data.

C. Other laws, regulations and national guidelines

8 In addition to the PIPL and the PCPCPI, the MPL requires identity verification procedures to be put in place for minors under specific circumstances, such as when they play online games or interact with live-streaming services. The Guidelines for Personal Information Notices and Consent[13] (which are currently in draft form and open for public consultation) also provide further detailed measures and steps that data controllers must follow in verifying the age of their users.

---

13 The Information Security Technology Guidelines for Personal Information Notices and Consent (Draft), which is only available in Chinese, was released for public comment in 2020, but has not yet come into effect. It deals with detailed requirements on notice and consent for all data subjects, and contains a provision with respect to the verification of the age of minors under 14.

IV. Europe and the United Kingdom

9 Kids' privacy rules are increasingly a key area of focus in the UK and EU.

A. General Data Protection Regulation

10 The General Data Protection Regulation[14] ("GDPR") which applied across the UK and EU from May 2018 includes the high-level obligation that children warrant specific protection, and that parental consent is required for individuals below the age of digital consent where consent is the legal basis relied on for the processing.

B. Country-specific codes

11 The UK and various EU Member States have implemented additional guidance or codes regarding the processing of children's data building on the high-level obligations under the GDPR. These include the UK's Age-Appropriate Design Code[15] ("AADC") (which has now been used as a model for California's Age Appropriate Design Code Act[16] ("AADCA")), the Irish Data Protection Commissioner's Fundamentals for a Child-Oriented Approach to Data Processing,[17] the Commission nationale de l'informatique et des libertés' ("CNIL") Recommendations[18] and the Dutch Code for Children's Rights.[19]

---

14 Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

15 Age Appropriate Design Code 2020 (UK).

16 Age-Appropriate Design Code Act 2022 (A.B. 2273).

17 Irish Data Protection Commission, *The Fundamentals for a Child-Oriented Approach to Data Processing* (18 December 2020).

18 Commission nationale de l'informatique et des libertés, *Recommendations on the Digital Rights of Children* (9 August 2021) <https://www.cnil.fr/en/digital-rights-children> (accessed 24 May 2023).

19 University of Leiden & Waag Organisation, *Code Voor Kinderrechten* (commissioned by the Ministry of the Interior and Kingdom Relations) (12 March 2021).

12 As per the United Nations Convention on the Rights of the Child,[20] these cover the protection of children under the age of 18. A common feature across these, again drawing on the Convention, is the need to act in the "best interests of the child". The guidance and rules cover key additional points around: providing understandable and child-friendly transparency and related privacy information; the need to take a risk-based approach to verifying the age of users; preventing the profiling of children; promoting parental controls; the ability of children to exercise their own rights; privacy by design principles (including requiring the highest level of data protection by default and affirming the principles of data minimisation and purpose limitation); and the obligation to carry out data protection impact assessments.

13 The German Interstate Treaty for the Protection of Minors[21] ("JMStV") also has specific rules focusing on age-gating and age-rating content.

C. Online safety

14 Some forthcoming laws which focus on online platforms and safety contain further additional obligations in respect of the protection of children and their privacy.

15 In the EU, the Digital Services Act[22] contains provisions on ensuring a high level of privacy, safety, and security of children, and a prohibition to stop all advertising to children based on profiling, which will apply from 17 February 2024 (and even sooner for very large online platforms).

16 In the UK the Online Safety Bill[23] is still in draft form but it will protect children by, for example, making platforms prevent children from

---

20 Convention on the Rights of the Child (20 November 1989) [UN General Assembly] 1577 UNTS 3 (entered into force 2 September 1990).

21 Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia (2002).

22 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

23 (UK) House of Commons, *Online Safety Bill* (HL Bill 87(Rev)).

accessing harmful and age-inappropriate content and enforcing age limits and age-checking measures.

V. United States

17 As of January 2023, the US has taken a sectoral approach to legislating consumer privacy and has not enacted a single, comprehensive federal law regulating the collection and use of personal information.

18 In respect of data collected from children under the age of 13, however, the US has enacted comprehensive federal legislation, namely, the Children's Online Privacy Protection Act[24] ("COPPA"). In addition, several states have enacted laws that impact the data collected from children, and which serve to supplement the requirements of COPPA. In the following sections, we summarise the requirements of COPPA as well as the state laws that have been enacted which impact the data collected from children.

A. Children's Online Privacy Protection Act

19 Originally enacted in 1998, COPPA empowers the Federal Trade Commission ("FTC") to promulgate regulations colloquially known as the "COPPA rule".[25] It was drafted to serve four primary goals: (a) empower parents to protect the privacy of children online; (b) protect children's safety in their use of online channels; (c) ensure the security of children's personally identifiable information; and (d) require parental consent when collecting personal information from children.[26]

B. What types of websites does Children's Online Privacy Protection Act apply to?

20 COPPA defines a "child" as any person under 13 years of age.[27] COPPA applies to websites and online service operators that are either: (a) directed towards children; or (b) have actual knowledge that a child is

24 15 USC (US) (1998) § 6501–6506.

25 Children's Online Privacy Protection Rule 16 CFR (US) Part 312 (2013).

26 144 Congressional Record 23926 (1998) (Sen Bryan).

27 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.2.

using the site or service.[28] Determining whether a site or service is child-directed can be difficult because it is a subjective standard. FTC guidance notes that operators should consider the subject matter, visual appearance of the websites, age of the models used on the site or whether characters used to promote the site or service typically appeal to children, marketing practices, and empirical data regarding the age of users that use the site or service in determining whether it is child-directed.[29] Child-directed websites are required to treat all users as if they are children and may not employ age-gates to restrict access to some users.[30]

21 Mixed-audience websites – sites that primarily target an audience other than children, but nevertheless present content that attracts children as a secondary audience – may still qualify as a child-directed website if, on balance, the factors mentioned above tend to show that the site or service is likely child-directed. Although sites or services that are directed towards children are not permitted to age-gate their websites in order to avoid complying with COPPA, a mixed-audience website may employ age-gates as a way to differentiate between users that are children and users that are not – and tailor data collection activities accordingly.[31]

C. How do operators of websites and online services comply with Children's Online Privacy Protection Act?

22 The key feature of COPPA is the requirement for operators of online sites or services to obtain "verifiable parental consent" prior to collecting

---

28 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.2.

29 Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section D.1.

30 Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section D.4.

31 Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section D.6.

personal information from children, subject to some limited exceptions.[32] Verifiable parental consent is a burdensome standard, and the FTC has identified several compliant methods sites or services can use to obtain the proper consent, including: providing signed consent forms; having a parent call a toll-free telephone number or video conference line staffed by trained personnel; checking a parent's government issued identification against a database; requiring a parent to answer knowledge-based questions that only a parent would know (*eg*, the parent's driver's license number, social security number, *etc*.); or requiring a parent to provide a credit card or financial account information in connection with a monetary transaction.[33] Given the administrative burden of obtaining verifiable parental consent, many operators choose not to collect personal information from children, or simply avoid collecting data about a user's age to avoid triggering the actual knowledge standard.

23 In addition to parental consent, COPPA also requires operators to post privacy notices that disclose the site or service's practices with respect to children's personal information. The privacy notice must give parents the information necessary to make an informed decision before consenting to collection of personal information from their children. Parent's also have a right to request the site or service delete their child's personal information and prevent further use of personal information.[34]

24 The FTC has maintained that operators must only collect the personal information from a child that is necessary to achieve the stated purpose, and only retain a child's personal information for as long as reasonably necessary to fulfill that purpose.[35] Operators are also prohibited from requiring a child to provide personal information in order to participate in an activity (*eg*, blocking access to a game unless an e-mail is provided).

---

32 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.5.

33 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.5(b).

34 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.4.

35 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.7; *see also* Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section M.

25 The FTC has also made it clear that the security of children's personal information is important. In fact, the FTC has stated that it will take the position that a company is in violation of COPPA's security provisions if the company fails to take reasonable security precautions, regardless of whether an actual breach occurs.[36]

26 Each of these requirements is notable, since the FTC can levy fines for each violation of COPPA up to $50,120.[37]

D. Additional considerations under Children's Online Privacy Protection Rule

27 COPPA provides some exceptions where a child's personal information can be collected without first obtaining verifiable parental consent. The "one-time use" exception allows an operator to collect contact information from a child for the purpose of responding to a specific request from a child. For example, an operator may collect contact information to enter a child into a contest and advise them if they have won or lost, or respond to an e-mail inquiry. The operator may only collect and use the child's personal information for the purpose of responding to the inquiry and must delete the information once the purpose has been fulfilled.[38]

28 COPPA also allows operators to collect persistent identifiers from children (*eg,* Internet Protocol ("IP") addresses and device identifications) under the "support for internal operations" exception. To qualify for this exception, the persistent identifier must be collected for the sole purposes described in the rule, including: maintaining or analysing site functions;

---

36 Commission Chair Lina Khan, FTC Open Commission Meeting (19 May 2022) <https://www.ftc.gov/system/files/ftc_gov/pdf/Transcript-Open-Commission-Meeting-May-19-2022.pdf> (accessed 24 May 2023).

37 Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section B.2.

38 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.5(c)(3); *see also*, Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section J.1.

performing network communications; authenticating users or personalising content (*eg*, choosing the proper language or region); serving contextual advertising or capping the frequency of advertising; protecting the security or integrity of the user, website, or online service; ensuring legal or regulatory compliance.[39] The FTC has clarified that this exception encompasses the following types of activities: intellectual property protection, payment and delivery functions, spam protection, optimisation, statistical reporting and debugging.[40]

29 Both of these exceptions are limited in scope, and businesses should be careful to rely on the exception only in the proper context.

E. California's Age Appropriate Design Code Act[41]

30 In 2022, the California legislature considered and passed the AADCA. The bill was modeled after the UK's Age-Appropriate Design Code and will take effect on 1 July 2024. The AADCA defines a child as anyone under the age of 18 and applies to websites and online services "likely to be accessed by children".[42]

31 The AADCA requires operators to assess whether the design elements or marketing materials are likely to appeal to children, either through the use of child-aged models or cartoon characters, games, or celebrities popular among children. Additionally, the AADCA would require operators to collect empirical data about audience demographics to determine whether a substantial number of children are using the online site or service. Compared with COPPA, the scope of the AADCA is broader and likely

---

39 Children's Online Privacy Protection Rule 16 CFR (US) (2013) § 312.5(c)(7); *see also*, Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section J.5.

40 Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" (July 2020) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (accessed 24 May 2023) at section J.5.

41 Age-Appropriate Design Code Act 2022 § 1798.99.29 *et seq*.

42 Age-Appropriate Design Code Act 2022 § 1798.99.31.

encompasses social media websites, gaming services and streaming content providers, to name a few.

32 The AADCA requires sites and services subject to the law to enable a high level of privacy by default and requires operators to conduct data protection impact assessments prior to the law's effective date, and anytime a new feature or service is developed thereafter. Assessments must include considerations about the type of content that children may be exposed to, whether the feature presents risk of harm or danger to children – including through the use of algorithms, whether the design elements promote extended use of the site or service (*eg,* auto-play features, time-locked rewards and notifications), and whether the targeted advertising methods are likely to result in harm to children. AADCA's harm reduction measures are a unique feature of the law. In certain circumstances the law requires websites or online services to consider the best interests of the child when developing and rolling out new features. Businesses subject to AADCA will also be required to draft privacy notices, terms of service and other important information and disclosures in clear language appropriate for the age of children likely to use the sites or service. Thus, empirical data regarding audience composition is not only important for determining whether the business is subject to AADCA, but also to determine what age groups are using the sites.[43]

F. Emerging trends in federal and state legislatures

33 Federal and state lawmakers are increasingly focusing more attention on children's privacy. At the federal level, lawmakers have initiated formal inquiries into the COPPA safe harbor programs, held hearings on children's privacy legislation, and introduced legislation to expand COPPA's protections to teens. The US Federal Trade Commission ("FTC") initiated proposed rulemaking efforts to modernise and update the COPPA rule in 2019, but has yet to publish a new rule. Members of the Commission have encouraged Congress to pass updated children's privacy legislation, while members of Congress have pushed the FTC to complete the rulemaking process.

---

43 Age-Appropriate Design Code Act 2022 § 1798.99.31.

34 At the state level, several states have introduced their own versions of AADCA which largely mirror the requirements in California.[44] Other states have proposed legislation similar to COPPA, but have increased the age requirements to provide additional protections for children up to 16 years of age. Lawmakers in Virginia are proposing to extend protections under its comprehensive consumer privacy legislation to children under 18. Finally, some states have proposed banning social media use for all children and teens, locking them out of those platforms completely.

VI. Charting Singapore's path forward

35 At the time of writing this article, Singapore has already made significant headway towards strengthening its legal frameworks for the protection of children's data privacy and online safety.

36 In particular, the PDPC has conducted a series of consultations to gather industry feedback on a proposed set of guidelines for the protection of children's data in Singapore. Under these guidelines, there will be an age assurance requirement if any children's personal data is being collected. This will be in addition to a self-declaration of a user's age, and is intended to provide assurance as to whether a user is or is not a child. Needless to say, any collection of personal data for the purpose of ascertaining a user's age must be accompanied by a clear, easy to understand and child-friendly notification of purpose and consent clause.

37 Age assurance can be carried out via two types of methods: age verification or age estimation. Age verification, sometimes known as an age gate, refers to the ascertainment of an individual's age to a high degree of certainty, by checking against data from a trusted third-party source. In Singapore, this could be a person's SingPass records for instance. The implication of such verification is to restrict or deny access, for example, to a digital product, service or content, from those who are not appropriately aged. As for age estimation, as its name suggests, this will involve approximating a user's age or age range based on profiling (*eg,* the usage patterns or behaviour of a user, such as their social media posts) or the use of facial images.

---

44 As of February 2023, Maryland, New Mexico and Oregon have proposed similar legislation.

38 The forthcoming guidelines also propose that a data protection impact assessment be conducted when an organisation processes children's data.

39 Any use of children's personal data should be in the best interests of the child, and not be used to target "harmful content" at the child. Any setting that collects geolocation data of children should be turned off by default. Whilst there is no need to perform a specific age verification or estimation, the organisation should nonetheless use such methods to ascertain if a user is a child or an adult.

40 Safeguards for the protection of minors have also been introduced by way of the Draft Code of Practice for Online Safety and Guidelines for Code of Practice for Online Safety ("Code") issued by the Infocomm Media Development Authority of Singapore ("IMDA"), which is expected to come into force in the latter half of 2023.

41 The Code introduces community standards for the following content categories: sexual, violent, self-harm, cyberbullying, endangering public health, and facilitating vice and organised crime. It protects all users, but with children requires online communication services to provide targeted measures when children access the specified content categories. Depending on age and severity, social media services are to provide safety information, limit exposure, or restrict access altogether. The Code requires user reporting tools and increased accountability.

VII. Concluding remarks

42 At present, there is no international norm or single standard for identifying an adult from a child. Where age verification is mandated, an organisation may be compelled to collect and process additional personal data, and this in turn could increase the risk of online harm that is posed to a child. Even the increasingly common practice of flagging under-aged users could inadvertently lead to the undesirable consequence of attracting unwanted attention and predatory behaviour which targets kid users on online platforms.

43 In this regard, the industry would benefit greatly from regulatory guidance over what constitutes an acceptable age verification method. Illustrations of common scenarios or examples of trusted third-party sources

that organisations can use to verify a user's identity including ascertaining their age will go a long way in providing certainty.

44 Ultimately, however, although the specific rules governing the processing of children's data and requirements may deviate from each other, the fundamental policy objectives that underpin kids' privacy globally remain the same. Just as children are, by their nature, more susceptible to improper use of their data as well as privacy violations, so too must their data be considered more sensitive as to warrant a higher standard of protection. In order to achieve our policy goals, data protection laws must also work in tandem and be aligned with any regulations that safeguard online users, so as to offer holistic protection of what we need to regard as a more vulnerable class of individuals, specifically, children.

A comparison of key United States, United Kingdom, European Union and China kids' privacy requirements					
Issue	**California**	**United States**	**United Kingdom**	**European Union**	**China**
Title	**California Age Appropriate Design Code Act ("AADCA")**	**Children's Online Privacy Protection Act 1998 ("COPPA")**	**UK General Data Protection Regulation ("GDPR")** Age-Appropriate Design Code ("AADC"), being a statutory code which provides more detail on the requirements in respect of the processing of children's data. The (draft) Online Safety Bill proposes to contain specific duties for services likely to be accessed by children, such as	**General Data Protection Regulation ("GDPR")** Various EU Member States have implemented additional guidance that is similar to the UK's AADC, including the Irish DPC's Fundamentals for a Child-Oriented Approach to Data Processing, the CNIL's Recommendations, the Dutch Code for	**Provisions on the Cyber Protection of Children's Personal Information 2019 ("PCPCPI") and the Personal Information Protection Law 2021 ("PIPL")**

			removing illegal content and preventing children from coming across harmful content, carrying out (and publishing) child safety risk assessments and enforcing age-verification measures.	Children's Rights and the Swedish Datainspektionen's Code for Children's and Young People's Rights on Digital Platforms. The German Interstate Treaty for the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag – "JMStV"), which applies to broadcasting and telemedia services, also has specific rules on age-gating content, age-rating content and taking appropriate measures to protect	

				minors from content which may impair their physical, mental or moral development. The forthcoming Digital Services Act ("DSA") will place further obligations and restrictions on platforms accessible to minors, requiring services to have in place appropriate and proportionate measures to ensure a high level of privacy, safety and security for children, as well as an outright prohibition on targeted advertising.

