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.