What is the age of a child in the legislation?	Under the age of 18.	Under the age of 13.	Under the age of 18. This is in accordance with the UN Convention on the Rights of the Child. However, AADC also requires companies to think about what is appropriate depending on the age of the child – for example, a five-year-old will need protecting differently to a 16-year-old and will be less capable of understanding choices and data usage. It provides some suggested different age band	Under the age of 18. This is in accordance with the UN Convention on the Rights of the Child. Under the GDPR, for information society services offered directly to a child and the purposes of consent, the processing of the personal data of a child shall be lawful where the child is at least 16 years old (though Member States can provide for a lower age, provided it is not below 13 years).	As per the PCPCPI, under the age of 14. According to the PIPL, a minor is a natural person under the age of 18. Personal information of a minor under the age of 14 is deemed as sensitive personal information and subject to enhanced protection.

			recommendations, but these are not mandatory. In the UK, for information society services offered directly to a child and the purposes of consent, the processing of the personal data of a child shall be lawful where the child is at least 13 years old.		
What services does it apply to?	Online services, products or features which are "likely to be accessed by" children, which means that it is reasonable to expect (based on certain	Websites, mobile applications, Internet of Things ("IoT") or connected products or other online services or platforms that are	The GDPR applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or	Applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or	The collection, storage, use, processing, transfer and disclosure of children's personal information via online or offline activities.

	indicators) that they would be accessed by children, including: (a) being directed to children, as defined by COPPA; (b) being routinely accessed by a significant number of children, based on competent and reliable evidence on audience composition (or is substantially similar or the same as another online service, product or feature determined to be); (c) having a significant child audience based on	"directed to children". Whether a site or service is "directed to children" can depend on a number of factors, including: (a) the subject matter of the site or service; (b) visual and audio content; (c) the use of animated characters or other child-oriented activities and incentives; (d) the age of models; (e) the presence of child celebrities or celebrities who appeal to kids, ads	services to individuals in the UK or monitor their activities. The AADC applies to online services which are "likely to be accessed by" children, which means that the possibility of children accessing the service needs to be "more probable than not".	services to individuals in the EU or monitor their activities. The DSA applies to intermediary services.	

	internal company research; (d) advertising to children; and (e) having design elements known to be of interest to children, including games, cartoons, music and celebrities who appeal to children.	on the site or service that are directed to children; and (f) other reliable evidence about the age of the actual or intended audience.			
What are the requirements on age gating?	A website or online service that is likely to be accessed by children should either estimate the age of child users with a "reasonable level of certainty appropriate to the risks of the business'	A website or online service directed to children must treat all visitors as children and provide COPPA's protections to every such visitor, meaning that the website or service	Under the AADC, a website or online service that is "likely to be accessed by" children should similarly treat all visitors as children and apply the AADC requirements to any data processing (for	No express requirement to age gate under the GDPR itself but this is implicitly necessary to achieve compliance with the requirements to (a) provide heightened	There are no age gating requirements under the PCPCPI and the PIPL. The Minors Protection Law ("MPL") requires identity verification under the following circumstances:

	data management practices", or treat all users as child users by applying the privacy and data protections to everyone.	may not screen users for age. However, if the website or service does not target children and is not intended for children as its primary audience but is deemed to be "directed to children" based on an examination of factors (see above), then an age gate is permitted to screen for users who indicate they are children under 13 and therefore to ensure that the website or service does not collect	which, see below) unless it can separate out adult and child users. There is no requirement to age gate therefore but age gating is one option for ensuring that only adults are using the services, or for separating out child users to apply the AADC requirements to and thereby avoid the restrictions in the AADC having to otherwise be applied to all users.	protections for children, and (b) obtain parental/guardian consent. Some of the Member State codes mentioned above go into more detail in the same way as the UK's AADC. There will be a new Code under the DSA which contains more detail on expectations and standards for age gating/age assurance.	(a) Online games: the service providers shall require the minors to register and log on to online games with their real identity information. (b) Online live-streaming services: the service providers shall not allow the account registration for minors under the age of 16. For minors above the age of 16, the service providers shall verify the identity information of the minors and obtain the consent of their parents or other guardians.

	personal information from those users or else obtains "verifiable parental consent". If the website or online service is directed to children, but not primarily so, it can implement this age gate so long as: (a) it does not collect personal information from any visitor prior to collecting age information, including through the use of cookies; and (b) it prevents the collection, use, or disclosure of personal			The draft Guidelines for Personal Information Notices and Consent require the personal information handler to take reasonable measures to verify the age of the data subject as follows: (a) Where the products or services are not directed to minors such as mobile banking and property leasing, it is appropriate to use less intensive verification methods, for example by way of a pop-up window asking the data

		information from visitors who identify themselves as under age 13 without first complying with the "verifiable parental consent" requirements (see below). A website or online service that is not deemed to be directed to children does not need to have an age gate.			subject if he/she is over 14 years old. (b) Where the products or services such as games, social media and education are directed to minors, a strong verification method, for example requiring the data subject to enter their birthday information or personal identification number, with the caveat that the verification method adopted should not exceed a reasonable limit. Please note that the draft Guidelines are

					still in the consultation phase and not finalised.
What consent is needed from the parent?	The AADCA does not have a parental consent mechanism. Parental consent requirements under COPPA still apply when information is collected online from children under 13.	Operators of a website or online service directed to children must obtain "verifiable parental consent" for the collection, use, or disclosure of personal information from children. There are several methods to obtain verifiable parental consent, and the appropriateness of the method depends on whether the operator will	The AADC is not focused on getting consent from the adult for processing their child's data in the same way as COPPA. Instead, it is essentially about doing less data processing for children who use services and protecting their data more stringently regardless of what the adult says. It would not therefore be possible to simply override the AADC	Under the GDPR, for information society services offered directly to a child, parental/guardian consent is required for individuals below the age of digital consent (*ie*, ranging from 13 to 16 years between Member States), where consent is the legal basis relied on for the particular processing. Organisations must make "reasonable	According to the PCPCPI, the data collector shall inform the child's guardians in a noticeable and clear manner and obtain the consent from the child's guardians. While seeking consent, the guardians shall be given an option of refusal. According to the PIPL, personal information of minors under the age of 14 is regarded as sensitive personal

		disclose children's personal information to third parties, or allow children to make it publicly available, in which case the standard for that which is adequate consent is higher. To obtain the highest degree of flexibility with regard to a child's personal information, the operator could require the parent to: (a) provide a signed consent form; (b) require in connection with a monetary	requirements by getting a parent to agree/waive it. Outside of AADC, consent from a parent is needed where GDPR requires it for online services such as if relying on consent for processing data, for example for direct marketing or for the installation of cookies and the child is under the age of 13. Where parental consent is needed, the AADC advises organisations to collect the minimum amount of 'hard	efforts" to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. The DSA does not contain specific requirements regarding parental consents.	information and collection of such information is subject to separate consent from the minor's parents or other guardians and the data collector is required to conduct impact assessment before collecting sensitive personal information.

		transaction, use of a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (c) call a toll-free telephone number; (d) video conference; (e) provide a form of government-issued identification to be compared against databases of such information; (f) require a parent to answer a series of knowledge based challenge questions; or	identifiers' (such as passport scans or credit card details) and says that if you are using a third-party verification service, you should use 'attribute' systems which offer a yes/no response when asked if an individual is over a given age, or if a person holds parental responsibility over the child.		

	(g) submit a picture of a driver's license or other photographic identification submitted by the parent and then compare that photo to a second photo submitted by the parent, using facial recognition technology. If the operator is only going to use children's personal information for internal purposes (*ie*, no disclosure to third parties and no ability for the child to disclose it to others), then it is			

		also possible to use an "e-mail plus" method of parental consent, which enables the parent to consent in a return e-mail after receipt of direct notice about the operator's privacy practices. Note: There are some exceptions for specific situations.			
What data does it apply to?	The AADCA does not apply to specific types of data, rather, it applies to online services and products or features likely to be accessed by children.	There is a specific list of items of data caught by the legislation. Although the list is enumerated, and therefore defined, it also includes persistent identifiers,	All "personal data" (any information that relates to an identified or identifiable individual) and the "processing" of that personal data (any operation which is	All "personal data" (any information that relates to an identified or identifiable individual) and the "processing" of that personal data (any operation which is	The PCPCPI and PIPL do not have a specific definition for children's personal information. Under the Cybersecurity Law, personal information refers to

		and items that could be construed broadly, including "[i]nformation concerning the child or the parents of that child that the operator collects online from the child and combines with" any of the specifically enumerated items.	performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction).	performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction).	all kinds of information related to an identified or identifiable natural persons recorded by electronic or other means and used independently or in combination with others, including, without limitation, name, birthday, personal identification number, biometric information, home address, telephone number, *etc*. Anonymised information is not regarded as personal information.

What are the information requirements?	Before a covered business rolls out a new feature or product, the business must complete a Data Protection Impact Assessment ("DPIA"). The DPIA should address whether the design of the product or feature is likely to expose children to harmful content, experience, be targeted or exploited by harmful contacts, witness or participate in harmful conduct; whether targeted	Operators must provide both a privacy policy anywhere children's information is collected, and a direct notice to parents. Direct notice to parents of children must include various information including the types of personal information collected, and that parental consent is required and how to provide consent. If the parent doesn't consent within a reasonable time, operators must	Before a covered business rolls out a new feature or product, the business must complete a Data Protection Impact Assessment ("DPIA"). The DPIA must take into account differing ages, capacities and developmental needs of the child. The AADC focuses on making privacy information age-appropriate. There are no new specific items of information that have to be given but AADC means that privacy policies,	Transparency and accountability are particularly important under the GDPR where children's data is concerned. Information should be concise, easily accessible, and should be in such a clear and plain language that the child can easily understand. Although the GDPR does not explicitly consider the processing of personal data of children to be a processing activity that carries a high	The general requirements for protection of personal information and sensitive personal information under the PIPL shall be applicable to children's personal information. In addition, the PCPCPI specifies the following requirements for collection and processing of children's personal information: (a) Operators shall follow the principles of legality, appropriateness,

	advertising or algorithms could harm children; whether automatic playing of media or features designed to increase time spent using the product could harm children; and whether any sensitive personal information is collected or processed. The DPIA should identify material risks to children and create a plan to remediate those risks. Businesses may be required to provide	delete the parent's online contact information from their records. There are strict notice requirements on the information that must be contained in a privacy policy, all operators that are collecting personal information, the types of the child's personal information collected and how it is used, and a description of the parents' rights.	privacy settings and controls and prompts (already required under GDPR) need to be designed to be understandable and child-friendly. This might, for example, include adding in videos, cartoons, infographics, *etc*. It also requires organisations to provide additional "bite-sized" explanations about how they use personal data at the point that use is activated.	risk, the Article 29 Working Party ("Art 29 WP)'s Guidelines on Data Protection Impact Assessment ("DPIA") and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 lists "vulnerable data subjects" (to include children) as one of the criteria that could trigger the need for a DPIA. Like the AADC, the additional EU guidance requires providing	necessity, security, informed consent and specific purpose in the collection and processing of children's personal information. Excessive collection of children's personal information not related to the services provided to children is not allowed. (b) Operators shall formulate special rules and user agreements for protection of children's personal information. (c) Operators shall designate personnel to be in charge of

	DPIAs to the California Attorney General. Covered businesses are also required to: (a) provide terms of service and privacy notices in terms that are capable of being understood by children that are likely to access the service; and (b) provide prominent notices and tools to help children exercise their privacy rights.		understandable and child-friendly transparency and related privacy information and the obligation to carry out DPIAs.	protection of children's personal information. When seeking consent, operators shall give notification on the purpose, scope and method of collection, storage, use, transfer or disclosure of children's personal information, the location and duration for the storage of children's personal information, the security measures adopted, what consequence if the data subject refuses

					to provide children's personal information, channel and method for whistle-blowing, complaints, requests for correction and deletion of children's personal information.
What are the restrictions and obligations on data use?	Websites and services likely to be accessed by children must configure default privacy settings to offer a high level of privacy. Websites and services likely to be accessed by children are prohibited from doing the following:	The focus is on getting parental consent rather than new restrictions on what can be done with data. But the Rule provides some requirements as to how data can be used and accessed, including that operators who	AADC has 15 standards that must be met when processing children's data. These contain various requirements and restrictions, the key ones being: (a) privacy settings must be set at "high privacy" by default;	The GDPR includes the general requirement that children merit specific protection with regards to their personal data, particularly around any marketing and profiling. The additional EU guidance builds on	All the obligations and restrictions under the PIPL shall apply to the collection and processing of children's personal information. In addition, the PCPCPI sets out the following specific obligations for

	(a) using personal information in a way that could be materially detrimental to the child; (b) profiling children by default; (c) using dark patterns to induce a child to provide personal information beyond what is reasonably necessary; (d) collect geolocation information without providing a clear signal that the service is actively collecting such information; and	have collected personal information subject to COPPA must: (a) provide parents with a means of reviewing the personal information collected; (b) take "reasonable" precautions before sharing information with third parties, including periodic monitoring, to confirm that any service providers or third parties with whom the operator shares children's personal information	(b) profiling (for example, for targeted advertising but also for personalisation and anything which is beyond the "core service") should be switched off by default; (c) nudge techniques can't be used – for example, messages that encourage a child to change settings which protect their privacy; (d) data should not be shared unless there is a compelling reason to do so; (e) geolocation should be switched off by default – an	the high-level obligations under the GDPR. Similar to the AADC, they cover key additional points around privacy by design principles (including requiring the highest level of data protection by default and affirming the principles of data minimisation and purpose limitation); the need to take a risk-based approach to verifying the age of users; preventing the profiling of children; promoting parental controls; and the ability of	collection and processing of children's personal information: (a) Operators shall strict control access to children's personal information. (b) Authorisation from appropriate person-in-charge is required before the staff can access children's personal information, which shall be kept on record. (c) Technical measures shall be adopted to avoid making a copy of or downloading

	(e) collect any personal information beyond what is necessary to provide the product or service.	maintain the confidentiality and security of that information; and (c) retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.	obvious sign should be provided to children when location tracking is active; (f) only data which is necessary should be processed, and all processing should be in the "best interests of the child" (which must be a "primary consideration" when designing and developing the service) – this means thinking about access to harmful content, considering their mental health through pause/not having continuous scroll, the potential	children to exercise their own rights. The DSA prohibits advertising to children based on profiling of their personal data.	children's personal information illegally.

			harm of like buttons, etc; and (g) data cannot be used in a way that is detrimental to children's wellbeing.		
Enforcement and penalties	AADCA is enforced by the California Attorney General. There is no private right of action. Penalties range from US$2,500 for negligent violations per affected child, to US$7,500 for intentional violations per affected child.	COPPA may be enforced concurrently by the Federal Trade Commission or other federal agencies and state attorneys general. Penalties of up to US$46,517 per violation may be assessed.	The ICO has powers to impose administrative fines under the UK GDPR of up to £17.5m or 4% of an organisation's annual worldwide turnover, whichever is higher.	The EU GDPR sets a maximum fine of €20m or 4% of annual global turnover, whichever is higher.	The PCPCPI itself does not contain specific penalties, but it refers to other Chinese laws and regulations for enforcements and penalties for non-compliance. According to the PIPL, the Cyberspace Administration of China (CAC) has the power to impose a wide range of

			administrative sanctions on violators. A company can be exposed to a wide range of penalties including request for rectification, suspension of business, shut down of website and online channels, revocation of operating permit and administrative fine up to RMB50m (approximately US$7.2m) or 5% of last year's turnover, whichever is higher. The senior management of the violating company is

				also subject to personal liability of a fine up to RMB1m (approximately US$150,000) and can be barred from taking a senior position for a certain period of time. According to the MPL, handlers of minors' personal information may face penalties including warnings, suspension of business, shut down of website, revocation of operating permit, confiscation of illegal gains and administrative fines

			up to RMB1m (approximately US$150,000). Persons in charge are also subject to fines of up to RMB100,000 (approximately US$15,000). Under the PIPL, violation of personal information protection can also give rise to civil and criminal liability.

PRIVACY-ENHANCING TECHNOLOGIES (PETs) – OPPORTUNITIES & CHALLENGES*

Lanx GOH†
LLB (University of Birmingham), DipSing (National University of Singapore), LLM (Intellectual Property and Privacy Law) (University of California, Berkeley), MSc (Criminology and Criminal Justice) (University of Oxford); CIPM, CIPP/A, CIPP/E, CIPP/US, FIP;
Advocate and Solicitor (Singapore), Accredited Mediator (Singapore Mediation Centre and Singapore International Mediation Institute)

Joshua KOW
LLB (Hons) (National University of Singapore); CIPP/A, CIPP/E, CIPM, FIP, CISSP;
Advocate and Solicitor (Singapore)

I. Introduction

1 Just ten years ago, Internet users worldwide numbered slightly over 2.5 billion.[1] Fast-forward to today, and that already-significant number has since more than doubled – a whopping 5.3 billion people around the globe are online, in part due to greater ease of access to technological gadgets like

* The authors are grateful to Hang Ying Yao for his helpful suggestions and comments on this article. Any views expressed in this article are the authors' personal views only and should not be taken to represent the views or policy positions of their respective employers. All errors remain the authors' own.

† Lanx Goh is the Global Head of Privacy with Prudential and recently selected as Top 10 Guardians of Cyber Space by the Cyber Express. He is also an Honorary Consul of Bulgaria to Singapore, Adjunct Associate Professor with the National University of Singapore, Faculty of Law and Adjunct Lecturer with the Singapore Management University, School of Law. Lanx now sits on the IAPP Asia and CIPP/A Exam Development Advisory Boards, Cyber Express Advisory Board, and IMDA Data Protection Trustmark Standards Development Working Group.

1 Statista, "Number of internet users worldwide from 2005 to 2022 (in millions)" (23 February 2023) <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> (accessed 18 May 2023).

computers and smartphones, as well as continued modernisation of communications networks.[2]

2 The sheer number of users connected to the Internet today has resulted in a corresponding increase in the amount of data, including personal data, being shared and stored online. While products and services that rely on Internet connectivity (*eg*, cloud computing, Internet of Things devices, *etc*) have dramatically improved many aspects of modern living, their normalisation, acceptance and proliferation in both our personal and professional spaces have also made it far easier for organisations to collect, use and disclose personal data.

3 An oft-heard misconception is that increased Internet connectivity always leads to the erosion of individual privacy, and that technological progress and increased digitalisation must always correlate negatively with the protection of personal data. While understandable, this cannot be further from the truth.

4 Despite not being a new concept, privacy-enhancing technologies ("PETs") have gained particular attention in the privacy community in recent years as a promising solution, allowing organisations to harness the benefits of data processing while protecting privacy at the individual level. PETs have also continued to feature in regulatory guidance. In draft guidance released in September 2022, the UK Information Commissioner's Office ("ICO") noted that PETs could "reduce the risk to individuals, while [enabling] further analysis of personal data"[3] and that, by using PETs, one could "obtain insights from datasets without compromising the privacy of the individuals whose data is in the dataset".[4] In February 2023, the United Nations Committee of Experts on Big Data and Data Science for

2 Statista, "Number of internet users worldwide from 2005 to 2022 (in millions)" (23 February 2023) <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> (accessed 18 May 2023).

3 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 4.

4 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 4.

Official Statistics also released its "Guide on Privacy-Enhancing Technologies for Official Statistics", focusing on PETs which protect data during analysis and dissemination of sensitive information so that the benefits of using data for official statistics can be realised while minimising privacy risks to those entrusting sensitive data to National Statistical Offices ("NSOs").[5]

5 Privacy regulators in Asia-Pacific are likewise aware of, and interested in, the use of PETs. In Singapore, the Infocomm Media Development Authority ("IMDA") and the Personal Data Protection Commission of Singapore ("PDPC") launched a Privacy Enhancing Technologies Sandbox[6] on 20 July 2022, to support businesses wishing to pilot projects involving PETs that address common business challenges. These challenges include: (a) identifying common customers in multiple datasets; (b) deriving additional features or attributes of common customers from multiple datasets; and (c) making data available for AI model development and testing.[7] PETs were also a key issue discussed at the 58th Asia Pacific Privacy Authorities ("APPA") forum held in Singapore last year,[8] where it

5 United Nations Committee of Experts on Big Data and Data Science for Official Statistics, *The PET Guide: The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics* (2023) at p 16.

6 Infocomm Media Development Authority, "Privacy Enhancing Technologies (PET) Sandbox" (20 July 2022) <https://www.imda.gov.sg/Content-and-News/Press-Releases-and-Speeches/Press-Releases/2022/IMDA-and-PDPC-launch-Singapore-first-Privacy-Enhancing-Technologies-Sandbox-as-they-mark-decade-long-effort-of-strengthening-public-trust> (accessed 18 May 2023).

7 Personal Data Protection Commission and Infocomm Media Development Authority, "Invitation to Participate in Privacy Enhancing Technology Sandbox 'PET Sandbox'" (20 July 2022) <https://www.imda.gov.sg/-/media/Imda/Files/Programme/PET-Sandbox/PET-Sandbox-CFP.pdf> (accessed 18 May 2023).

8 See Office of the Privacy Commissioner of Canada, "Data protection authorities from Asia Pacific region discuss privacy issues, best practices" (1 December 2022) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/an_221201_appa/> (accessed 18 May 2023) and Asia Pacific Privacy Authorities, "The 58th APPA Forum hosted by the Personal Data Protection Commission of Singapore" <https://www.appaforum.org/forums/communiques/the-58th-appa-forum-hosted-by-the-personal-data-protection-commission-singapore/> (accessed 18 May 2023).

was noted that PETs "[increased] opportunities for business-to-business data collaboration, cross border data flows and development of AI systems".

6 What are PETs, and how can organisations in Singapore harness them to generate business value while complying with the Personal Data Protection Act 2012[9] ("PDPA")? As off-the-shelf PET solutions mature and become increasingly ready for adoption, we note that adopting these technologies is not without challenge – even today, considerable confusion still exists among organisations as to how they may be effectively implemented – as noted by the ICO, "differences between the implementation of a PET in theory and its practical application [and a] lack of appropriate organisational measures can lower or even completely undermine the effectiveness of a PET".[10]

7 This article aims to provide legal and privacy professionals with an overview of PETs and explain how PETs may be used by organisations in a manner that complies with the PDPA, with a particular focus on data sharing and data analytics. We do this with reference to two commonly-cited and easily adoptable PETs: multi-party computation ("MPC") and differential privacy ("DP") respectively, with commentary on the opportunities and challenges that accompany their implementation in specific industries (*eg*, healthcare).

II. Privacy-enhancing technologies and the Personal Data Protection Act

8 Despite their rising popularity, no universally-agreed definition of PETs currently exists. Among prior attempts that have been made at categorising them,[11] PETs generally refer to a set of technologies which allow data *utilisation* while preserving the *security* and *privacy* of personal

9 2020 Rev Ed.

10 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 5.

11 See, for example, Organisation for Economic Co-operation and Development, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches* (8 March 2023) at p 12, and Johannes Heurix *et al*, "A taxonomy for privacy enhancing technologies" (2015) 53 *Computers & Security* 1.

data. Some have aptly described PETs as helping to solve the "privacy-utility trade-off",[12] complementing legal and/or administrative approaches such as the use of agreements between organisations and data processors.

9 For the purposes of this article, PETs may be broadly understood as comprising two main categories – first, those which facilitate *input* privacy (*ie*, allowing two or more parties to submit data into a calculation without the other respective parties seeing the underlying data);[13] and second, those which facilitate *output* privacy (*ie*, concealing sensitive individual data from being identified or re-identified from the disseminated output).[14] The outcome of a successful implementation of any PET, regardless of where or how they are implemented, would therefore be to allow an organisation to derive additional value and insights from personal data in its possession or control, while also complying with its security and privacy commitments (whether ethical, reputational or otherwise) as well as applicable law (*eg*, the PDPA).

10 A wide range of tools, techniques and systems may properly be considered PETs. For example, technologies such as federated learning[15] and homomorphic encryption[16] have been put forward by privacy practitioners and academics alike as viable means to comply with obligations in laws such as the European Union's General Data Protection

12 Katharina Koerner & Brandon Lalonde, "Cheering emerging PETs: Global privacy tech support on the rise" (24 January 2023) <https://iapp.org/news/a/cheering-emerging-pets-global-privacy-tech-support-on-the-rise/> (accessed 18 May 2023).

13 United Nations Committee of Experts on Big Data and Data Science for Official Statistics, *The PET Guide: The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics* (2023) at p 20.

14 United Nations Committee of Experts on Big Data and Data Science for Official Statistics, *The PET Guide: The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics* (2023) at p 21.

15 See, for example, Nguyen Truong *et al*, "Privacy Preservation in Federated Learning: An insightful survey from the GDPR Perspective" (2021) arXiv:2011.05411.

16 See, for example, Marcelo Corrales Compagnucci *et al*, "Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?" (2019) 3 EPLR 144.

Regulation ("GDPR")[17] in highly-regulated industries (*eg*, healthcare and pharmaceuticals). However, as alluded to above, each technology does so in a slightly different way.

11 The aim of federated learning, for example, is to allow multiple parties to train artificial intelligence ("AI") models on their own data, before combining some of the patterns identified into a single, more accurate "global" model without having to share the underlying training data with one another.[18] On the other hand, homomorphic encryption aims to allow computations to be performed on encrypted data without needing prior decryption.[19] This illustrates the importance of identifying the parties and the intended outcome of the processing activity in question before selecting an appropriate PET. There is no one-size-fits-all approach to selecting and implementing a PET and organisations should only adopt PETs which are reasonable and appropriate in the circumstances.[20]

12 From the above, one can also immediately observe how PETs could assist organisations in complying with the PDPA in various ways. Among the various obligations imposed by the PDPA, we submit that the use of PETs is most relevant to the Protection Obligation[21] and Transfer Limitation Obligation,[22] although we acknowledge that organisations can use PETs to comply with other PDPA obligations as well.

---

17 Regulation (EU) 2016/679 of the European Parliament and of the Council 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, OJ L 119, 4.5.2016 at p 1.

18 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 23.

19 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 12.

20 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 17.2.

21 Personal Data Protection Act 2012 (2020 Rev Ed) s 24.

22 Personal Data Protection Act 2012 (2020 Rev Ed) s 26.

13 Section 24 of the PDPA states that:

> **Protection of personal data**
> **24.** An organisation must protect personal data in its possession or under its control by making ***reasonable security arrangements*** to prevent —
> (*a*) ***unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks***; and
> (*b*) the loss of any storage medium or device on which personal data is stored.
> [emphasis added in bold italics]

14 In explaining what constitutes "reasonable security arrangements", the PDPC noted in its Key Concepts Guidelines that security arrangements may take various forms such as administrative measures, physical measures, technical measures, or a combination of these.[23] Although PETs would, as a category, have no difficulty being considered as technical measures, we submit that PETs are potentially administrative measures (*viz*, ensuring that only the appropriate amount of personal data is held)[24] and physical measures (*viz*, implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security)[25] as well. It would be limiting to think of PETs as mere technological solutions when they are in fact much more.

15 Section 26(1) of the PDPA states that:

> **Transfer of personal data outside Singapore**
> **26.**—(1) An organisation must 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***.
> [emphasis added in bold italics]

---

23 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 17.5.

24 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 17.5, administrative measure example 4.

25 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 17.5, physical measure example 6.

16 The PDPC considers the Transfer Limitation Obligation to be a "manifestation of the Accountability Obligation",[26] and subjects organisations to requirements to protect personal data being transferred out of Singapore to a standard that is comparable to that under the PDPA. Depending on how a particular PET is implemented, one might argue that: (a) no *personal* data is being transferred out of Singapore; (b) by virtue of the method of computation, there is no *transfer* out of Singapore; or (c) the standard of *protection* conferred on the personal data by the implemented PET, among other measures, allows for transfer out of Singapore.

17 For completeness, besides the Protection Obligation and Transfer Limitation Obligation, s 11(1) of the PDPA also states that organisations must, in meeting their responsibilities, consider what a reasonable person would consider appropriate in the circumstances. As PET solutions become more commonplace and available, we submit that it is only a matter of time before PET implementation becomes expected and appropriate in various circumstances.

18 MPC and DP, which facilitate input and output privacy respectively, are two effective examples of PETs that can help organisations comply with the Protection Obligation and Transfer Limitation Obligation. When appropriately implemented, both MPC and DP contribute to a high standard of protection[27] and minimise the risk of re-identification and data breaches, while allowing for more effective data analytics to unlock the value of personal data in an organisation's possession or control. We elaborate below.

III. Input privacy – multi-party computation

19 MPC is a cryptographic technique allowing multiple parties to jointly compute a function or receive an output of that computation based on the datasets that they each have, without revealing those datasets to all other parties. In doing so, each party's dataset, which may include personal data of that party, is kept private. However, all parties who are part of the computation benefit from the output of that function.

---

26 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 19.2.

27 In accordance with Personal Data Protection Act 2012 (2020 Rev Ed) s 24.

20 MPC can be utilised by a large group, or as few as two independent parties.[28] Using a simplified example, assume that a group of four individuals (named A, B, C and D respectively) want to know the average annual salary between them, without having to disclose their exact annual salary figures to one another. Their salaries are as follows:

Person A	Person B	Person C	Person D
$60,000	$64,000	$56,000	$72,000

21 Based on the sums above, the average salary of the group is $63,000. This is currently not known to any one participant.

22 Through an MPC algorithm, each party breaks their exact annual salary figures into four random parts (which can include negative amounts). Each broken part is given the suffix 1, 2, 3 or 4, as shown:

Person A	Person B	Person C	Person D
A1: $15,000	B1: $32,000	C1: -$5,000	D1: $80,000
A2: $5,000	B2: $24,000	C2: $31,000	D2: -$10,000
A3: $50,000	B3: -$2,000	C3: $17,000	D3: $4,000
A4: -$10,000	B4: $10,000	C4: $13,000	D4: -$2,000

23 Each party keeps one part to themselves and exchanges the remaining three parts with each other party. In other words, each party will hold on to no more than one part from another party, as shown:

Person A	Person B	Person C	Person D
A1: $15,000	A2: $5,000	A3: $50,000	A4: -$10,000
B1: $32,000	B2: $24,000	B3: -$2,000	B4: $10,000
C1: -$5,000	C2: $31,000	C3: $17,000	C4: $13,000
D1: $80,000	D2: -$10,000	D3: $4,000	D4: -$2,000

24 Each party then adds up all parts that they have, discloses that sum to the group, and together they obtain the average of the four sums:

28 See, for example, the "Millionaire Problem" in Andrew C Yao, "Protocols for secure computations" (1982) *23rd Annual Symposium on Foundations of Computer Science* DOI: 10.1109/SFCS.1982.38.

Person A	Person B	Person C	Person D
$122,000	$50,000	$69,000	$11,000

25 Based on the sums above, the average salary of the group is $63,000. This figure is derived without each party knowing the exact annual salary figures of any other party.

26 By fragmenting their exact annual salary figures, each of the four parties is not able to learn the exact annual salary figure of anyone else in the group. Each party also receives no more than one broken part (which, on its own, is meaningless in relation to another party's exact annual salary figure) from each of the other parties. However, the group is still able to compute their average annual salary.

27 In more complex calculations, public and private keys to encrypt the underlying dataset (both at rest and in transit) as well as more complex algorithms themselves, are used in accordance with the number of parties and the sensitivity of the data being processed. For example, in an implementation of MPC by the Boston Women's Workface Council, more than 100 participating organisations provided inputs and contributed to a spreadsheet containing more than 600 cells of data, with the Council receiving the summation of each cell across all participating organisations.[29]

28 As illustrated above, MPC could also be used in situations where personal data needs to be shared for research or other purposes, but where the parties' underlying datasets are sensitive and cannot easily or legally be shared with one another. For example, separate hospitals may want to collaborate on research using patient data (*eg*, to find out the average age of patients with a certain disease) without disclosing such data (*eg*, the specific age of each individual patient) to the other hospitals. By using an MPC protocol to perform the joint computation, each hospital can obtain the research outcome without further disclosure.

29 United Nations Committee of Experts on Big Data and Data Science for Official Statistics, *The PET Guide: The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics* (2023) at pp 66–68.

29 Although the PDPA does not separately prescribe a closed list of "sensitive personal data" or special category data,[30] the PDPC has indicated that it takes a stricter view when considering a case where the personal data compromised is of a sensitive nature (*eg*, financial or medical data),[31] and that "implementing additional checks and controls when handling sensitive personal data is not a mandatory requirement but one that should be adopted where appropriate".[32]

30 We submit that MPC could, in this case, be such an additional control – the fact that the underlying datasets are not disclosed to the other parties allows each party to prevent further unauthorised access or disclosure of personal data as required under the Protection Obligation, and this mitigates the risk of a personal data breach incident. In the event of any such breach, the personal data that is inadvertently disclosed could also, as a mere part of the original dataset that is likely meaningless by itself, be deemed as less severe in type and nature.[33]

31 As a technique, MPC has been recognised by the European Data Protection Board as forming part of an effective supplementary measure for the purposes of transfer to third countries,[34] subject to appropriate safeguards. This makes it particularly well-suited for collaborative data analytics involving parties in different countries, as the personal data of each party does not necessarily need to "leave" their respective countries of collection and/or origin, but a computation involving all such personal datasets can be provided to all parties. Moreover, if parties to the

---

30 See, for example, the "special categories of personal data" listed in Art 9(1) GDPR.

31 Lanx Goh & Nadia Yeo, "Sensitive Personal Data in the Singapore Context" [2019] PDP Digest 37.

32 Personal Data Protection Commission, "Being Accountable to Stakeholders" (September 2019) <https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/Sept-19/Being-Accountable-To-Stakeholders> (accessed 18 May 2023).

33 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 27.5, where "the type and nature of the personal data affected by the noncompliance by the organisation or person, as the case may be" is a listed factor.

34 European Data Protection Board ("EDPB"), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0)*, adopted on 18 June 2021, at p 34.

computation can demonstrate that *personal* data is not disclosed at all (*ie*, the part of the underlying dataset being disclosed is, by *itself*, not personal data), then arguably personal data protection laws would not even apply. The PDPA defines "personal data" as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

32 Of course, MPC could go wrong if the parties involved in the computation do not have sufficient trust or security measures in place. If, for example, one party is compromised (*eg*, there is over-disclosure on the part of one party to another due to a technical vulnerability or human error) or acts maliciously, then the entire computation could be jeopardised. While not the focus of this article, it is imperative that any implementation of MPC between parties be rigorously tested from a cybersecurity perspective, both before and regularly during use.[35]

IV. Output privacy – differential privacy

33 First developed in 2006,[36] DP is a mathematical framework centred on algorithmically adding noise to datasets, allowing that dataset to maintain its overall usefulness for analysis while protecting the privacy of individuals whose personal data may form part of the dataset being analysed.[37] The purpose of such noise is to limit the amount of information that can be learned about that individual from a dataset, while still allowing other parts of the dataset to be useful for analysis (*eg*, to expand new research opportunities for large data sets that were otherwise too sensitive to

35 *ComGateway (S) Pte. Ltd.* [2017] SGPDPC 19 at [6], [7] and [37(d)].

36 United States Census Bureau, "Comparing Differential Privacy with Older Disclosure Avoidance Models" (12 August 2021) <https://www.census.gov/library/fact-sheets/2021/comparing-differential-privacy-with-older-disclosure-avoidance-methods.html> (accessed 18 May 2023).

37 In its *Guide to Basic Anonymization* (31 March 2022) the Personal Data Protection Commission recognised that differential privacy "involves several concepts, including answering queries instead of providing the anonymised dataset […]" in addition to the points on noise and mathematical guarantees raised in this article. See fn 21, at p 49.

share).[38] Applications of DP have been successfully adopted by a wide range of organisations that publicly disclose statistics and anonymised datasets, including foreign government agencies.[39]

34 As a concept, DP is intended to "[address] the paradox of learning nothing about an individual while learning useful information about a population".[40] Through the introduction of noise into the applicable dataset, DP allows organisations to guard against known and emerging re-identification threats,[41] which may be brought about due to future technological advances as well as other unknown but publicly-available datasets that could be matched against the anonymised dataset.[42] Such noise can be added to the dataset either during aggregation (*ie*, global or centralised DP) or to individual records before aggregation (*ie*, local or decentralised DP),[43] but both types provide similar anonymous information as output. When appropriately implemented, "plausible deniability"[44] can also be achieved, where it is not possible to determine with confidence

38 Organisation for Economic Co-operation and Development, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches* (8 March 2023) at p 18.

39 Personal Data Protection Commission, *Guide to Basic Anonymization* (31 March 2022).

40 Cynthia Dwork & Aaron Roth, "The Algorithmic Foundations of Differential Privacy" (2014) 9(3) *Foundations and Trends in Theoretical Computer Science* 211 at p 5.

41 United States Census Bureau, "Comparing Differential Privacy with Older Disclosure Avoidance Models" (12 August 2021) <https://www.census.gov/library/fact-sheets/2021/comparing-differential-privacy-with-older-disclosure-avoidance-methods.html> (accessed 18 May 2023) at p 2.

42 Personal Data Protection Commission, *Guide to Basic Anonymization* (31 March 2022) at p 25, "Step 5: Manage your Re-Identification and Disclosure Risks".

43 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 30.

44 Cynthia Dwork & Aaron Roth, "The Algorithmic Foundations of Differential Privacy" (2014) 9(3) *Foundations and Trends in Theoretical Computer Science* 211 at p 15.

whether information relating to a specific individual is in the dataset or not.[45]

35 Through the idea of "privacy budgets" which can be allocated to different parts of a dataset or different queries made to the dataset for the purpose of making it harder to identify an individual, the resulting dataset may conceivably not be subject to the PDPA. This is because data that has been anonymised is no longer considered personal data for the purposes of the PDPA.[46] By carefully allocating these budgets, we submit that datasets can become sufficiently anonymised while still allowing useful insights to be gained from the data.

36 By using DP, organisations can ensure that their data analysis and sharing practices comply with the PDPA, while still being able to gain insights from datasets that include personal data. By way of a simplified example, assume that certain researchers want to analyse the effectiveness of a new medication using a dataset comprising medical records of several patients, some of whom have taken the medication and some of whom have not. To better ensure that individuals cannot be identified from the medical records in the dataset, an appropriate amount of noise can be added (*eg*, adding a random number between -3 and 3 to each patient's age, rounding off some but not all of the patients' heights and weights to the nearest multiple of 10, *etc*) using an algorithm before the researchers commence analysis.

37 This makes it much more difficult for the researchers to identify any one particular patient, while still allowing them to draw insights overall about the medication's effectiveness. If appropriately implemented, researchers who know an individual who *may* be in the dataset should also not be able to determine whether that individual is in the dataset or not. In the circumstances, considering the sensitivity of medical records and the

45 UK Information Commissioner's Office ("ICO"), "ICO publishes guidance on privacy enhancing technologies" (7 September 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/> (accessed 18 May 2023) at p 30.

46 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 3.5.

need to accord such medical data a higher standard of protection,[47] implementing DP not only goes towards discharging an organisation's responsibilities under the Accountability Obligation, but also mitigates the penalties that it may receive in the event of an inadvertent breach.

38 To do so, calibrating the privacy budget is crucial. Various calls have been made for policymakers to provide more guidance about the amount of noise that must be introduced.[48] This is because if the privacy budget is set too high (*ie*, too much noise is introduced), the underlying dataset could return inaccurate or biased results, rendering it less useful for analysis. Conversely, if the privacy budget is set too low (*ie*, too little noise is introduced), individuals are far more likely to be identified from their data especially if the querying party has sufficient background information about the individual. Applications of DP should also take into account the fact that multiple repeated queries against the database could reduce the effect of the added noise, and appropriate rate limits should be set if the dataset is intended to be frequently queried by the same users, such as through contractual or other legally-enforceable means.

39 For completeness, DP could also be used in instances of processing where National Registration Identification Card ("NRIC") numbers are necessary to accurately establish or verify the identity of an individual to a high degree of fidelity (*eg*, medical check-ups and reports, but also including insurance applications and claims and disbursements of substantial financial aid),[49] without impacting the overall usefulness of the dataset for analytics purposes.

---

47 *Re Singapore Health Services Pte Ltd* [2019] SGPDPC 3 at [51], where it was held that "medical data is personal data of a sensitive nature which should be accorded a higher standard of protection. The health sector handles some of the most sensitive personal data and patients have the right to expect that their data will be looked after".

48 Organisation for Economic Co-operation and Development, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches* (8 March 2023) at p 17.

49 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers* (31 August 2018).

V. Conclusion

40 Although the PDPC has not issued any specific decisions concerning the use of PETs to date, it is clear that organisations can use MPC, DP, as well as other PETs to use and disclose personal data in a PDPA-compliant manner. This can help to build trust with customers and other stakeholders by demonstrating a commitment to protecting personal data, while also enabling the organisation to leverage personal data for important analytics and decision-making purposes.

41 Over and above mere compliance, organisations that adopt PETs are better placed to extract valuable insights from the personal data that they have, while mitigating both the likelihood and impact of any inadvertent personal data breach incident. MPC and DP, if appropriately implemented, offer promising solutions for organisations across multiple industries.

42 Notwithstanding the focus of this article, it is important to note that MPC and DP are just two of many technologies that could properly be considered PETs, and which organisations can use to demonstrate compliance with the PDPA and other privacy laws. The appropriateness of any one PET over another, for any particular data processing activity, must be evaluated carefully. There is no one-size-fits-all solution. As with any other form of technology, risks and challenges associated with poor implementation could potentially undermine any potential upside.

THE RIGHT OF PRIVATE ACTION – DID ALLOWING EMOTIONAL DISTRESS CREATE REAL RISK?

Alexander YAP Wei-Ming[†]
MA (Oxon);
Advocate and Solicitor (Singapore)

TAY Yong Seng[‡]
MA (Oxon), BCL (Oxon);
Advocate and Solicitor (Singapore)

ANG Ann Liang[§]
LLB (University College London);
Advocate and Solicitor (Singapore)

I. Introduction

1 In our previous article "Civil Proceedings under the Personal Data Protection Act 2012",[1] we discussed considerations relevant to the commencement of civil proceedings under the then-s 32 of the Personal Data Protection Act 2012[2] ("PDPA"), and the District Court decision *IP Investment Management Pte Ltd v Alex Bellingham*[3] ("*Alex Bellingham (DC)*").

2 The then-s 32(1) of the PDPA states: "(1) Any person who suffers loss or damage directly as a result of a contravention [of any provision in Part IV, V or VI by an organisation shall] have a right of action for relief in civil proceedings in a court."[4]

---

† Partner, Allen & Gledhill LLP.
‡ Partner, Allen & Gledhill LLP.
§ Senior Associate, Allen & Gledhill LLP.
1 Wei-Ming Alexander Yap *et al*, "Civil Proceedings under the Personal Data Protection Act 2012" [2020] PDP Digest 154.
2 Act 26 of 2012.
3 [2019] SGDC 207.
4 Personal Data Protection Act 2012 (Act 26 of 2012) s 32(1).

3 Since then, there have been several updates to the law. The right of private action can now be found in s 48O of the PDPA.[5] The case of *Alex Bellingham (DC)* has been appealed to the General Division of the High Court ("High Court"), and thereafter to the Court of Appeal. The High Court released its written judgment on 25 May 2021. The Court of Appeal released its written judgment on 9 September 2022.

4 In this article we summarise the various judgments and discuss whether the right of private action for breaches of the PDPA now constitutes a real risk to organisations in Singapore.

II. *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 – the District Court action

5 In *Alex Bellingham (DC)*, the initial plaintiffs were members of the IP Investment Management Group of Companies (the "IP Group").[6] The defendant, Mr Bellingham, was a former employee of the plaintiffs.[7]

6 During Mr Bellingham's term as an employee of the plaintiffs, Mr Bellingham was involved in marketing an investment fund set up by the plaintiffs, known as the Edinburgh Fund.[8] The Edinburgh Fund was launched to acquire, develop and manage student property in Edinburgh.[9]

---

5 Pursuant to s 15 and s 23 of the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020), which came into effect on 1 February 2021. Section 48O(1) states:

> (1) A person who suffers loss or damage directly as a result of a contravention —
>
> (a) by an organisation of any provision of Part 4, 5, 6, 6A or 6B; or
>
> (b) by a person of any provision of Division 3 of Part 9 or section 48B(1),
>
> has a right of action for relief in civil proceedings in a court.

6 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [3].

7 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [5].

8 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [7].

9 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [8].

7 In the course of Mr Bellingham's work marketing the Edinburgh Fund, Mr Bellingham got to know the investors and prospective investors personally and would spend time interacting with them.[10]

8 Subsequently, Mr Bellingham left the employ of the plaintiffs to join a rival fund, known as Q Investment Partners ("QIP").[11] Knowing that some of the investors were due to exit the IP Group's Edinburgh Fund, Mr Bellingham sent e-mails to three of these investors to: (a) state their impending exit from the Edinburgh Fund; and (b) enquire if they would be interested in new investment opportunities.[12]

9 Following the receipt of these e-mails, the three investors (the "Relevant Investors") contacted the plaintiffs to express their concern about the e-mails.[13]

10 This led the plaintiffs to file the private action under the then-s 32 of the PDPA against Mr Bellingham for breaches of the PDPA, *ie*, that Mr Bellingham had collected, used and/or disclosed personal data about the Relevant Investors without their consent and for using their personal data for purposes other than those which the Investors had previously been informed of.[14]

11 In the course of the action, Mr Bellingham argued that it was the Relevant Investors, and not the plaintiffs, who have standing to sue (the "Standing Argument").[15] Subsequently, one of the Relevant Investors, Michael Reed ("Mr Reed"), joined in as a plaintiff to the suit.[16]

---

10 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [9].

11 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [11].

12 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [12].

13 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [14].

14 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [24].

15 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [25].

16 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [15].

12 Mr Bellingham also argued that he had not acted in breach of the PDPA because:[17]

(a) He had not used the personal data of the Relevant Investors (the "Personal Data Argument").

(b) None of the plaintiffs suffered the requisite loss or damage to have standing to sue (the "No Loss Argument").

(c) Even if the plaintiffs were entitled to sue under the then-s 32 of the PDPA, the plaintiffs should not be granted the reliefs prayed for (the "Relief Argument").

13 The District Court found and held as follows.

14 First, the District Court rejected Mr Bellingham's Personal Data Argument. The District Court found that Mr Bellingham had made use of the following personal data of the Relevant Investors, *ie*, (a) their names; (b) their personal e-mail addresses; and (c) their personal investment activity in the Edinburgh Fund.[18]

15 Mr Bellingham had argued that the names and e-mail addresses of the Relevant Investors were available in the public domain. However, the District Court held that these would have no value to Mr Bellingham if they were not accompanied by the information that these names and addresses were those of persons who had invested in and were about to exit from the Edinburgh Fund.[19] Accordingly, Mr Bellingham had misused personal data.

16 Second, in relation to the Standing Argument, the District Court agreed with Mr Bellingham that the persons entitled to exercise rights of private action under the PDPA are limited to data subjects (in this case the Relevant Investors) and not the IP Group entities. Applying the principles of statutory interpretation, the District Court found that the then-s 32 of

17 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [25].

18 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [28].

19 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [51]–[52].

the PDPA could only be exercised by the data subjects, *ie*, the very individuals whose personal data had been compromised.[20]

17 In the circumstances of the plaintiffs, the IP Group entities had no standing to sue. However, the third plaintiff, *ie*, Mr Reed, was undoubtedly a data subject and therefore had standing to proceed with the action as against Mr Bellingham.[21]

18 Third, in relation to the No Loss Argument, Mr Bellingham argued that Mr Reed had not suffered any requisite loss so as to be entitled to a right of private action. The District Court observed that Mr Bellingham had clearly contravened the PDPA.[22] Having regard to the PDPA's aim of safeguarding individuals' personal data against misuse, and to local and Canadian cases, the District Court held that Mr Reed had suffered the requisite loss.[23]

19 Finally, based on the above, the District Court granted relief to Mr Reed in the form of (a) an injunction to restrain Mr Bellingham from using, disclosing or communicating to any person or persons any personal data belonging to Mr Reed;[24] and (b) directing Mr Bellingham to affirm on affidavit that he had destroyed Mr Reed's personal data in Mr Bellingham's possession.[25]

20 Dissatisfied with the outcome, Mr Bellingham appealed the decision to the General Division of the High Court.

---

20 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [59]–[112].

21 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [113].

22 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [133].

23 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [134]–[141].

24 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [162].

25 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 2017 at [172].

III. *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 – the High Court action

21 The High Court's decision can be found in *Alex Bellingham v Michael Reed*[26] ("*Alex Bellingham (HC)*").

22 On appeal, the High Court affirmed the District Court's finding that Mr Bellingham had misused Mr Reed's personal data and acted in breach of the PDPA.[27]

23 However, the High Court found that Mr Reed had not suffered the requisite loss to have standing to sue under the then-s 32 of the PDPA.

24 The relevant question was whether the term "loss or damage" should be interpreted *narrowly* to refer to heads of loss or damage under common law (pecuniary loss, damage to property, personal injury including psychiatric illness) (the "Narrow Interpretation"), or *widely* to include distress and loss of control over personal data (the "Wide Interpretation").[28]

25 The High Court preferred the Narrow Interpretation.

26 The High Court noted that interpreting "loss or damage" to include loss of personal data would render the very term "loss or damage" otiose, as in every case of contravention of the PDPA there would be loss of control over personal data (the "Wide Interpretation – Loss of Control Argument").[29]

27 Second, in relation to whether distress could constitute sufficient loss or damage, the High Court held that the then-s 32 of the PDPA created a statutory tort.[30] The High Court held that Parliament intended to exclude emotional harm from s 32. The High Court also distinguished the Singapore position from the positions in Canada, New Zealand, Hong Kong, the EU and the UK, as these were driven primarily by the need to recognise the right to privacy.[31]

---

26 [2022] 4 SLR 513.
27 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [39].
28 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [43].
29 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [47].
30 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [49].
31 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [56]–[57].

28 The High Court agreed with the appointed Young *Amicus Curiae* that the PDPA was not driven by a recognition of the need to protect an absolute or fundamental right to privacy, unlike the foreign jurisdictions above.[32]

29 Having regard to the purpose of the PDPA to enhance Singapore's competitiveness and to strengthen Singapore's position as a trusted business hub (as much as it was also the PDPA's purpose to safeguard individuals' personal data against misuse), the High Court noted that the PDPA takes a balanced approach and was not driven by any recognition of the right to privacy as a fundamental right.[33]

30 In the circumstances, the High Court was of the view that the Narrow Position would further the purpose of s 32 as a statutory tort.[34]

31 The High Court also had regard to the Protection from Harassment Act[35] ("POHA"). In relation to the POHA, Parliament had expressly stated that the issue of damages would be left to the courts to decide by applying *common law principles*. The High Court thought it would be strange for Parliament to have a different intention when it came to the PDPA.[36]

32 The High Court then went on to find that, under the Narrow Interpretation, Mr Reed had not suffered the requisite loss or damage for the purposes of s 32. Mr Reed had not suffered any financial loss, psychiatric injury or nervous shock as a result of Mr Bellingham's breaches of the PDPA.[37]

33 In the circumstances, the High Court allowed Mr Bellingham's appeal and set aside the reliefs granted by the District Court to Mr Reed.[38]

34 Mr Reed appealed the High Court's decision to the Court of Appeal.

---

32 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [72].
33 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [73]–[75].
34 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [76].
35 Cap 256A, 2015 Rev Ed.
36 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [77].
37 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [89]–[92].
38 *Alex Bellingham v Michael Reed* [2022] 4 SLR 513 at [93].

IV. *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 – the decision of the Court of Appeal

35 The decision of the Court of Appeal can be found in *Michael Reed v Alex Bellingham*[39] ("*Alex Bellingham (CA)*").

36 At the Court of Appeal, Mr Reed sought the reinstatement of the District Court's orders as against Mr Bellingham. Mr Reed argued that:[40]

> (a) The High Court had erred in preferring the Narrow Interpretation, *ie*, that emotional distress and loss of control are excluded under s 32.
>
> (b) Mr Reed had indeed suffered loss or damage because he had lost control over his personal data, and also because he was emotionally distressed over the misappropriation of data concerning his personal investments.
>
> (c) In this regard, even though the Courts had found Mr Bellingham to be in breach of the PDPA and such finding was not challenged, Mr Bellingham nevertheless refused to undertake not to misuse Mr Reed's personal data in the future.

37 Mr Bellingham maintained his arguments in the High Court. The Attorney-General also intervened to submit that the Narrow Interpretation ought to be preferred, *ie*, s 32 does not recognise emotional distress and loss of control of personal data.[41]

38 Further to the arguments above, the Court of Appeal also sought clarification as to whether Mr Reed could not be found in breach of the PDPA as he was "acting in the course of his employment with an organisation" under s 4(1) of the PDPA.[42] Mr Bellingham submitted that he was so acting. The Attorney-General submitted that principles of vicarious liability ought to be considered.

---

39 [2022] 2 SLR 1156.

40 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [26].

41 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [32]–[33].

42 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [29]–[30].

39 The Court of Appeal noted that there were three issues to be determined:[43]

> (a) whether s 4(1)(*b*) of the PDPA exempts Mr Bellingham from liability (the "Course of Employment Exception");
> (b) whether "loss or damage" in s 32 includes emotional distress or loss of control of personal data; and
> (c) whether Mr Reed suffered emotional distress or loss of control of personal data.

40 In relation to the Course of Employment Exception, the Court of Appeal first rejected Mr Bellingham's interpretation that the relevant provisions of the PDPA (*ie*, s(s) 13 and 18 which Mr Bellingham was found to have breached) applied only to corporate entities and not individuals.[44]

41 The Court of Appeal also held that the Course of Employment Exception did not apply to absolve Mr Bellingham in the present case, and that Mr Bellingham could not rely on such a defence. It was for Mr Bellingham to satisfy the Court that the Course of Employment Exception applied.[45]

42 The Court of Appeal also held that the concept of vicarious liability is distinct and has no application here. The employer's liability under the PDPA is fault based.[46]

43 The Court of Appeal held that the issue of whether an employee acted in the course of his employment for the purposes of the PDPA is a question of mixed fact and law. In this case, there is no evidence that Mr Bellingham acted in the course of his employment and for the purposes of his employment by misusing Mr Reed's personal data. Amongst other things, such misuse took place after Mr Bellingham had left the employment of the IP Group and joined QIP.[47]

44 In relation to the question as to whether "loss or damage" in s 32 can include emotional distress and/or loss of control of personal data, the Court of Appeal held as follows.

---

43 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [35].
44 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [39]–[40].
45 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [45].
46 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [49]–[50].
47 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [51]–[55].

45 The Court of Appeal accepted that s 32 of the PDPA created a statutory tort. However, the Court of Appeal disagreed with the High Court that this is sufficient reason to restrict "loss or damage" to actionable heads of loss or damage under common law.[48]

46 The Court of Appeal distinguished between a statutory tort and a common law tort of breach of statutory duty. In the former, where the statute creating the duty expressly provides a civil right of action for injured parties, the Court of Appeal held that the juridical basis of the action is no longer the common law, but the statute itself.[49]

> (a) For statutory torts which create the right of private action, the scope of that right of action is to be determined first and foremost by the principles of statutory construction. Common law principles are relevant only in so far as the rules of statutory construction permit.[50]
>
> (b) By contrast, for breach of statutory duty, its requirements are determined by common law.[51]

47 The Court of Appeal held that, adopting a purposive interpretation of s 32, "it is plain that emotional distress can found the s 32 action".[52]

48 The Court of Appeal was satisfied that Parliament intended to displace common law that emotional distress is not actionable. Considering the scheme and purpose of the PDPA as a whole, excluding emotional distress as a head of "loss or damage" under s 32 would cut across Parliament's intention to promote the right of individuals to protect their personal data.[53]

49 There is nothing in the language or context that prevents the adoption of the Wide Interpretation insofar as it relates to emotional distress.[54]

50 In this regard, the Attorney-General (and Mr Bellingham) had argued that the Personal Data Protection Commission (the "Commission"), and

---

48 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [62].
49 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [63]–[64].
50 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [65].
51 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [65].
52 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [68].
53 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [77].
54 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [78]–[79].

not the Courts, should be the primary body responsible for determining action to be taken in respect of a breach of the PDPA. The Court of Appeal disagreed. The Court of Appeal held that remedies from the Commission and remedies from the Courts complement each other. A right of private action to the Courts serves a different purpose from a right of complaint to the Commission, and an aggrieved individual should have the choice of which avenue to pursue.[55]

51 The Court of Appeal went on to hold that it is clear that the PDPA intended to safeguard the protection of personal data, and even if there were other interests that have been recognised (*eg*, enhancing Singapore's competitiveness), this should not be misconstrued as evincing an intention to confer weak protections on individuals.[56]

52 While trivial annoyance or negative emotions are not actionable, emotional distress is an actionable head of loss under s 32.[57] Parliament had intended to bring Singapore's standards of protection in line with the key jurisdictions that MICA had studied, *ie*, Canada, New Zealand, Hong Kong, the EU and the UK,[58] and intended robust protection for individuals' personal data.[59] Remedial action under the PDPA must be effective.[60]

53 In other words, restricting s 32 such as to exclude emotional distress would render s 32 denuded of practical use.[61]

54 However, in relation to whether loss of control of personal data (as opposed to emotional distress) is sufficient to ground a claim under s 32, the Court of Appeal agreed with the High Court that accepting so would render s 32, particularly the requirement for "loss or damage" thereunder, tautological. The Court of Appeal declined to recognise loss of control as being sufficient for a right of private action under the PDPA.[62]

---

55 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [81]–[85].
56 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [88].
57 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [93].
58 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [97].
59 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [98].
60 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [99].
61 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [99].
62 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [108]–[111].

55 Having laid down the applicable principles, the Court of Appeal found, on the facts, that Mr Reed's emotional distress satisfied s 32.

56 The Court of Appeal held that the test as to whether emotional distress has been suffered must be anchored in whether the very individual before the court subjectively suffered emotional distress. The Court of Appeal agreed with Mr Reed that a multi-factorial approach should be used, and provided the following list of non-exhaustive considerations:

> (a) The nature of the personal data involved in the breach: for instance, financial data is likely to be sensitive …
> (b) The nature of breach: *eg*, whether the breach of the PDPA was one-off, repeated and/or continuing.
> (c) The nature of the defendant's conduct: for instance, proof of fraudulent or malicious intent may support an inference that the plaintiff was more severely affected … In contrast, an accidental breach by a single typographical error is unlikely to cause cognisable distress … In addition, if the claimant reasonably seeks an undertaking from the defendant not to misuse his or her personal data, but the defendant unreasonably refuses to furnish an undertaking, this is a weighty factor in favour of the existence of emotional distress.
> (d) Risk of future breaches of the PDPA causing emotional distress to the claimant.
> (e) Actual impact of the breach on the claimant.[63]

57 On the facts, taking into account Mr Reed's and Mr Bellingham's conduct (including that there is no reasonable explanation for Mr Bellingham's failure to assure Mr Reed that Mr Reed's Personal Data would be protected), Mr Bellingham's dismissive and cavalier attitude and evasive responses, the fact that investment activity constitutes sensitive financial data, and Mr Reed's reasonable apprehension of further misuse, the Court of Appeal found that Mr Reed did suffer emotional distress that is significant enough to be actionable.[64]

---

63 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [115].

64 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [117]–[133].

V. Discussions and implications

58 The Court of Appeal decision provides robust protection for individuals' personal data.

59 The right of private action under the PDPA should be available to claimants who have suffered pecuniary losses and other heads of loss recognised at common law. In addition, in an appropriate case, a claimant who suffers emotional distress directly due to a PDPA breach may be able to obtain damages and/or an injunction pursuant to the right of private action under the PDPA.

60 However, we would argue that the data protection risk profile for organisations in Singapore has not materially increased following the Court of Appeal decision, for two key reasons.

61 First, the Court of Appeal has addressed the spectre of floodgates by allowing for a nuanced multi-factorial test, and courts may consider, at least for the moment, an essentially unlimited list[65] of factors before coming to a decision. Second, *Alex Bellingham (DC)* was decided in October 2019, more than three years ago, and based on searches via the Singapore Academy of Law's LawNet service,[66] there have been *no* new reported civil proceedings under the then-s 32, or current s 48O, of the PDPA.[67]

62 We should also highlight the following portion of the specific fact pattern, and a factor in the nuanced multi-factorial test, from the Court of Appeal decision. Even if a defendant has breached the PDPA, and a claimant has suffered emotional distress, the defendant is *not* automatically liable.

63 Instead, it is only where a defendant further unreasonably refuses to furnish an undertaking not to further misuse personal data, and behaves in a dismissive manner in relation to data protection concerns made explicit by the claimant, that a defendant was found to be liable. Liability arises

---

65 *Michael Reed v Alex Bellingham* [2022] 2 SLR 1156 at [115].

66 As at 28 February 2023.

67 There appear to have been no reported civil proceedings under the then-s 32, or current s 48O, of the PDPA, except for *Alex Bellingham (DC), Alex Bellingham (HC)* and *Alex Bellingham (CA)*. Some reasons for this are also discussed in our previous article, "Civil Proceedings under the Personal Data Protection Act 2012" [2020] PDP Digest 154, at paras 2, 5–7.

because it is arguable that the risk of repeated future breaches is likely to occur and is left un-remedied by the defendant. An identical situation may perhaps only occur infrequently. If a defendant's breach is inadvertent, it is difficult to imagine why the defendant would refuse such an undertaking and behave in such a manner.

UNDERSTANDING HOW THE PDPA PERMITS ORGANISATIONS TO LEVERAGE ON PERSONAL DATA IN ACHIEVING INNOVATION

Steve TAN[†]
LLB (National University of Singapore), LLM (University College London); CIPP/A

Victoria TAN[‡]
LLB (King's College London)

I. Introduction

1 In today's data-driven and technology-focused world, organisations face an increasing need to leverage personal data to stay competitive and drive innovation. The rapid pace of economic digitalisation underscores the importance of responsible management of personal data. In this context,

---

† Partner and Deputy Head, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. Senior Accredited Specialist in Data & Digital Economy Law. Steve has been appointed Adjunct Professor of the National University of Singapore, teaching "Privacy & Data Protection Law" at the law faculty. Highly regarded for his expertise in data privacy and technology law work, Steve has pioneered several data-protection-related services which organisations have found valuable. Steve has been recognised as a leading lawyer in *PLC Cross-border Media and Communications Handbook, Asia Pacific Legal 500*, *AsiaLaw Profiles*, *Practical Law's Which Lawyer, Chambers Asia Pacific Best Lawyers*, *The International Who's Who of Telecoms and Media Lawyers* and *Who's Who Legal: Data*. Steve was awarded Asian Legal Business's Top 15 Technology, Media and Telecoms ("TMT") Lawyers in 2022. Steve is cited as "one of the best in the field of personal data protection" in *Legal 500* 2017 and as being "one of the gurus in the field of data protection" in *Legal 500* 2019. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

‡ Senior Associate, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. In the course of her practice, Victoria has advised clients on a wide range of transactional and regulatory matters with a particular focus on data privacy, intellectual property and technology law.

the Singapore Personal Data Protection Act 2012[1] ("PDPA") is a crucial piece of legislation that has the twin objectives of safeguarding an individual's personal data and ensuring its proper use by organisations. The data protection obligations, as enunciated in the PDPA, have become conditions or statutory requirements that many organisations are now aware of and which, in the minds of their management, have to be complied with. It is therefore not surprising if organisations form an impression that the PDPA is all about the protection of individuals' personal data and accompanying imposition of restrictions on organisations with respect to personal data processing. These organisations may view the PDPA as limiting their ability to fully utilise personal data, without fully understanding the underlying "DNA" of the PDPA.

2 The PDPA was never intended to be weighted in favour of individuals but had been thoughtfully designed to straddle a middle ground between providing individuals with rights related to the protection of their personal data versus the right for organisations to use such personal data for their commercial activities. This balance of interests is encapsulated in the statutorily enshrined purpose of the PDPA, which is "to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances".[2] In tandem with that latter spirit of balancing rights of an individual versus that of an organisation, the concept of reasonableness forms part of the underlying architecture of the PDPA. In this regard, s 11(1) of the PDPA states that "[i]n meeting its responsibilities under this Act, an organisation must consider what a reasonable person would consider appropriate in the circumstances". The latter is supported by the concept of reasonableness qualifying the data protection obligations, such as the Protection Obligation in s 24 of the PDPA. The PDPA recognises that while it is important to protect personal data, such protection must be reasonable and commercially sensible. If the standard for protection were set too high, it would stymie the innovative use and collection of personal data by organisations, thereby impeding progress and development for industries. Therefore, the reasonableness standard provides for a prescient

1 2020 Rev Ed.

2 Personal Data Protection Act 2012 (2020 Rev Ed) s 3.

and pragmatic approach in the regulation and enforcement of the various statutorily imposed obligations in the PDPA. It therefore can be said that in enacting the PDPA, lawmakers have recognised that personal data is a critical resource for driving a vibrant digital economy and have therefore sought to strike a balance between promoting innovative and effective use of data by organisations, while also enforcing accountability in the management of personal data.

3 This article seeks to provide an ill-understood, but accurate, perspective that the PDPA in fact balances between protecting the rights of the individual and permitting organisations to leverage personal data to achieve innovation.

II. The Personal Data Protection Act's framework for the collection, use and disclosure of personal data to encourage and facilitate innovative uses of personal data by organisations

4 The PDPA is a consent regime data protection law. Operationally, it means that before an organisation collects, uses or discloses an individual's personal data, it requires the consent of the individual unless there is an applicable exception to the requirement of consent under the PDPA ("Consent Obligation").[3] In obtaining such consent from the individual, an organisation is required to notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data ("Notification Obligation").[4] These purpose(s) for collection, use or disclosure of the personal data must be consistent with what a reasonable person would consider appropriate in the circumstances ("Purpose Limitation Obligation").[5]

5 In complying with the Consent Obligation and the Notification Obligation (herein referred to as the "Consent and Purpose Principles"), the PDPA recognises both express and deemed consent. The availability of a deemed consent mechanism is an example of the PDPA seeking to balance the rights of an individual versus that of an organisation seeking to

3 Personal Data Protection Act 2012 (2020 Rev Ed) s 13.
4 Personal Data Protection Act 2012 (2020 Rev Ed) s 14.
5 Personal Data Protection Act 2012 (2020 Rev Ed) s 18.

process personal data for its legitimate business needs. The deemed consent mechanism alleviates the operational difficulties that may be encountered by an organisation in seeking to obtain express consent, and creates statutorily lawful pathways for the organisation to collect, use or disclose an individual's personal data if the circumstances fall within such mechanism. While "consent" is not defined in the PDPA – in contrast with the term "deemed consent" which is expounded upon in the PDPA, such as at s 15 (deemed consent by conduct) – consent generally refers to any agreement to, or acceptance of, the matter which is being consented to.[6] Deemed consent by conduct applies to situations where the individual voluntarily provides his/her personal data to the organisation and such purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances.[7]

6 In a move to accommodate modern commercial arrangements and to support data use for business innovation in an increasingly digital economy, the Personal Data Protection (Amendment) Act 2020 ("Amendment Act") which came into effect in February 2021 expanded the categories of deemed consent under the PDPA to include not only deemed consent by contractual necessity but also deemed consent by way of notification of the purpose of data processing (the latter shall be referred to as "Deemed Consent By Notification"). Deemed consent by contractual necessity recognises the commercial activities of organisations in dealing with contractual transactions with individuals, thus allowing for the transacting individual's personal data to be processed without express consent where it is reasonably necessary to conclude or perform the contract between the individual and the organisation. This permits organisations to be more nimble in handling contractual transactions where personal data of consumers would necessarily need to be collected, used or disclosed, as opposed to seeking to rely on the more operationally onerous express consent route.

7 Deemed Consent By Notification creates a sphere of opportunity for organisations to be able to leverage the personal data of their customers, in

---

6 *Re German European School* [2020] PDP Digest 198 at [12].

7 Personal Data Protection Act 2012 (2020 Rev Ed) s 15(1); Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in Personal Data Protection Act* (revised 17 May 2022) at para 12.20.

seeking to process such personal data without the need for express consent, or for new purposes that previously obtained express consent did not cover. Lest individuals come away with the impression that this opens up a Pandora's box where organisations could in bad faith exploit this new basis for deemed consent, one must not forget that the concept of reasonableness as enshrined in s 11 of the PDPA, coupled with the application of the Purpose Limitation Obligation, continues to regulate and restrict excessive behaviour of organisations. Such regulation and restriction can also be seen by the fact that various conditions have to be met by an organisation should it choose to rely on Deemed Consent By Notification. These include: (a) conducting an appropriate data protection impact assessment to reach the conclusion that the intended processing of the individual's personal data will not have an adverse effect on the individual; (b) taking reasonable steps to notify affected individuals of the organisation's intention to process their personal data in reliance on this concept for specified purposes; and (c) giving such individuals the right to opt out within a certain reasonable period of time. Deemed Consent By Notification as a new basis for deemed consent has been introduced at an apposite time when organisations have been pivoting to embrace the digital economy. Its value can be seen when compared with the obtaining of express consent, which can be time-consuming and challenging for organisations who have to repeatedly engage with consumers to do so and without certainty of a positive response from consumers. This problem is only exacerbated if organisations instead choose to adopt a "kitchen-sink" approach to include broadly worded purposes in their data protection policies and notices to consumers. In such cases, individuals cannot properly ascertain or comprehend purposes for which data is collected which is unlikely to constitute meaningful and valid consent for the collection, use and disclosure of their personal data.[8] Additionally, such an approach may also fall foul of the Purpose Limitation Obligation.

8 Being a consent regime data protection law, it would not be surprising to form the perception that compliance with this basis for processing of personal data presents greater operational difficulties than in other countries where there are alternative bases apart from consent. However, one should

8 Ministry of Communications and Information and the Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 4.

bear in mind that the PDPA has balanced this with the availability of a list of circumstances which can be relied upon by organisations as exceptions to the requirement of consent. This list of exceptions to consent has been further supplemented by new exceptions through the Amendment Act. This framework of exceptions provides for application in situations which facilitate and encourage the innovative use of personal data by organisations.

9 Notable is the business improvement purposes exception ("BIP Exception")[9] to consent. In a nutshell, the BIP Exception permits an organisation to use existing personal data of individuals it possesses, or to obtain individuals' personal data from a related corporation, without the consent of such individuals, provided the purposes of use are: (a) to improve, enhance or develop existing/new goods or services; (b) to improve, enhance, or develop existing/new methods or processes for operations; (c) to learn about and understand the behaviour and preferences of customers; or (d) to identify goods or services that may be suitable for customers, or to personalise or customise any such goods or services for customers. Other conditions would also have to be satisfied. The BIP Exception provides a clear framework for innovative use of personal data of consumers by organisations, that is consistent with the commercial reality of how an organisation or a group or organisations collaborate and share data across business divisions, to further innovation and growth. The BIP Exception and Deemed Consent By Notification framework can be said to facilitate use of personal data by organisations while ensuring that such is balanced against the need to protect individuals whose personal data are being used or processed.

10 Another key exception to consent that was introduced into the PDPA under the Amendment Act is the legitimate interests exception. In order for this exception to apply, an organisation needs to ensure that various conditions are met, including: (a) that the collection, use or disclosure of personal data about an individual is in the legitimate interests of the organisation or another person; (b) that the legitimate interests of the organisation or other person outweigh any adverse effect on the individual; (c) the conduct of a Data Protection Impact Assessment prior to carrying

9 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 5; Second Schedule, Pt 2, Div 2.

out such processing of the individual's personal data; and (d) providing the individual with reasonable access to information concerning the organisation's reliance on this exception.[10] So long as the aforementioned conditions are met, the legitimate interests exception provides organisations with leeway to collect, use or disclose personal data for purposes that are in the interests of the organisation including innovative uses of personal data by the organisation. This exception has the potential to provide organisations with some flexibility in being able to leverage personal data for purposes that are beneficial to the organisation's business and operational activities. An example of this would be the prevention of fraud in the context of an organisation's e-commerce business.

11 Organisations that intend to conduct broader research and development which may not have *immediate* application to their products, services, business operations or customer experience (and therefore may not fall under the BIP Exception) should consider the research exception.[11] This exceptions allows organisations to *use* personal data for research purposes including historical and statistical research if (a) the research purpose cannot be reasonably accomplished unless personal data is provided in an individually identifiable form; (b) there is a clear public benefit to using personal data for research purposes; (c) results of the research will not be used to make any decision that affects the individual; and (d) any publication of the results of the research will not identify the individual.[12] If the organisation wishes to rely on the research exception to *disclose* personal data for a research purpose, the organisation must fulfil the aforementioned conditions and also show that it is impracticable for the organisation to seek the individual's consent for the disclosure.[13] The exception provides businesses with greater flexibility in data collection and usage practices leading to potential new insights and opportunities.

---

10 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 3.

11 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in Personal Data Protection Act* (revised 17 May 2022) at para 12.80.

12 Personal Data Protection Act 2012 (2020 Rev Ed) Second Schedule, Pt 2, Div 3.

13 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in Personal Data Protection Act* (revised 17 May 2022) at paras 12.82–12.83.

12 Another significant exception to the requirement of consent under the PDPA relates to personal data which is publicly available[14] as defined in the PDPA. In construing what is publicly available personal data, it is apposite to note that the PDPC takes a pragmatic approach that so long as the personal data in question was publicly available at the point of collection, organisations will be able to use and disclose personal data without consent under this exception, notwithstanding that the personal data may no longer be publicly available at the point in time when it is used or disclosed.[15] The latter position is consistent with the objective of the PDPA being to facilitate organisations' need to use personal data for lawful business activities, while ensuring that individuals' personal data are accorded a sufficient level of protection.

13 Some countries' data protection laws provide for restrictions on the cross border transfer of personal data out of these countries – in other words, data localisation requirements. Some examples would be China's Personal Information Protection Law and Russia's data localisation law. In a digital economy where personal data courses through the "veins" and "arteries" of many organisations, such personal data constitutes a key asset for organisations, in particular organisations which conduct direct to consumer businesses. The reality of a digital economy is that there is a need for cross border flows of personal data, which will bring about economic growth and facilitate commerce for both organisations and the countries in which such organisations are based. Anathema to the aforesaid would be data localisation requirements where the laws restrict the outward transfer of personal data across borders. The PDPA does not create data localisation requirements. Recognising the continuing need for organisations to protect individuals' personal data, the PDPA provides a framework for organisations to participate in the cross-border transfer of personal data by ensuring compliance with certain requirements. This includes ensuring that the overseas recipient is bound by legally enforceable obligations to provide a standard of protection to the personal data so transferred that is comparable to the protection under the PDPA.[16] As such, the PDPA facilitates organisations' participation in the global economy by not

14 Personal Data Protection Act 2012 (2020 Rev Ed) First Schedule, Pt 2, para 1.

15 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in Personal Data Protection Act* (revised 17 May 2022) at para 12.88.

16 Personal Data Protection Act 2012 (2020 Rev Ed) s 26.

prohibiting the cross border transfer of personal data, and at the same time ensures that individuals' personal data continues to be protected despite such cross border transfer activities.

14 The field of artificial intelligence plays an existential and significant role in enabling innovation in organisations. The PDPC's position with respect to anonymised data is laudable in encouraging innovation in this respect. The nub of this is that personal data, once anonymised, can be used by organisations for their business needs without constraint, as personal data that has been anonymised is no longer personal data, and hence will no longer be subject to the PDPA. The data protection laws and data protection authorities of different countries do not necessarily adopt the same formula for when personal data is considered anonymised. The European General Data Protection Regulation sets a high bar for when personal data is considered anonymised. The approach of the UK's Information Commissioner's Office ("ICO") to the anonymisation of personal data is apposite in this respect. In the Anonymisation Code of Practice, the ICO acknowledges that achieving truly anonymised data can be difficult in practice, and that there is still the risk of re-identification of individuals from supposedly anonymised data.[17]

15 The PDPC takes a commercially sensible approach as to when personal data is considered anonymised. While the PDPA does not specifically define "anonymous data", the PDPC provides guidance that "anonymisation" refers to the process of converting personal data into data that cannot identify any particular individual and, depending on the specific process used, can be reversible or irreversible.[18] Personal data would not be considered anonymised if there is a serious possibility of re-identification of the individual in question, whether from the data itself or from the data matched with other information, while taking into consideration safeguards that may have been put in place to mitigate the risk of re-identification. Through this interpretation of anonymised data, it has made possible the ability to disclose sets of personal data that have been subject to anonymisation techniques to recipient organisations, in order for such recipient organisations to be able to obtain valuable business insights

17 Published in November 2012.

18 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 17 May 2022) at para 3.1.

from such datasets. In fact, one could say that this commercially practical interpretation of anonymisation would increase the protection for individuals with respect to their personal data in the hands of organisations, as organisations would be encouraged to deploy anonymisation techniques to reduce identifiable information into anonymised datasets, instead of seeking to analyse personally identifiable information. The PDPC's balanced approach is testament to its commercial sensibilities and desire to support business innovation by providing greater clarity on how organisations can adopt alternative options of anonymising personal data in order to avoid being regulated under the PDPA for such datasets.

16 Finally, the data protection regime in Singapore boasts of an ecosystem that engenders trust, by consumers, in organisations that have been certified to be trustworthy. In this regard, organisations in Singapore can apply for the Data Protection Trustmark ("DPTM") administered by the Infocomm Media Development Authority. The DPTM is a voluntary certification, which certified organisations can leverage to demonstrate their achievement of accountable data protection practices. The certification provides assurance to consumers that the organisation they are dealing with is compliant with the PDPA. As consumers become increasingly concerned about the privacy and security of their personal data, the DPTM can be an important factor in building consumer trust and increasing the willingness of consumers to share their personal data with such organisations and allowing certified organisations to leverage personal data for innovative uses.

III. Conclusion

17 As shown from the foregoing, the PDPA, while ensuring that personal data is adequately protected by organisations, provides organisations with the ability to carry out the innovative use of personal data to support their business needs and transformation in a digital economy. This mutually beneficial arrangement is a win-win situation for all parties involved.

WHEN DATA TRANSFER BORDERS TIGHTEN: WHAT CAN DATA TRUSTS BRING TO THE TABLE?*

LIM Sui Yin, Jeffrey
LLB (Hons) (Bristol University);
Advocate and Solicitor (Singapore), Barrister-at-law (England & Wales)

LEE Kai Xuan, Samuel
LLB (Hons)

I. Introduction

1 One factor motivating the recent retreat from globalisation,[1] with its apparent emphasis on economic "de-coupling" between geopolitical rivals[2] and the impact on connected economies,[3] is a concern over the potential for

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

1 A different view is that it is not so much a retreat from globalisation but a descent of the rate of globalisation (dubbed "slowbalisation"). Commentators note also that cultural integration (with its concomitant increase in global data flows) continues without deceleration. See The Economist, "Globalisation has faltered" (24 January 2019) <https://www.economist.com/briefing/2019/01/24/globalisation-has-faltered> (accessed 24 May 2023): "A minority of yardsticks show rising integration. … The volume of data crossing borders has risen by 64 times, according to McKinsey, a consulting firm…".

2 One prominent rivalry is that between China and the US, marked by the technological dimensions of competition. See Gavin Bade, "'A Sea Change': Biden reverses decades of Chinese trade policy" *Politico* (26 December 2022) <https://www.politico.com/news/2022/12/26/china-trade-tech-00072232> (accessed 24 May 2023): "In his September speech, Sullivan outlined three broad sectors where the administration would try to stall Chinese development: computing (including chips, quantum computing and artificial intelligence), biotechnology and bio-manufacturing, and clean energy tech."

3 The US-China rivalry also impacts organisations headquartered in other countries, *eg*, A Japanese car maker (Nissan) raised concerns with the proposed sale by its French partner (Renault) in the transfer of intellectual property ("IP") to a Chinese car maker (Geely). See Neil Vinton, "Renault Nissan

(*continued on next page*)

the abuse of data and of technology by the government or commercial organisations of other countries. This motivation has, in some instances, been identified as one that has driven the development of data protection or data privacy law, motivating governments to push forward positions that pose challenges to businesses who need to transfer personal data across borders.[4]

2 Organisations engaging in cross-border data transfers find themselves inadvertently caught up in these developments. There is a need to find legal and governance mechanisms that can help them provide an accountable and practical response. Precisely what response best fits the circumstances would vary according to the type of legislative or policy actions governments put into motion. The range of actions can vary and a full list of the types of such actions is beyond the scope of this article, but some notable types of positions taken by governments include the following (or a combination of them):

> (a) "Hard" data localisation requirements or targeted prohibitions of transfers: Examples of this include proposed bills in some jurisdictions that are explicit in their intention to prevent the flow of data to organisations or to locations considered to be under the sway (or the reach) of governments considered to be geopolitical rivals.[5]

Alliance Framework Deal Includes Stake Rebalancing" *Forbes* (30 January 2023) <https://www.forbes.com/sites/neilwinton/2023/01/30/renault-nissan-alliance-framework-deal-includes-stake-balancing/?sh=144286373b4f30> (accessed 24 May 2023): "One stumbling block for Renault's strategy has been joint IP between Nissan and Renault, which Renault would like to transfer to Ampere and the 'Horse' JV with Geely."

4 The Personal Information Protection Law of the People's Republic of China is reported to be partly motivated by such concerns. See Business Times, "China rolls out new data law over 'national security' (1 September 2021) <https://www.businesstimes.com.sg/international/china-rolls-out-new-data-law-over-national-security-fears> (accessed 24 May 2023): "Beijing has also flagged national security concerns as justification for the law. As Chinese tech firms look to branch out overseas, authorities fear domestic data will end up in foreign hands. … Crucially, organisations and individuals are forbidden to hand over information to overseas law enforcement authorities without Beijing's permission."

5 For example, the US Senate bill for "Protecting Americans' Data from Foreign Surveillance Act of 2022" which was introduced with bipartisan

(*continued on next page*)

Legislation of this nature could include categorising transfers of data to specific categories of recipients or to locations as coming under special treatment (*ie*, with hard limitations or additional controls).[6]

(b) Placing restrictions and controls in the hands of government agencies: This is typically by placing controls over transfers by implementing or requiring that transfers meet with or come under approval or assessment processes. The focus of such assessments or approvals could include a review of national security implications of transfers, leaving government agencies with the discretion to assess and make decisions regarding the implementation of national policies.[7]

---

co-sponsorship on 23 June 2022 seeks to establish certain export controls on personal data of U.S. nationals and individuals living in the United States. The bill would direct the US Department of Commerce to identify categories of personal data that could be exploited by foreign governments and harm US national security if exported, re-exported, or in-country transferred in a quantity that exceeds the threshold established by that department, and envisages imposing licensing requirements in respect of such cross-border data transfers.

6 For example the US bill for "Protecting Personal Data from Foreign Adversaries Act", introduced on 9 January 2023, aims to "regulate or prohibit transactions using mobile applications or software programs that engage in the theft of" or transmission of a user's data "in an unauthorized manner" so as to "provide to a covered country, or covered foreign political party, access to such data", where "covered country" means a Communist country, a foreign adversary; or a state sponsor of terrorism. The bill "covered foreign political part[ies]", with the Chinese Communist Party being specifically singled out.

7 For example, imposing security assessments by agencies, such as in the case of the Personal Information Protection Law of the People's Republic of China where the Cyberspace Administration of China ("CAC") would assess the proposed transfer, particularly if the transfer meets particular threshold criteria. This approach creates dependencies in the way the assessing agencies would operate. See Derek Ho & Mandy Zhu, "China cross-border data transfer mechanisms and its implications" *International Association of Privacy Professionals* (22 August 2022) <https://iapp.org/news/a/china-cross-border-data-transfer-mechanism-and-its-implications/> (accessed 24 May 2023): "The uncertainty, however, is the amount of time it would take for the security assessment process to be completed, especially if the assessment is deemed to be complicated, and with the probable involvement of the national and

(*continued on next page*)

(c) Imposing adequacy standards: These subject transfers to conformity with qualitative factors, requiring organisations to ensure that adequacy requirements are met. This can result in organisations having to conduct multi-factorial transfer assessments or reviews, to ensure that they do not become liable to enforcement action by home regulators or regulators located in business-significant jurisdictions.

3 There is one measure which may usefully feature in any compliance response, although it would not be a cure-all or panacea in all respects, and that is the data trust.

II. Data trusts – stewardship models imposing rigorous legal duties and standards

4 A good working definition of a data trust is provided by the Open Data Institute which defines it simply as "a legal structure that provides independent stewardship of data" in its report of 2019 ("ODI Report").[8] This definition has the value of not confining data trusts to any specific conceptual framework. It would avoid, for example, references to traditional property trust law structures. Instead, the definition distils the primary features of legal oversight that trust law traditionally brought, a point that a detailed legal study on the topic (the "Reed Report"), aptly summarises as follows:

> Trust law is not an appropriate legal structure for data trusts. But the fundamental underlying concept, that those who are stewards of data should be responsible for proper oversight of its sharing and use, is achievable through different legal structures. Both an appropriate corporate structure and a contractual structure can be used to impose the required obligations on data stewards, though the more complex a data trust is (particularly if it will have a changing membership and evolving purpose) the more likely it is to need a corporate structure.[9]

---

provincial-level CAC, State Council authorities and other specialized organizations."

8 The authors are greatly indebted to insight given in the ODI Report. Open Data Institute, *Data trusts: lessons from three pilots* (April 2019).

9 Chris Reed, Queen Mary University of London, BPE Solicitors & Pinsent Masons, *Data trusts: legal and governance considerations* (April 2019) p 8.

5 Indeed, the Reed Report had also considered advantages and disadvantages of various of legal structures which could be used to implement data trusts,[10] and it is noticeable that each sampled form (ranging from traditional trusts, contractual frameworks, corporate models and other legal vehicles) presents its own set of advantages and disadvantages, leading the Reed Report to conclude that bespoke legal structures are needed.[11]

6 Considering data trusts without limiting their form to any specific legal framework is salutary because it allows us to think of data trusts with an open mind, and it gives compliance and legal teams options to consider adjustments and customisations in developing legal structures and arrangements that could be more fit-for-purpose in approaching any particular situation. It is this flexible and adaptable concept of data trusts that this article raises for discussion. To adopt an overly rigid view of what a data trust is would also be to potentially risk delving into conceptual limitations and obstacles that could undermine its utility in addressing issues in cross border transfers.

7 To illustrate, consider the difficulties that could arise if one were wedded to the approach of treating data trusts as needing to conform to the traditional common law trust framework. Those concepts are founded on the recognition of proprietary rights. In such a framework, one immediate problem that we then run into is the question of whether personal data could ever constitute or be recognised as "property", such that a division of property rights (into legal and equitable rights in the traditional sense) can then be relied on to apply specific rights and duties to the actors in the trust (*ie*, settlors, trustees and beneficiaries).

---

10 Chris Reed, Queen Mary University of London, BPE Solicitors & Pinsent Masons, *Data trusts: legal and governance considerations* (April 2019) s 2, pp 14–19.

11 "One important conclusion from our research is that each data trust will need its own, individually designed, legal structure. It is not possible to recommend any single form of legal structure or even to produce a set of templates from which data trusts could choose. This is because a data trust's legal structure needs to be designed so as to accommodate the rights and interests of all potential stakeholders." Chris Reed, Queen Mary University of London, BPE Solicitors & Pinsent Masons, *Data trusts: legal and governance considerations* (April 2019) p 58.

8 If one had to tackle the question of whether (and to what extent) there would be property rights in personal data, one could go down a proverbial "rabbit hole" of legal and policy considerations.[12] So, for example, one question that needs to be addressed is what one means precisely by property rights where the subject matter is data or information. Though one could start with considering the 11 incidents of ownership by the late Tony Honore,[13] that proposition becomes more complicated when one considers that imbibing personal data with property rights would impact the collection, usage or disclosure of personal data by different stakeholders. Some of these complications stem from the nature of personal data when viewed through the lens of seeing it as a resource.[14]

9 For example, in the context of considering whether Non-Fungible Tokens, with their use of unique identifiers and information, could be seen as having property rights, the case of *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")*[15] ("*Janesh*"), involved the court taking on the *Ainsworth* test.[16] The court in that case acknowledged the limitations[17] in applying

12 For reading into the various considerations and implications of treating personal data as property, see Hu Ying, "Private and Common Property Rights in Personal Data" (2021) 33 SAcLJ 173.

13 A M Honore, "Ownership" in *Oxford Essays in Jurisprudence: A Collaborative Work* (Oxford University Press, 1961). The 11 incidents are: the right to possess, the right to use, the right to manage, the right to income, the right to capital, the right to security, the incident of transmissibility, the incident of absence of term, the prohibition of harmful use, the liability to execution and residuary character.

14 One well noted point as conveyed by Hu is that "personal data is non-rivalrous, that is, possession and use of a piece of data by one person does not prevent another person from possessing or using the same data. Moreover a piece of data can often be copied easily and at a relatively low cost. As a result it is often difficult for a person to exclude others from accessing his personal data." Hu Ying, "Private and Common Property Rights in Personal Data" (2021) 33 SAcLJ 173 at para 26.

15 [2022] SGHC 264.

16 *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175. Namely that the subject matter must be "definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability".

17 *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")* [2022] SGHC 264 at [69]:

(*continued on next page*)

such analysis and in doing so it also quoted commentary making the point that:

> … the real objections to treating information as property are twofold. First, the free flow of information is of paramount importance, so informational access should not be curtailed as a general rule. **Second, information has a poor fit with conventional concepts of ownership, title and transfer because of its fluidity and variability in function and conception. These are serious hurdles, but they are by no means absolute impediments.** As alluded to above, the individual's interests in privacy and self-determinacy are significant counterweights that may justify some curtailment of access to information. While it is true that information should not, in general, be privatised, personal data may warrant special treatment as a means of augmenting the data subject's legal rights and control. Of course, information being intangible and non-rivalrous is not, in its natural state, an excludable resource. Such exclusivity, if desired, can only be artificially constructed by legal means.[18] [emphasis in original]

10 Another point to note that is that, as the ODI Report points out,[19] there are other models for sharing or accessing data besides data trusts, *ie*, data cooperatives, data commons, personal data stores and research partnerships. Data trusts are therefore not the only possible solution, but

---

> The Ainsworth test, however, as some may point out, is to some degree circular: Gray and Gray, *Elements of Land Law* (Oxford University Press, 5th Ed, 2009) at p 97. Prof Low also argued that the problem with using the test is that it "mixes up the various meanings which common lawyers give to the word 'property'" notwithstanding the fact that what "may be the subject matter of a trust and what may be the subject matter of a proprietary injunction, is wider than that envisaged by Lord Wilberforce in *Ainsworth*": *Bitcoins as Property* at p 349. Here, I would emphasise that the present case was an urgent ex parte hearing – I therefore did not have the benefit of submissions from the defendant. [emphasis in original]

Citing Kelvin F K Low, "Bitcoins as Property: Welcome Clarity?" (2020) 136 *Law Quarterly Review* 345.

18 *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")* [2022] SGHC 264 at [56], the court quoting Prof Lee Pey Woan from "Personal Data as a Proprietary Resource" in *AI, Data and Private Law: Translating Theory into Practice* (Gary Chan Kok Yew & Yip Man eds) (Hart Publishing, 2021) at p 101.

19 Open Data Institute, *Data trusts: lessons from three pilots* (April 2019) at p 9.

this article takes the view that the potential it has for flexible adaptation does offer hope for a targeted approach to different issues or concerns.

11 Indeed, data trusts have been proposed for various reasons ranging from addressing power imbalances between consumers/data subjects and corporations, to freeing up the use of personal data, to promoting research and development into artificial intelligence solutions.[20]

12 As with those other applications, the use case under consideration here (*ie*, to overcome a trust gap as evidenced in cross data transfer restrictions) relies on the same premise that other use cases for data trusts have also been based on, namely, the framework for stewardship over data sharing (and transfers) and for managing interactions between stakeholders in a way that imposes high standards of conduct and accountability.

III. Key features of data trusts that are salient

13 At the outset, it is also possible identify some of the following key features of a data trust:

> (a) The appointment of stewards of the data, who are independent of the organisations which collect and hold the data, and who administer their roles for the benefit of a particular group of people or stakeholders.
>
> (b) The stewards are expected to execute their roles in reference to parameters and principles set out in a legally binding document such as trust charters. Policies and processes in turn are developed and implemented to give effect to these parameters and principles. Administrative, operational and technological tools would then be customised and focused to ensure the decision making by the stewards is consistent with the charter's mission, values or objectives.
>
> (c) The execution and administration of the trust is done with accountability, such as providing for audits (or certifications),[21] and a degree of transparency (which may include a right of challenge by the

20 See George Zarkadakis, "'Data Trusts' Could Be the Key to Better AI" *Harvard Business Review* (10 November 2020) <https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai> (accessed 24 May 2023).

21 A useful discussion of certification standards for data trusts can be found in Oxford Insights, *Exploring Data Trust Certifications* (April 2019).

stakeholders whose interests are being protected or looked after under the charter).

(d) The use of/reliance on legally enforceable rights and duties in relation to stakeholders, including duties that hold stewards to the discharge of their duties. This can include legal mechanisms such as contracts, reliance on conditional and scoped data subject consents given under the legal framework of data protection or data privacy laws, the law of confidence, intellectual property rights, fiduciary duties, *etc*.

14 Beyond these features, it is possible to see other variations which can speak to the differences of the purposes which data trusts can be applied to, but these could stand as key features which would provide a common basis for consideration when looking into data trusts.

15 The potential for variations themselves shows how, even when adopting these core features, there is room to customise and focus the trust to fit specific needs. For instance, "bottom up" data trusts[22] envision data trusts that are formed by pooling the rights of data subjects and placing them under a data trust to make decisions in relation to the interests of the collective group and meet its agreed purposes or objectives.

16 An example of such a "bottom up" data trust could be where patients suffering the same medical condition might decide to collectivise their rights and participate in research and development with corporations researching therapies for treatment. Collectivising their rights under a trust might then present the corporations with an accessible and manageable single point in handling the data subjects and the data subjects might, in return, receive greater transparency, and exercise controls and access to the research and development.

17 The "bottom up" trust contrasts with "top down" data trusts, which include trusts created by corporations or organisations who are holders of pooled/aggregators of stored data. There, corporations would arrange for their data to be held under a data trust for certain purposes or projects. The

22 See Sylvie Delacroix & Neil D Lawrence, "Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance" (2019) 9(4) *International Data Privacy Law* 236.

trust is used by them to have such data stewarded in a manner providing independent accountability.

18 The flexibility and adaptability of the data trust, with its emphasis on bespoke and customised objectives, policies and parameters, is one of its strengths. This is also why some commentators who have looked at data trusts have looked to it as one of the ways by which organisations can develop early responses to fast-paced changes and build in a forward-looking mindset to managing risks including regulatory risks.[23]

IV. How do data trusts address global cross border transfer risks?

19 The current regimen or prescription of measures to address issues arising under cross border data transfer restrictions includes executing standard contract clauses ("SCCs"),[24] reliance on adequacy determinations (if these are available under relevant laws in the jurisdiction from which personal data is exported), binding corporate rules, data transfer and processing agreements, procuring approvals/assessments, certification and generally satisfying any means testing under certain criteria for particular

23 In Element AI and Nesta, *Data Trusts: A new tool for data governance* (2019), data trusts are discussed as part of the conversation to develop "[n]ew anticipatory models of data governance are needed to co-evolve regulation and technology while protecting and advancing the public interest", the thinking being that this would pave the way for stakeholders in society to a look ahead and avoid having to rely on slow-moving regulation to keep pace with new challenges that emerge from time to time. (Element AI now acquired by Service Now Inc.)

24 This range of standard contract clauses ("SCCs") is interesting, there being distinctly different styles of drafting levels or prescriptiveness – an interesting comparison being between the EU SCCs (see European Commission, "Standard Contractual Clauses (SCC)" (4 June 2021) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> (accessed 24 May 2023)), with the ASEAN Model Contract Clauses (see Association of Southeast Asian Nations, *ASEAN Model Contractual Clauses for Cross Border Data Flows* (2021)).

transfers.[25] None are perfect cure-alls for all situations – the right tool for the right job is the best way to navigate uncertainties.

20 As the anxiety over the *Schrems* series of litigation[26] shows, government sponsored and driven frameworks for the cross-border transfers of personal data can sometimes be subject to developments and changes, which impact (and potentially wrong-foot) compliance programmes[27] that organisations adopt and rely on to address issues. Fundamentally, however, organisations could be seen by sceptical regulators as self-interested and approaches driven by caring for profit margins and managing home regulators or business risks can create set patterns of behaviour that could lock organisations and regulators into a cycle of repeated enforcement actions and mistrust, leading to potentially greater legislative or policy restrictions.

21 This is precisely where data trusts, envisioned as flexible and adaptive frameworks, could play a part. On the one hand, "living" charter documents (or, depending on the legal organisation or framework adapted, constitutional documentation or contractual documentation) could be a key feature of data trusts designed to give organisations access to adaptable governance mechanisms – *ie*, developing data trusts with open-ended governance objectives that can evolve, iterate and quickly adapt to new developments.

---

25 The Singapore Personal Data Protection Regulations 2021 (S 63/2021), Pt 3 is an example of how a range of different routes can be undertaken to clear exports of data.

26 As in the litigation by Maximillian Schrems challenging the EU-US Safe Harbor Framework *(Maximillian Schrems v Data Protection Commissioner* (2015) Case C-362/14) ("*Schrems I*"), and the EU-US Data Privacy Shield (*Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (2018) Case C-311/18) ("*Schrems II*"). The question of whether the replacement for the EU-US Data Privacy Shield, dubbed the "Privacy Shield 2.0" is a matter that could be tested via a future "Schrems III" decision.

27 A fuller discussion of the history of the Schrems cases is outside the scope of this article, but the fact that each decision led to the invalidation of intergovernmental arrangements meant that organisations had to adjust, either undoing earlier assumptions based on past arrangements or looking to set in place new arrangements.

22 A data trust's policies and objectives could, with the proper framing, have an anticipatory element, looking ahead and requiring a renewal/refresh process where solutions and parameters adopted for the transfer can be executed, under appropriate accountability and transparency oversight. In this regard, data trusts would be designed not with closed and exhaustive dictated statements of scope and purpose, but rather with review and renewal processes which are built to allow for adaptation and responsiveness to new developments explicitly recognising that standards and expectations set out in legal and policy requirements must keep pace with developments.

23 When it comes to scoping the data trust, the ODI Report described that (taking into account its observations from data trust pilots it studied) the scoping of a data trust is a phased process envisioning eight key activities, headlined as: aligning the trust to a challenge; researching existing efforts; understanding the ecosystem; engaging data holders, users and beneficiaries; developing use cases; considering data access models; securing funding for co-design; and understanding risks,[28] each of which should be executed "in parallel, iteratively, and inform each other", at the inception of the data trust.

24 These activities need not all be confined to the inception of the trust. Activities such as continuing research into "existing" efforts would require a review over the lifespan on a data trust. Engagement with stakeholders such as data holders, users and beneficiaries could be undertaken regularly and periodically to gather feedback and manage "on-the-ground" issues. Reviewing the ecosystem should ideally be done regularly and iteratively, if only to keep track of changing conditions under which the data trust operates. Reviewing data access models would certainly be a key step in ensuring that the purposes of the data trust are being properly and effectively implemented. Properly designed data trusts with such adaptability could in turn offer a responsive and effective solution to evolving standards and parameters concerning cross-border data transfers.

25 In the case of executing or procuring data transfer agreements or assessments, a key issue that comes up is accountability for the potential for personal data to be accessed by a (foreign) governmental authority, and what rights there would for organisations to receive notifications for such

28 Open Data Institute, *Data trusts: lessons from three pilots* (April 2019) at pp 15–17.

access, and also what remedies or opportunities there would to challenge them. At the heart of such concerns is the need to foster trust and build confidence that data holders have appropriate governance mechanisms in place to resist inappropriate collection, use or disclosure of personal data, whether by foreign governments or by other third parties.

26 If decisions in reviewing access and transfer decisions included duties of loyalty, prudence, duties not to act in conflicts of interest, *etc*, (to the extent that these are properly articulated within the data trust's legal documentation and made part of stewardship arrangements) this could provide a basis for showing that an independent and reliable arrangement is available for reviewing cross-border data transfers.

27 Indeed, the introduction of fiduciary duties through the use of data trusts mirrors the impulse to introduce fiduciary duties occasionally seen through proposals over data privacy or data protection legislation. For instance, the proposal for the Data Care Act in 2021[29] in the US aimed to impose duties of care, loyalty and confidentiality. That bill looked to introduce a duty of "loyalty", and would have imposed it as a consideration over various stakeholders as a matter of general application. Such an approach would have wide implications across many organisations and stakeholders.

28 These proposals are part of a larger discussion in some circles about whether to introduce fiduciary duties as a replacement or enhancement to the "notice and consent" framework approach to privacy law, as has been mooted by scholars[30] and is seen by some as a way to provide stronger

---

29 Data Care Act of 2021 (US) S. 919 (117th). See, § 3b(1) on the duty of care, § 3(b)(2) on the duty of loyalty, and § 3(b)(3) on the duty confidentiality.

30 Neil Richards & Woodrow Hartzog, "A Duty of Loyalty for Privacy Law" (2021) 99 *Washington University Law Review* 961. The writers give further details to the duty of loyalty as follows:

> The duty of loyalty has its roots in other areas of law which address self-dealing under Anglo-Saxon common law and previous work by other scholars on the concept of 'information fiduciaries'. The duty of loyalty does not aim as high or impose as stringent a standard as a fiduciary duty (usually seen in trust arrangements, corporate directorship arrangements, *etc*), and is calibrated to be of a lower order of stringency, acknowledging the otherwise deterrent impact of costs on an organisation looking to comply. The duty aims at addressing the 'risk of opportunism' by

(*continued on next page*)

controls that bring data privacy law closer to the spirit of the Fair Information Practice Principles which some commentators see as having eroded by the way in which certain legal works have evolved.[31]

29 The widespread adoption of data trusts would help to pre-empt such proposals and allow industries to evolve solutions that address issues of mistrust that are more tailored and individually customised to specific risks.

30 Where legislative proposals are issued for the enactment of "hard" cross-border data transfer restrictions, data trusts could also, as part of its implementation to meet trust purposes, look to federate data holder and data access arrangements. The stewards in a trust arrangement may also look to other solutions, directing data holders to undertake specific arrangements that could settle local requirements.

31 Other options in shaping data trusts could be tweaked to address political scepticism and the climate of geopolitical suspicion. This article will not delve into them but a short summary of these include:

(a) appointing trusted and respected individuals to act as stewards;

(b) locating the headquarters or administrative organs (if not the infrastructure data) of the data trust in geo-politically "neutral" territories with reputable legal systems; and

(c) developing implementation models (data storage and control models) which a data trust could manage and develop independently or with data holders.

---

organisations who collect data by prohibiting the use of tools or processing in a way that conflicts with a 'trusting party's' (consumers, or persons who are placed in disadvantageous reliance on the organisation to conduct itself) best interests. In short, it makes the organisation responsible for constraining its own activities and paying heed to the vulnerabilities and dependencies of the consumer/data subject. Loyalty does not mean 'obedience' to an inferred instruction or interest of the consumer/data subject, but rather the 'best interests' of the vulnerable trusting party. This approach would force organisations to eschew manipulative behaviour, attempts to procure mandates for 'obedience' via notice-and-consent regimes which are considered flawed due to dark patterns, asymmetrical capacities to manage effective choice as between organisation and individual.

31 Fred H Cate, "The Failure of Fair Information Practice Principles" in *Consumer Protection in the Age of the Information Economy* (Routledge, 2006).

V. Conclusion – data trusts would be part of larger solutions

32 As at the time of the writing of this article, recent developments included the conclusion of US Congressional hearings in relation to the Chinese social media platform TikTok,[32] where, among other matters, the representative from TikTok, Mr Chew Shou Zi, a Singaporean, described Project Texas, a project of TikTok intended to address data protection and national security concerns with US agencies, including the Committee on Foreign Investment in the United States ("CFIUS") of which a key feature include oversight of the data of US residents, and which involves storage of that data in the US. Whilst the nature of oversight is not explicitly a data trust, it does nevertheless attempt to build stewardship and governance over data – functionally, one of the aims of data trusts. The parallels include the appointment of trusted stewards and individuals who will provide controls or barriers to unauthorised access in accordance with mandates.

33 Leaving aside political and politically-motivated commentary, it is noteworthy that the intent of establishing legal and operational controls over access and use of personal data to address threatened or actual legal action is a key step that organisations are indeed looking to establish as a means of addressing concerns of external stakeholders. Data trusts naturally fit the bill for tools to be used to establish such controls.

34 Additionally, privacy enhancing technologies or approaches to data governance which prevent or avoid reliance on the transfer of personal data across borders, and technologies such as federated learning or data management approaches involving in-place integration, are also providing different means to address data protection concerns that would help deal with concerns regarding cross-border transfers. These additional and continued developments in these technologies, and their growing sophistication, can present opportunities and practical means and approaches to supplement or reinforce legal and governance oversight mechanisms.

35 It is certainly not this article's intention to argue that data trusts would be a complete and comprehensive solution to dealing with barriers

32 The full video of the hearing before the US House Energy and Commerce Committee can be found at <https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms>.

being erected over the flow of personal data due to geopolitical rivalries and tensions. Some issues or concerns that drive such barriers are fundamentally political in nature, with underlying social, economic, cultural and technological tensions operating at scales that are far more profound than can be addressed by any single legal tool or framework.

36 It is also acknowledged that data trusts are not simple arrangements to execute. They take specialised skills, foresight and investment in resources and time to ensure that they are properly established and can work accountably to address the very risks they are meant to deal with. This can include investment in infrastructure and skills, technological solutions and the provision of resources (with the accompanying question of financing) that would need to be addressed before realising the trust.

37 That said, if we have clearly entered a new age of "slowbalisation" marked by greater distrust, it could be argued that the data trust presents one of various tools and options that organisations may have at their disposal to navigate a world fraught with political tension and legal risks. Whilst data trusts would not take an organisation to complete the journey of acquiring trust with different governments, it may at least be argued that "a little data trust could go a long way".

YEAR-IN-REVIEW: PERSONAL DATA PROTECTION COMMISSION'S DECISIONS IN 2022

LIM Chong Kin[†]
LLB (Hons), LLM (National University of Singapore);
Advocate and Solicitor (Singapore); Solicitor (England and Wales)

Anastasia Su-Anne CHEN[‡]
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

Mark YEO[§]
LLB (Hons) (London School of Economics and Political Science);
Advocate and Solicitor (Singapore)

I. Introduction

1 2022 marked a significant year for data protection in Singapore. With the higher maximum financial penalties for breaches of the Personal Data Protection Act[1] ("PDPA") coming into effect from October 2022, the impetus for organisations to ensure compliance has taken on renewed importance.

2 At the same time, the Personal Data Protection Commission's ("PDPC's") enhanced powers to accept voluntary undertakings as an enforcement measure has also provided organisations able and willing to adopt prompt remedial measures with an avenue to achieve more satisfactory regulatory outcomes arising from data breaches.

---

† Managing Director (Corporate & Finance), Head (Telecommunications Media & Technology) and Co-Head (Data Protection, Privacy & Cybersecurity), Drew & Napier LLC; Co-Head, Drew Data Protection & Cybersecurity Academy. See also: <https://sg.linkedin.com/in/chong-kin-lim>.

‡ Director (Data Protection, Privacy & Cybersecurity), Drew & Napier LLC. See also: <https://sg.linkedin.com/in/anastasiasuannechen>.

§ Senior Associate (Data Protection, Privacy & Cybersecurity), Drew & Napier LLC. See also: <https://sg.linkedin.com/in/mark-yeo-0b8aab6>.

1 2020 Rev Ed.

3 This article will review the PDPC's enforcement decisions and undertakings accepted in 2022, with a view to identifying recurring challenges faced by organisations in ensuring compliance and best practices in data breach response.

II. Accountability Obligation

4 As with previous years, the PDPC continues to emphasise the importance of organisations demonstrating accountability by putting in place clear policies, procedures and practices governing the handling of personal data, and ensuring that all employees are aware of their responsibilities in data protection.

5 At the most basic level, organisations must develop and implement policies and processes for handling personal data and designate at least one individual responsible for overseeing data protection responsibilities and ensuring compliance with the PDPA.[2] Regrettably, despite the PDPA being more than a decade old, some organisations continue to be found wanting in their basic data protection awareness. For instance, in *Re ACL Construction (S) Pte Ltd*[3] ("*ACL Construction*"), investigations following a data breach revealed that the organisation had neither a Data Protection Officer nor any data protection policies in place whatsoever. The organisation was thus found in breach of the Accountability Obligation.

6 While employees handling personal data or information technology ("IT") systems may require more in-depth training on personal data protection, organisations should remain mindful that this does not negate the need for a baseline standard of data protection training and awareness across the board for all employees. This was illustrated in *Re PINC Interactive Pte Ltd*[4] ("*PINC Interactive*"), where the organisation sought, in its representations to the PDPC, to distinguish between its "technical" and "non-technical" staff. The organisation argued that its team lead's onboarding briefing to "technical" staff covering the IT systems, branch creation rules and coding standards constituted data protection policies for the purposes of the Accountability Obligation. This distinction was rejected

2 Commonly referred to as a Data Protection Officer.
3 [2022] SGPDPCS 2.
4 [2022] SGPDPC 1.

by the PDPC. In finding the organisation in breach, the PDPC stressed the critical role that data protection policies and practices play in accountability by increasing all employees' awareness and ability to protect personal data by enabling them to recognise a matter as one involving data protection.[5]

III. Consent Obligation

7 A key obligation of the PDPA is that organisations collect, use or disclose personal data only for the purposes which an individual has given his/her consent to (subject to statutorily prescribed exceptions). To be able to demonstrate compliance with this requirement, it is important for organisations to obtain and retain written documentary evidence of consent.

8 Where personal data is obtained from other sources/organisations, reasonable due diligence should be conducted to verify that due consent has been obtained in respect of that personal data. The perils of failing to do so were illustrated in *Re Ngian Wen Hao Dennis*[6] ("*Ngian Wen Hao Dennis*"), where an insurance financial adviser leaving the industry ("D") sold his client list to two other insurance financial advisers ("M" and "W") containing the personal data of approximately 1,000 clients. However, D had failed to notify his clients and obtain their consent to the disclosure of their personal data to other insurance financial advisers.[7] Though M and W claimed they had relied on D's verbal assurances that D had informed his clients of the change in their insurance financial adviser, the PDPC found that M and W had failed to take reasonable steps to verify from D that there had, in fact, been proper notification to and consent from the clients for the disclosure of their personal data, such as by obtaining from D a sample of the written notifications and consent. Accordingly, D, M and W were all found in breach of the Consent and Notification obligations.[8]

---

5 *Re PINC Interactive Pte Ltd* [2022] SGPDPC 1 at [13]–[16].

6 [2022] SGPDPCS 9.

7 *Re Ngian Wen Hao Dennis* [2022] SGPDPCS 9 at [6].

8 *Re Ngian Wen Hao Dennis* [2022] SGPDPCS 9 at [11]–[12].

IV. Protection Obligation

A. Password policy – a key IT policy

9 Despite the growing availability of other authentication methods,[9] passwords remain a primary method adopted by organisations in securing personal data. It is therefore unsurprising that the PDPC continues to emphasise the importance of robust password policies as a key plank of compliance with the Protection Obligation.[10] As the following cases illustrate, it is not merely sufficient for stringent password requirements to be imposed – these should be documented in a written password policy which is disseminated to employees and supplemented by periodic training.

10 The fundamental importance of robust password policies as a key security measure was stressed by the PDPC in *Re Lovebonito Singapore Pte Ltd*[11] ("*Lovebonito*"). Here, the organisation used an external vendor's cloud-based Content Management System ("CMS") to host and run its e-commerce website. Investigations found that the organisation's CMS account with administrator privileges was likely compromised and used by a threat actor to access and exfiltrate customer personal data, including order data and credit card data.

11 In finding the organisation in breach, the PDPC noted that the organisation had followed the PDPC's recommendations[12] by adopting a default password policy implementing password length requirements and a lockout after a number of failed login attempts. However, the PDPC found that considering the volume and sensitivity of the personal data, more

9 *Eg*, biometric authentication, token-based authentication, multi-factor authentication, and others.

10 *Ie*, an organisation's obligation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. Personal Data Protection Act 2012 (2020 Rev Ed) s 24.

11 [2022] SGPDPC 3.

12 Set forth in Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017).

robust and stringent measures were required and the organisation's password policy should also have:[13]

(a) mandated periodic password changes, the frequency being based on the risk of damage to the individual if the data was compromised;
(b) prevented the organisation's employees from using easily guessable passwords (*eg*, incorporating the organisation's name); and
(c) complemented its technical password policy with a written password policy.

12 The cases also establish that the larger the volume and the greater the sensitivity of personal data in an organisation's possession or control, the stronger the security arrangements that must be put in place in order for the organisation to meet the Protection Obligation.

13 In *Re Quoine Pte Ltd*[14] ("*Quoine*"), the organisation ran a global cryptocurrency exchange and regularly dealt with a large volume of sensitive financial personal data. An account used by the organisation for automation tasks and to run codes ("DevOps Account") was compromised by a threat actor and the personal data of 652,564 customers was exfiltrated. In finding the organisation in breach of the Protection Obligation, the PDPC highlighted two shortcomings:

(a) the organisation should have carried out correctly-scoped periodic security reviews to detect vulnerabilities, assess security implications and risks, and ensure reasonable security arrangements were implemented for the DevOps Account. The failures in this regard were especially egregious, given how the DevOps Account had privileged access to the organisation's cloud platform containing Application Programming Interface ("API") keys/tokens to its databases and the personal data of customers stored within;[15] and
(b) the organisation had failed to put in place IT controls to manage data protection risks, including setting appropriate access control rules, access rights, restrictions for specific user roles, and strengthening database security. For instance, the organisation could have implemented two-factor authentication ("2FA") for the DevOps

13 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [18]–[22].
14 [2022] SGPDPC 2.
15 *Re Quoine Pte Ltd* [2022] SGPDPC 2 at [16]–[22].

Account, and could have limited access to the password change functions of that account.[16]

14 Further, the PDPC will not consider the implementation of system-enforced password requirements alone as sufficient. Such requirements should be properly documented in the form of a written password policy, disseminated widely to employees, and supplemented by appropriate employee training.

15 In *Re Tanah Merah Country Club*[17] ("*Tanah Merah Country Club*"), the organisation had disseminated e-mail IT newsletters and implemented a system-enforced domain password policy (*viz*, changing passwords once every three months, and using passwords of at least eight characters with a combination of uppercase, lowercase, special characters and numbers). However, the organisation failed to further develop its password requirements into a fully-fledged password policy in writing and disseminate it in a manner which could be easily referred to by new and old employees at any time.[18] Further, its IT newsletter had endorsed a password incorporating the organisation's name ("TMCC_Password_123") as a good password, even though such passwords would be easily guessable.[19] Subsequently, an employee's e-mail account with the password ("TMCC@1234") was compromised in a likely password spraying attack, and the personal data of 467 individuals was accessed and used to send various phishing e-mails.[20]

16 In finding the organisation in breach of the Protection Obligation, the PDPC emphasised the importance of a properly documented password policy as a key IT policy for the protection of personal data. The PDPC also emphasised the critical and necessary importance of training all employees who have to handle personal data in the course of their work, so

16 *Re Quoine Pte Ltd* [2022] SGPDPC 2 at [26]–[29].

17 [2020] SGPDPCS 7.

18 *Re Tanah Merah Country Club* [2020] SGPDPCS 7 at [6].

19 *Re Tanah Merah Country Club* [2020] SGPDPCS 7 at [11]. The PDPC declined to endorse this as a good password, and highlighted that a password complying with recommended complexity rules could still be weak if it incorporates easily guessable components like the organisation's name.

20 *Ie*, where a few common/default passwords are used against many different accounts, as opposed to a traditional brute force attack where many passwords are used against a single/few targeted account(s).

that the organisation can successfully adopt and implement policies and best practices necessary to protect personal data in its possession and/or control. In this case, the organisation had failed to provide structured and organised staff training on the handling and protection of personal data.[21]

B. Multi-factor authentication

17 As cyberthreats and the tools available to guard against them increase in sophistication, the PDPC's expectations have correspondingly risen. In *Re Trinity Christian Centre Limited*[22] ("*Trinity Christian Centre*"), a threat actor exploited compromised administrator account credentials to remotely enter the organisation's network via an open and publicly exposed remote desktop protocol port and executed ransomware attacks, rendering the organisation's database servers inaccessible. The personal data of 72,285 individuals was affected, though there was no evidence of exfiltration.

18 In finding the organisation in breach of the Protection Obligation, the PDPC noted that separate access controls (*ie*, separate logins) could have been implemented for better protection. Given the number and type of personal datasets concerned, and considering the prevalence of increasingly sophisticated phishing/social engineering techniques, the PDPC considered that adding another layer of access control protection for backend database servers (above and beyond reliance on frontend password protection) was a required reasonable security measure, which the organisation had failed to do.[23]

19 Further, in *Lovebonito*, the PDPC stressed that given their broader availability, 2FA/multi-factor authentication ("MFA") tools should be adopted as a baseline standard for all accounts with administrative privileges/access to systems holding large volumes of personal data or personal data of a confidential or sensitive nature where a data breach could result in adverse impact to the affected individuals.[24] The PDPC elaborated on this with a three-tiered approach:[25]

---

21 *Re Tanah Merah Country Club* [2020] SGPDPCS 7 at [9], [12]–[13].

22 [2022] SGPDPCS 3.

23 *Re Trinity Christian Centre Limited* [2022] SGPDPCS 3 at [9].

24 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [45]–[48].

25 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [51].

(a) First, 2FA/MFA should be implemented as a baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data. Failure to do so can *ipso facto* amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.

(b) Second, remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should *a fortiori* be secured by 2FA/MFA. The higher the risks concerning remote access, the higher the expectation to implement 2FA/MFA will be.

(c) Third, organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA/MFA, if this is a feature that is available out-of-the-box – and omission to do so may be considered an aggravating factor.

C. Data inadvertently publicly accessible

20 Another concern to highlight from the cases is the importance of organisations taking steps to ensure that files containing personal data are neither accidentally made available on a website/web application (in particular code repositories such as GitHub), nor stored in publicly accessible folders or areas potentially subject to web crawling/indexing.

21 For instance, in *Re Budgetcars Pte Ltd*[26] ("*Budgetcars*"), by changing a few digits of a tracking ID used on the organisation's delivery tracking website, access could be gained to the personal data of another individual. In finding the organisation in breach of the Protection Obligation, the PDPC reiterated the risks of unauthorised access arising from altering numerical references (*ie*, insecure direct object reference).[27]

22 Web crawlers in search engines (as well as ChatGPT and other artificial intelligence technologies) also pose a concern in securing personal data against inadvertent public disclosure. In *Re North London Collegiate*

26 [2022] SGPDPCS 13.

27 *Re Budgetcars Pte Ltd* [2022] SGPDPCS 13 at [5].

School (Singapore) Pte Ltd[28] ("*North London Collegiate School*"), the organisation failed to secure its website directory/folder adequately from automatic indexing by web crawlers. As a result, documents submitted by parents of prospective students for admission to the organisation were indexed by search engines and could show up in online search results. The affected personal data included the passport, National Registration Identity Cards ("NRICs"), photographs, birth certificates, academic reports and immunisation records of up to 1,742 individuals.

23 While the organisation had relied solely on a Robots.txt file deployed on its website to instruct search engines to refrain from indexing the documents, the PDPC highlighted that the robots exclusion protocol was not mandatory and relied on web crawlers' compliance without an enforcement mechanism (*eg*, proper directory/folder permissions and access controls) to prevent unintended access by web crawlers.[29] Accordingly, the organisation was found in breach of the Protection Obligation.

24 The embedding of keys/passwords in source code and the storing of source code in online and unsecured public repositories is another common pitfall which organisations should be aware of. In *Re MyRepublic Limited*[30] ("*MyRepublic*"), customers applying for mobile telecommunication services from the organisation would submit documents for identity verification ("KYC Documents") on the organisation's portal ("Portal"). These documents were stored in a bucket on cloud storage provided by Amazon Web Services ("AWS Bucket"). The AWS Bucket was publicly accessible but could only be accessed through a key ("Access Key").

25 A threat actor subsequently obtained the Access Key, gained access to the AWS Bucket, exfiltrated and deleted a large amount of data including the personal data of 79,388 individuals such as scanned NRIC copies. Investigations determined that the threat actor had likely exploited two vulnerabilities:

(a) the disclosure of the Access Key in the Portal's functionality which displayed technical information; and

---

28 [2021] SGPDPCS 14.

29 *Re North London Collegiate School (Singapore) Pte Ltd* [2021] SGPDPCS 14 at [6].

30 [2019] PDP Digest 224.

(b) the Access Key was stored in the Portal's source code to facilitate transfer of the KYC Documents to the AWS Bucket. Unfortunately, this source code was then stored on a repository which was available to all the organisation's developers, one of whom may have inadvertently disclosed the Access Key.[31]

26 In finding the organisation in breach of the Protection Obligation, the PDPC noted that given the high volume and sensitivity of customer personal data, stronger security measures should have been implemented. In particular, the PDPC found that:

(a) The organisation should not have left the Access Key publicly accessible through the "PHP Info" URL, as anyone who knew or could guess this URL could have obtained the Access Key and used it to access the AWS Bucket. The organisation should have either disabled the "PHP Info" function or moved the Access Key from the Portal's system environment variables to configuration files available only to authorised parties.[32]

(b) The organisation should not have embedded the Access Key into the Portal's source code (which was available to all the organisation's developers via the source code repository), as this was an avenue for the inadvertent disclosure of the Access Key by one of the developers or otherwise for the threat actor to gain access. This was a risk cautioned against by AWS' reference guide on security credentials. The organisation could have stored the Access Key in a file separate from the source code and secured with separate access controls, or utilised third party access key management solutions.[33]

(c) Given the high volume and sensitivity of personal data in the AWS Bucket, the AWS Bucket should not have been publicly

31 *Re MyRepublic Limited* [2019] PDP Digest 224 at [8].

32 *Re MyRepublic Limited* [2019] PDP Digest 224 at [18]. As noted by the PDPC, the "PHP Info" functionality is a standard function of the PHP programming environment which helps programmers to understand the configuration of the environment. If enabled by executing a PHP script file, accessing the "PHP Info" URL would display the Portal's operating system environment variable values (including the Access Key).

33 *Re MyRepublic Limited* [2019] PDP Digest 224 at [19].

available and access should have been restricted to only authorised applications users who required access.[34]

D. Vendor management

27 Another common pitfall emerging from the cases is the failure of organisations to conduct proper due diligence on third-party vendors. The PDPC has taken a relatively strict approach towards ensuring that organisations are aware of the risks posed by third-party vendors and that they take adequate measures to protect personal data when engaging such vendors, including having a written contract with and to have oversight over them, as the cases illustrate.

28 In *Re Nature Society (Singapore)*[35] ("*Nature Society*"), vulnerabilities in the organisation's website were exploited through a Structured Query Language ("SQL") injection attack which led to the personal data of 5,131 individuals being accessed and exfiltrated by unknown parties. Notably, after the organisation's website was designed and developed by an external vendor in 2011, the organisation did not have any contract/retainer agreement with the external vendor to maintain the website's security. Consequently, the organisation bore sole responsibility for protecting its website, but failed to carry out any security measures, *eg*, conducting necessary security updates, patches and penetration tests, thus leaving its website vulnerable to attacks. The organisation was found in breach of the Protection Obligation and a financial penalty of $14,000 was imposed.[36]

29 In *Trinity Christian Centre*, the PDPC also noted that the initial unauthorised entry to the organisation's network was through an administrator account that the organisation had assigned to an IT vendor it had engaged to develop and test applications. The organisation had failed to stipulate data protection requirements in its contract with its IT vendor, despite being aware that the IT vendor would process personal data. In finding the organisation in breach of the Protection Obligation, the PDPC emphasised the need for organisations to ensure that any engaged IT

34 *Re MyRepublic Limited* [2019] PDP Digest 224 at [22]–[25].

35 [2021] SGPDPCS 15.

36 *Re Nature Society (Singapore)* [2021] SGPDPCS 15 at [8].

vendors are aware of the need for personal data protection by stipulating this in the contractual terms.[37]

30 In *Re Audio House Marketing Pte Ltd*[38] ("*Audio House*"), the organisation's website was built/developed by a company ("Website Developer") engaged by the organisation's main IT vendor on behalf of the organisation. As such, the organisation did not have any contract with the Website Developer and failed to stipulate clear job specifications or any data protection requirements on the Website Developer. The organisation's contract with its main IT vendor also lacked any data protection requirements, despite the organisation's reliance on the main IT vendor to manage and maintain its IT systems. In finding the organisation in breach of the Protection Obligation,[39] the PDPC highlighted that organisations engaging IT vendors should:[40]

> (a) stipulate personal data protection requirements on the vendors;
> (b) make clear the job specifications, especially where they include security maintenance and software updates;
> (c) exercise reasonable oversight over the vendor responsible for the technical capabilities of the organisation so as to offer adequate protection to the types of personal data that may be affected by the engagement of the vendor; and
> (d) in cases where sub-contracting is contemplated, the organisation should identify requirements in its main contract that it requires its main IT vendor to impose similar obligations on and exercise adequate oversight over its sub-contractor.

31 In *Re Vhive Pte Ltd*[41] ("*Vhive*"), a threat actor exploited the organisation's outdated webserver service and unpatched firewall to remotely execute unauthorised code on the organisation's e-commerce

---

37 *Re Trinity Christian Centre Limited* [2022] SGPDPCS 3 at [7(b)]–[10].

38 [2022] SGPDPCS 11.

39 A threat actor exploited vulnerabilities in PHP files used to develop a web application on the organisation's website to carry out a SQL injection ransomware attack on the organisation's customer database. Personal data of 98,000 individuals including name, addresses and other contact information were affected.

40 *Re Audio House Marketing Pte Ltd* [2022] SGPDPCS 11 at [8].

41 [2022] SGPDPCS 8.

server, gain backdoor access and carry out a ransomware attack. Although the organisation had engaged an IT vendor to host, manage and maintain all its IT systems (including its e-commerce server), there was, in fact, no written contract. In finding the organisation in breach of the Protection Obligation, the PDPC highlighted the need to consider and properly document an IT vendor's scope of work as part of the written contractual terms. The PDPC found that the organisation's failure to do so not only meant that there was a lack of clarity on the scope of work expected from the IT vendor, but also that the organisation had failed to stipulate clear written security maintenance and data protection requirements to its IT vendor. This ultimately resulted in a lack of system maintenance, including security maintenance by the organisation.[42]

E. Intra-group arrangements

32 Following on from the point above, the cases also illustrate that the imperative for organisations to clearly delineate data protection responsibilities and requirements applies not just when dealing with external vendors, but also with organisations within the same corporate group.

33 In *North London Collegiate School*, the organisation had relied on a related group company to set up and manage its website, including making necessary security arrangements to protect collected personal data. However, the PDPC found that there were no clear business requirements (*eg*, contractual stipulations) specifying the organisation's reliance on its related group company to recommend and/or implement security arrangements to protect the affected personal data. Notably, the PDPC highlighted that when using/receiving IT services provided by a related group company, an organisation should ensure that the related group company is bound by either written agreements or group rules to protect personal data in the course of providing such services. Absent such clear written personal data protection requirements, the responsibility for

42 *Re Vhive Pte Ltd* [2022] SGPDPCS 8 at [7]–[9].

compliance with the Protection Obligation remained squarely with the organisation.[43]

F. E-mail auto-forwarding risks

34 E-mail auto-forwarding is also a risk which organisations should be cognisant of. In *Re Farrer Park Hospital Pte Ltd*[44] ("*Farrer Park*"), e-mails were automatically forwarded from two employees in the organisations' marketing department to a third party. The personal data of 3,539 individuals was affected including name, gender, nationality, date of birth, NRIC/passport details and medical information. At the time of the incident, the organisation's work e-mail accounts were hosted on Microsoft Office 365 ("Office 365") and employees were able to access their e-mail accounts via web-mail. Subsequently, it was discovered that the affected e-mail accounts had been configured to automatically forward all incoming e-mails to the third party.

35 The PDPC highlighted the well-known security risks associated with the automatic forwarding of e-mails to external domains and their exploitation by threat actors in prior cases. While the PDPC acknowledged the usefulness of e-mail auto-forwarding in serving valuable needs for some e-mail accounts, it also highlighted that the Protection Obligation requires organisations as part of their periodic security review to assess and manage the risks of doing so.[45]

36 In this case, the organisation had conducted a risk assessment on the use of Office 365, but this lacked a specific assessment of the risks arising from Office 365's default setting allowing the use of e-mail auto-forwarding. Nevertheless, considering the lack of industry practice, guidance, standards or benchmarks at the time of the incident recommending the disabling of e-mail auto-forwarding, the organisation was given the benefit of the doubt and the PDPC did not factor in the omission to assess the risk of enabling e-mail auto-forwarding in determining the enforcement action to be taken. The organisation was

---

43 *Re North London Collegiate School (Singapore) Pte Ltd* [2021] SGPDPCS 14 at [7]–[8].

44 [2022] SGPDPC 6.

45 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [22]–[26].

found in breach of the Protection Obligation on the basis of other inadequacies in protecting the e-mail accounts.

37 In future cases, the PDPC stressed (and organisations would do well to note) that failure to make a reasonable assessment of the risks arising from e-mail auto-forwarding would be a breach of the Protection Obligation that would be met with the appropriate enforcement action.[46]

V. The Personal Data Protection Commission's enforcement approach

A. Aggravating and mitigating factors

38 The PDPC has discretion in determining what sanctions to impose for breaches of the personal data protection provisions of the PDPA. A review of the cases is helpful in yielding certain observations on fact matrices which the PDPC may regard as aggravating or mitigating in deciding the appropriate enforcement measure to pursue (*eg*, accepting a voluntary undertaking, issuing directions for compliance, imposing a financial penalty and the quantum of such penalty, *etc*).

39 The case of *Re Neo Yong Xiang*[47] ("*Neo Yong Xiang*") presents some examples of factors which the PDPC regards as aggravating. Here, an exclusive retailer of mobile SIM cards misused the personal data of customers to register additional SIM cards for illegal sale which were subsequently used to send spam and/or scam messages in breach of the Do Not Call ("DNC") provisions of the PDPA. In imposing a financial penalty, the PDPC considered the following factors as aggravating:[48]

> (a) the breaches were difficult to detect and involved high degree of planning/premeditation to evade detection;
> (b) there was abuse of customer trust by misusing personal data;
> (c) the breaches caused inconvenience to innocent parties who received unsolicited spam and/or scam messages; and

46 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [27].
47 [2021] SGPDPC 12.
48 *Re Neo Yong Xiang* [2021] SGPDPC 12 at [18].

(d) the respondent had received financial gain of at least $15,000 through his misuse of the personal data.

40 Conversely, in imposing financial penalties, the PDPC considers mitigating factors including the personal and financial circumstances of the organisation/individual, bearing in mind that financial penalties imposed should avoid imposing a crushing burden or cause undue hardship on organisations.[49] Thus in *Neo Yong Xiang*, in reducing the quantum of the financial penalty to $21,000, the PDPC also considered the fact that the respondent was facing financial difficulties, had low savings/monthly income, had several outstanding vehicle, housing and renovation loan liabilities, and was responsible for paying the medical bills of his parent.[50] Similarly, in *Ngian Wen Hao Dennis*, the PDPC found that a financial penalty would impose a crushing burden resulting in undue hardship and hence administered a warning instead on the basis that the respondent was in poor health, was unemployed since 2018, had little savings, and was dependent on his aged father for financial support.[51]

B. Extensive mitigation/remediation plan as a factor in the Personal Data Protection Commission accepting voluntary undertakings

41 The introduction of voluntary undertakings as an enforcement measure has also afforded the PDPC additional flexibility in handling cases where organisations have demonstrated willingness and ability to adopt remedial measures to address concerns and improve personal data protection practices. In particular, the PDPC decisions relating to voluntary undertakings have highlighted the need for organisations to have a clear and effective data breach remediation plan in place before any data breach incident, so as to rectify the causes of a breach and minimise its impact in a timely manner.

42 In the 2022 cases where the PDPC accepted voluntary undertakings (namely, JT Legal LLC,[52] Asia Petworld Pte Ltd[53] and HSL Constructor

49 *Re Neo Yong Xiang* [2021] SGPDPC 12 at [21].

50 *Re Neo Yong Xiang* [2021] SGPDPC 12 at [19]–[20].

51 *Re Ngian Wen Hao Dennis* [2022] SGPDPCS 9 at [11].

52 Personal Data Protection Commission, "Undertaking by JT Legal LLC" <https://www.pdpc.gov.sg/Undertakings/Undertaking-by-JT-Legal-LLC> (accessed 27 February 2023).

Pte Ltd[54]), the data breaches concerned had arisen from cyberattacks (*eg*, e-mail phishing, ransomware) and involved personal data such as names, addresses, NRIC details and financial and medical information. A common observation in these cases is that post-incident, each of the organisations had readily implemented a mitigation/remediation plan comprising various steps including:

(a) reformatting affected computers/resetting affected passwords;

(b) implementing MFA protection for administrative/user accounts;

(c) implementing password protection for files/documents in accordance with a password policy prescribing complexity/periodic password change requirements;

(d) implementing dedicated anti-virus software;

(e) closing unused firewall ports;

(f) conducting an IT infrastructure review (including decommissioning outdated and unsupported hardware/software and regularly installing security patches/updates);

(g) developing, reviewing and updating its personal data protection policy/guidelines, including an internal reporting system for data incidents; and

(h) implementing training and awareness for staff.

43 The measures identified above will offer organisations some instructive lessons in developing a remediation plan for data breaches which may go some way towards the PDPC's acceptance of a voluntary undertaking. The PDPC's acceptance, and the successful completion by organisations, of the undertaking will lead to a more satisfactory regulatory outcome as the organisation will not be found to be in breach of the PDPA. This avoids the imposition of any financial penalties, and also preserves the organisation's business reputation and customer confidence.

---

53 Personal Data Protection Commission, "Undertaking by Asia Petworld Pte Ltd" <https://www.pdpc.gov.sg/Undertakings/Undertaking%20by%20Asia%20Petworld%20Pte%20Ltd> (accessed 27 February 2023).

54 Personal Data Protection Commission, "Undertaking by HSL Constructor Pte Ltd" <https://www.pdpc.gov.sg/Undertakings/Undertaking%20by%20HSL%20Constructor%20Pte%20Ltd> (accessed 27 February 2023).

VI. Concluding remarks

44 Overall, the decisions of the PDPC reflect the growing importance of personal data protection in Singapore, in light of challenges and risks arising from the digital transformation of businesses and the growing prevalence of emerging technologies such as artificial intelligence, blockchain-based technologies and the Internet of Things. As the nature of threats to data protection and the technological tools available to secure personal data evolve, it is expected that the PDPC's expectations of organisational compliance with the PDPA and its approach towards enforcement is likely to grow correspondingly.

45 Organisations would therefore do well to take data protection seriously and implement appropriate measures to protect themselves from data breaches. This includes implementing appropriate security measures, investing in training and awareness programmes for employees, having written contracts with vendors on their data protection responsibilities and exercising supervision over them, and having a clear and effective management and remediation plan for data breaches. The PDPC's enforcement approach in the cases illustrates the importance of accountability for all organisations subject to the PDPA.

ISSN 2529-7708

MCI (P) 048/04/2023